HANSER

Leseprobe

zu

Mensch und Informationssicherheit

von Kristin Weber

Print-ISBN: 978-3-446-47645-5
E-Book-ISBN: 978-3-446-48040-7
E-Pub-ISBN: 978-3-446-48077-3

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446476455
sowie im Buchhandel

Inhalt

1 Der Faktor Mensch in der Informationssicherheit 1
1.1 Der Mensch als Lösung 2
1.2 Wer bin ich – und wenn ja, wie viele? 7
1.3 Informationssicherheit 12

2 Der Mensch als Bedrohung 19
2.1 It's me, hi, I'm the problem, it's me 19
2.1.1 Typische Szenarien – (un)sicheres Verhalten 20
2.1.2 Gründe für unsicheres Verhalten 24
2.2 Enemy Mine – Malicious Insider 30
2.2.1 Insider 31
2.2.2 Insider Threats 33
2.2.3 Typen von Malicious Insidern 34
2.2.4 Maßnahmen gegen Malicious Insider 38

3 Der Mensch als Opfer 43
3.1 Die Kunst des No-Tech-Hackings 44
3.1.1 Social Engineering 44
3.1.2 Social Engineering Attack Cycle 45
3.1.3 Social Engineering-Ontologie 49
3.2 Die Methoden der Social Engineers 51
3.2.1 Phishing 51
3.2.2 Watering Hole Attack 56
3.2.3 Impersonating/Pretexting 57
3.2.4 Reverse Social Engineering 59
3.3 Menschen manipulieren 60
3.3.1 Thinking, Fast and Slow 60
3.3.2 Autorität 61
3.3.3 Soziale Bewährtheit 63
3.3.4 Sympathie, Ähnlichkeit und Täuschung 65
3.3.5 Verpflichtung, Gegenseitigkeit & Konsistenz 66
3.3.6 Ablenkung 68

4 Information Security Awareness 71
4.1 Grundlagen Information Security Awareness 72

4.1.1 Awareness im Kontext Informationssicherheit 72
4.1.2 Erkenntnisse aus der Verhaltenspsychologie 77
4.1.3 Individualisierung 83
4.2 Vorgehensmodell zur zielgerichteten Sensibilisierung 90
4.2.1 Das Vorgehensmodell im Überblick 91
4.2.2 Analysephase 93
4.2.3 Umsetzungsphase 98

5 Information Security Awareness fördern 103
5.1 Wissen erhöhen und Fähigkeiten fördern 104
5.1.1 Wissen 105
5.1.2 Lernen 106
5.1.3 Gestaltung didaktischer Szenarien 111
5.1.4 Mediendidaktik 113
5.2 Verhaltensabsicht fördern und beeinflussen 114
5.2.1 Einstellungen 116
5.2.2 Wahrgenommene Norm 120
5.2.3 Persönliche Handlungsfähigkeit 125
5.3 Salienz fördern 133
5.3.1 Begriff und Konzepte zur Salienz 133
5.3.2 Förderung der Salienz 136
5.4 Gewohnheiten fördern 140
5.4.1 Merkmale von Gewohnheiten 141
5.4.2 Gewohnheitsmäßiges Verhalten 142
5.4.3 Faktoren zur Förderung von Gewohnheiten 143
5.4.4 Überführung von alten in neue Gewohnheiten 148

6 Messen von Information Security Awareness 151
6.1 Hintergrund – warum, was und wie messen 151
6.2 Messen von Wissen und Fähigkeiten 155
6.3 Messen der Verhaltensabsicht 160
6.3.1 Einstellungen bewerten 161
6.3.2 Bewertung wahrgenommener Normen 164
6.3.3 Bewerten der persönlichen Handlungsfähigkeit 167
6.4 Messen von Salienz 171
6.4.1 Salienz personenbezogen messen 172
6.4.2 Salienz unternehmensbezogen messen 174
6.5 Messen der Gewohnheitsstärke 178

7 Zukunft Mensch 181

Literaturverzeichnis 185

Stichwortverzeichnis 195

3 Der Mensch als Opfer

„Only amateurs attack machines; professionals target people."

(Schneier, 2000)

Angreifende entscheiden sich häufig bewusst dafür, nicht die technische Infrastruktur anzugreifen. Sie versuchen, Sicherheitsmaßnahmen zu umgehen, indem sie gezielt den Menschen angreifen bzw. ausnutzen. Der Mensch ist ein lohnendes Angriffsziel, da er wertvolle Informationen besitzt oder Zugriff darauf hat (vgl. H. Lauer & Kuntze, 2022, S. 38). Als Social Engineering werden die meisten Angriffsformen bezeichnet, bei denen Menschen geschickt manipuliert werden. Phishing-Mails dienen beispielsweise dazu, Passwörter abzugreifen, oder Social Engineers geben sich als Technikpersonal aus, um Zugang zu einem Gebäude oder Raum zu erhalten.

Obwohl hier in der Rolle als „Opfer" werden Mitarbeitende auch zur „Bedrohung", wenn sie auf Angriffe und Manipulationsversuche falsch reagieren (vgl. Abschnitt 2.1). Wenn sie beispielsweise eine Phishing-Mail nicht an den Helpdesk melden, wenn sie eine unbekannte Person auf dem Firmengelände nicht ansprechen, wenn sie auf einen Link in einer Phishing-Mail klicken oder einen gefundenen USB-Stick mit ihrem Rechner verbinden. Häufig erkennen Menschen nicht, dass sie gerade Opfer eines Angriffs sind.

Dieses Kapitel erläutert das Phänomen Social Engineering näher und erklärt, warum Menschen so leicht Opfer von geschickter Manipulation werden. Prinzipien, Taktiken und Techniken des Social Engineerings werden vorgestellt. Der Social Engineering Attack Cycle zeigt den typischen Ablauf eines Social Engineering-Angriffs. Die Social Engineering-Ontologie dient dazu, Social Engineering-Angriffe systematisch zu beschreiben und zu analysieren.

Im Anschluss werden typische Formen von Social Engineering wie (Spear) Phishing, CEO Fraud, Impersonating und Watering Hole Attacks anhand von Beispielen erläutert. Social Engineers sind Meister der Manipulation und nutzen geschickt psychologische Prinzipien aus, um ihre Opfer auszutricksen, sodass sie im Sinne der Social Engineers handeln. Diese Tricks werden am Ende des Kapitels erklärt.

3.1 Die Kunst des No-Tech-Hackings

„Cracking the human firewall is often easy,
requires no investment beyond the cost of a phone call,
and involves minimal risk.“

(Mitnick & Simon, 2002, S. 13)

Social Engineering ist eine ernst zu nehmende Bedrohung für die Informationssicherheit. Diese raffinierte Angriffsmethode ist eine Kunst, die gezielt menschliche Schwächen und soziale Manipulation nutzt, um Zugang zu sensiblen Informationen oder Systemen zu erlangen. Die IT-Infrastruktur kann durch teure Maßnahmen noch so sicher sein, gegen neugierige Blicke und gezielte Angriffe auf den Menschen helfen diese Maßnahmen nicht.

Dieser Abschnitt erläutert das Phänomen Social Engineering näher. Um Social Engineering erfolgreich zu erkennen und abzuwehren, ist es wichtig, zu verstehen, wie Social Engineering funktioniert. Mit dem Social Engineering Attack Cycle wird der typische Ablauf eines Social Engineering-Angriffs in vier Phasen erläutert. Die erste und wichtigste Phase ist das Information Gathering, in welcher Social Engineers ihre Opfer ausspionieren. Wie Social Engineers dabei vorgehen und welche geschickten Techniken (z. B. Dumpster Diving, Tailgating) sie dabei einsetzen, zeigt die Social Engineering-Ontologie.

3.1.1 Social Engineering

Social Engineering kann verschiedene Formen annehmen. Eine Verkäuferin, die ihren Kunden überredet, einen Anzug zu kaufen, der weit über seinem Budget liegt. Ein Polizeibeamter, der die Wahrheit herausfindet, obwohl der Kriminelle nicht die Absicht hatte, diese preiszugeben. Eine Anwältin, welche die Richterin dazu bringt, eine Entscheidung zugunsten ihres Mandanten zu treffen. Oder einfach ein Kind, das seine Eltern dazu überredet, am Abend eine weitere Folge seiner Lieblingsserie schauen zu dürfen.

In all diesen Beispielen überzeugt – oder manipuliert – Person A die Person B, etwas zugunsten von Person A zu tun. Oft merkt Person B nicht einmal, dass sie etwas getan hat, was sie eigentlich nicht beabsichtigt hatte. Person A ist in der Regel darin geschult, Menschen zu überreden, und es ist Teil ihrer Arbeit. Manchmal – zum Beispiel bei Kindern – ist es einfach ein ganz natürliches Verhalten oder sogar ein besonderes Talent.

Social Engineering beschreibt die gezielte Manipulation von Menschen. Menschen sollen so beeinflusst werden, dass sie im Sinne der Social Engineers und nicht notwendigerweise in ihrem eigenen Interesse handeln (Hadnagy & Wilson, 2011). In den oben genannten Fällen handelt es sich um typische und legale Formen der Interaktion zwischen Menschen. Social Engineering kann sogar zum Wohle der Manipulierten eingesetzt werden. Beispielsweise, wenn die Ärztin ihren Patienten davon überzeugt, regelmäßig seine Medikamente zu nehmen. Oder wenn der Vater seine Tochter dazu bringt, jeden Tag ihre Hausaufgaben zu machen.

Im Zusammenhang mit Informationssicherheit wird Social Engineering meist in seiner bösartigen und illegalen Form eingesetzt. Das sogenannte Human Hacking ist die am meisten

verwendete Angriffstechnik auf den Menschen. Die Konsequenzen eines solchen erfolgreichen Social Engineering-Angriffs sind schlimmer als der Kauf eines zu teuren Anzugs oder eine extra Stunde Fernsehen.

> *„Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."*
>
> (Mitnick & Simon, 2002, S. 2).

Manipulierte USB-Sticks oder Phishing-E-Mails sind typische Formen von Social Engineering. Ein gefundener USB-Stick soll bei den Findenden Neugier und Hilfsbereitschaft wecken. Sie verbinden den USB-Stick mit ihren Rechnern, um zu schauen, was sich darauf befindet – schon installiert sich eine Schadsoftware. Eine Phishing-E-Mail will die Adressierten dazu verleiten, ihre Log-in-Daten oder Kreditkartennummern auf einer Webseite der Angreifenden einzugeben. Beides sind Handlungen, die definitiv gegen die Interessen der Opfer verstoßen.

Aber auch gezielte Informationsbeschaffung zur Vorbereitung eines Angriffs ist Teil von Social Engineering. Schon scheinbar harmlose Fragen, eine gezielte Informationsrecherche über Organisationsstrukturen und Ansprechpersonen auf sozialen Netzwerken oder achtlos weggeworfene Dokumente helfen den Social Engineers, ihrem Ziel näher zu kommen.

Beim Social Engineering geben Angreifende häufig vor, jemand anders zu sein (sogenanntes Pretexting): die Chefin auf Dienstreise, der hilfsbereite IT-Administrator, ein interessierter Forschungspartner oder die Hilfe suchende Praktikantin. Die Angreifenden nehmen per E-Mail oder telefonisch Kontakt mit ihren Opfern auf und erzählen eine erfundene Geschichte. So braucht der angebliche IT-Admin ein Passwort oder einen Zugang zum PC, die erfundene Praktikantin ganz schnell einen Ausdruck oder die vermeintliche Chefin sofort eine Überweisung auf ein ausländisches Konto, um eine geheime geschäftliche Transaktion durchzuführen.

Die Social Engineers nutzen die auf diese Weise erlangten Informationen oder die unachtsamen Handlungen des Opfers in ihrem eigentlichen Angriff und erreichen so ihr beabsichtigtes Ziel. Sie erhalten beispielsweise Zugang zu vertraulichen Informationen oder stehlen Geld.

Human Hackers kennen sich gut mit Psychologie aus. Sie verstehen, wie Menschen „funktionieren", und sind in der Lage, sie zu ihren Gunsten zu beeinflussen. Beispielsweise vertrauen Menschen Autoritätspersonen fast blind und stellen deren Entscheidungen nicht unbedingt infrage. Social Engineers nutzen diese für Menschen typische angeborene oder antrainierte Verhaltensweisen gezielt zu ihrem Vorteil aus.

3.1.2 Social Engineering Attack Cycle

Ein wichtiger Schritt im Erkennen und Verhindern von Social Engineering-Angriffen ist, zu verstehen, wie Social Engineers arbeiten, wie sie ihre Angriffe vorbereiten und wie sie sie ausführen. Der Attack Cycle beschreibt das typische Muster eines Social Engineering-Angriffs (Allen, 2006; Mouton et al., 2016; Nyriak, o. D.). Der Angriffszyklus besteht aus vier Phasen. Ein typischer Social Engineering-Angriff zeigt alle vier Phasen in der genannten Reihenfolge (vgl. Bild 3.1). Er beginnt mit *Information Gathering*, gefolgt von *Establish Relationships and Rapport*, dann folgen *Exploitation* und schließlich *Execution*.

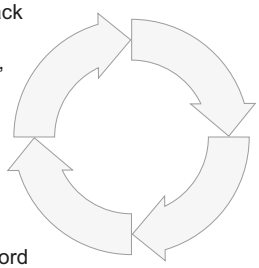


Bild 3.1 Die vier Phasen des Social Engineering Attack Cycle (in Anlehnung an Nyriak, o. D.)

Das „Sammeln von Informationen" über das potenzielle Opfer und seine Umgebung ist wahrscheinlich die wichtigste Phase von Social Engineering. Je mehr die Human Hacker über ihre Opfer wissen, desto besser können sie ihren Angriff planen und durchführen. Für das Sammeln von Informationen nutzen Social Engineers zunächst meist öffentlich verfügbare Informationen. Daher wird es auch als Open Source Intelligence, kurz **OSINT**, bezeichnet.

Social Engineers sammeln Informationen sowohl über das Unternehmen, welches sie angreifen wollen, als auch über die darin arbeitenden Personen. Relevante Informationen über Personen könnten sein (Hadnagy & Wozniak, 2018, S. 19):

- Welche Social-Media-Konten nutzt die Person?
- Welche Position hat die Person im Unternehmen?
- Arbeitet die Person von zu Hause aus, und wem ist sie unterstellt?
- Was und wo hat die Person studiert?
- Welche Hobbys hat sie, und wohin fährt sie in den Urlaub?
- Was sind die Lieblingsrestaurants der Person?
- Wie lauten die Namen der Familienmitglieder?

Die Informationen, die sie sammeln, betreffen auch das Unternehmen selbst. Zum Beispiel:

- Wie nutzt das Unternehmen das Internet und soziale Medien?
- Mit welchen Partnern und Dienstleistern arbeitet das Unternehmen zusammen?
- Wie nimmt das Unternehmen Zahlungen entgegen und bezahlt Rechnungen?
- Wo befinden sich der Hauptsitz, Callcenter oder andere Niederlassungen?
- Erlaubt das Unternehmen das Mitbringen eigener Geräte (BYOD)?
- Ist ein Organigramm verfügbar?
- Welche IT-Systeme nutzt das Unternehmen?

Als Quellen für die Informationssuche können zahlreiche Webseiten, Social-Media-Plattformen und Internettools verwendet werden[1]. Zudem nutzen Social Engineers nichttechnische Mittel, indem sie das Unternehmen, deren Partnerunternehmen oder Mitarbeitenden beobachten, auskundschaften, überwachen oder belauschen (ein sehr sehenswertes Video dazu (Long, 2007)).

Typische Mittel sind Shoulder Surfing, Dumpster Diving und Eavesdropping. **Shoulder Surfing** bedeutet, einer Person über die Schulter oder auf den Bildschirm bzw. die Tastatur zu schauen, während sie etwas in ihren Computer oder ihr Smartphone eingibt, mit dem Ziel, z. B. Log-in-Daten oder andere sensible Informationen abzulesen. Diese Technik funktioniert besonders gut in vollen und beengten Räumen oder öffentlichen Plätzen, wo die beobachtende Person ihrer Zielperson unbeobachtet oder unauffällig ganz nahekommen kann, z. B. im Zug, Flugzeug oder Café. Unter **Dumpster Diving** versteht man das Herumwühlen im Müll. Social Engineers versuchen so über mehr oder weniger öffentlich aufgestellte Müllcontainer an unachtsam und unsachgemäß entsorgte Informationen oder Datenträger des Unternehmens zu kommen, beispielsweise an alte Rechnungen. So eine alte Rechnung liefert unglaublich viele wertvolle Informationen: Mit wem macht das Unternehmen Geschäfte; wie sehen Briefkopf, Logo und Fußbereich einer Rechnung aus; welche Kontoverbindungen werden genutzt; wer arbeitet in der Buchhaltung; wie sehen typische Zahlungsziele aus usw. **Eavesdropping** bedeutet nichts anderes, als Personen zu belauschen, z. B. bei öffentlich geführten Gesprächen, Telefonaten oder Videokonferenzen. Auch durch geöffnete Fenster hindurch können sensible Informationen aus Gesprächen herausgehört werden. Sind Videokonferenzsysteme nicht richtig konfiguriert, kann sich jede Person, welche den richtigen Link hat, unbemerkt einklinken. Je nach Größe oder Anonymität der Veranstaltung werden ungewünschte Zuhörende nicht auffallen.

Ausgestattet mit den gesammelten Informationen bereiten die Social Engineers in der Regel einen sogenannten **Pretext** (deutsch in etwa „Vorwand") vor. Das sind eine gefälschte Person und Geschichte, die sie benutzen, um ihre Ziele zu erreichen; sei es die nette IT-Admin, der hilflose Praktikant, der verzweifelte Inspektor, die drängelnde Chefin oder die geistesabwesende Putzkraft. Je besser die gesammelten Informationen, desto besser passt der Pretext. Wenn er authentisch und plausibel ist, wird das Opfer wahrscheinlich darauf hereinfallen.

> *Annika, die sich über die verfrühte Einladung zur Faschingsparty freut, ist seit Jahren sehr fleißig auf Social Media unterwegs und postet Fotos von Partys, ihren Outfits und auch von ihren Fußballerfolgen im Verein. Ab und zu freut sie sich auch mit ihren Kolleg:innen über deren berufliche Erfolge. Für Pascal reichen diese Informationen schon aus, um eine passende Phishing-Mail zu generieren. Er hat Annikas Namen und den des Unternehmens, für das sie arbeitet. Somit kann Pascal ihre E-Mail-Adresse erraten oder auf der Webseite des Unternehmens recherchieren. Er weiß, dass Annika Fußball spielt und bei welchem Verein. Auf dessen Homepage wiederum finden sich bereits die Infos zur bevorstehenden Faschingsparty, die Kontaktdaten des Vereins und auch ein entsprechendes Logo. Und dass Annika immer auf den Faschingspartys unterwegs ist, ist für Pascal ebenfalls offensichtlich.*

[1] Für eine ausführliche Beschreibung mit zahlreichen Beispielen sei auf (Hadnagy & Wozniak, 2018, S. 32 ff.) verwiesen.

In der nächsten Phase „Aufbauen einer Beziehung“ versuchen die Social Engineers, getarnt mit ihrem Vorwand eine Verbindung zu ihrem Opfer herzustellen. Das kann bereits durch ein freundliches Lächeln und durch Augenkontakt passieren, wenn der Human Hacker zur Tür eilt, damit die Zielperson ihm die Tür offenhält. Eine persönliche Beziehung kann auch am Telefon aufgebaut werden, wenn über angeblich gemeinsame Hobbys, das letzte Urlaubsziel oder vermeintliche Bekanntschaften gesprochen wird. Oder die Empfangsdame in der Lobby wird in ein Gespräch über die Familie verwickelt, welches durch das Zeigen von Fotos oder nette Anekdoten untermauert wird. Es kann auch so weit gehen, dass eine Online-Beziehung mit der Zielperson über ein gefälschtes Profil auf einer Datingseite oder Social-Media-Plattform aufgebaut wird. An diesen Beispielen sieht man, wie wichtig es ist, möglichst viele nützliche Informationen über das Opfer gesammelt zu haben. Je mehr man über das Opfer weiß, umso eher gelingt es, eine Beziehung über angebliche Gemeinsamkeiten aufzubauen oder indem man bestimmte Anreize setzt, wie Hilfsbereitschaft, Neugier oder Anerkennung (vgl. Haucke et al., 2018). Mehr zu den beim Social Engineering eingesetzten psychologischen Prinzipien zeigt Abschnitt 3.3. Idealerweise ist die Verbindung so stark, dass das Opfer den Social Engineers vertraut.

> *Die von Pascal erstellte Phishing-Mail ist auf Basis der gesammelten Informationen so gestaltet, dass sie auf den ersten Blick legitim aussieht. Mit der vermeintlich richtigen Absendeadresse des Vereins, persönlicher Anrede, den richtigen Informationen zur Faschingsparty und einem passenden Footer mit Adresse und Logo baut die E-Mail Vertrauen auf. Zudem baut die Mail Druck auf Annika auf, schnell auf den Link zu klicken und sich anzumelden, weil die Karten immer begrenzt und schnell ausverkauft sind.*

In der dritten Phase „Ausnutzung“ wird die zum Opfer aufgebaute Beziehung zum Vorteil der Social Engineers ausgenutzt. Ziel ist es, das Opfer zu manipulieren und Sicherheitsmechanismen zu unterwandern, ohne dass es bemerkt wird. Die Ausbeutung kann auf unterschiedliche Weise erfolgen, Beispiele sind (Nyriak, o. D.):

- die Social Engineers anderen Mitarbeitenden im Unternehmen (als vertrauenswürdige Person) vorstellen
- Passwort und Log-in über das Telefon verraten
- einen manipulierten USB-Sticks in einen Firmencomputer einstecken
- Geschäftsgeheimnisse in einer Diskussion mit einer vermeintlichen „Kollegin“ offenlegen
- einen infizierten E-Mail-Anhangs öffnen
- Zugang zu einem abgeschlossenen Bereich gewähren

> *Für Annika sieht die Mail wie die Einladung zur diesjährigen Faschingsparty im Vereinsheim aus. Sie klickt auf den darin enthaltenen Link, um sich anzumelden.*

In der letzten Phase „Ausführung“ erreichen die Social Engineers das eigentliche Ziel ihres Angriffs. Wenn Social Engineers erfolgreich sind, haben sie möglicherweise Zugang zum gesamten Unternehmensnetzwerk, zu allen Datenbanken mit allen Kundendaten oder zu vertraulichen Informationen über das geistige Eigentum des Unternehmens. Sie wissen über die noch geheime Marketingkampagne oder die Pläne für die zukünftige Entwicklung des Unternehmens Bescheid und können diese Informationen an die Konkurrenz verkaufen.

Oder sie spionieren die Firma über Webcams aus. Sie können Daten verschlüsseln, sodass niemand mehr darauf zugreifen kann, und Lösegeld fürs Entschlüsseln verlangen. Sie sind in der Lage, Daten und Systeme zu manipulieren, z. B. die Zusammensetzung von Medikamenten, Produktions- oder Versandpläne, Finanztransaktionen, die Temperatur im Lager, die Webseite des Unternehmens oder den Webshop.

> *Durch den Klick auf den Link und den Besuch der gefälschten Webseite wird Pascals Code ausgelöst. Annikas Computer wird mit einer bösartigen Datei infiziert und verbindet sich mit dem System von Pascal. Sobald Annikas Computer verbunden ist, versucht Pascal, Informationen zu stehlen oder eine Ausweitung der Berechtigungen (Privilege Escalation) vorzunehmen. Ist er damit erfolgreich, kann Pascal Daten stehlen, in vertrauliche Bereiche vordringen oder Schlimmeres. Seine Social Engineering-Attacke war erfolgreich.*

Häufig endet die Attacke, bevor das Opfer anfängt, sich Fragen darüber zu stellen, was eigentlich gerade passiert. Stattdessen schaffen es geschickte Social Engineers, ihre Opfer mit einem guten Gefühl zurückzulassen, z. B. weil das Opfer jemandem geholfen, eine (noch geheime) Neuigkeit erfahren oder einen neuen Freund gewonnen hat. Idealerweise wissen die Opfer somit gar nicht, dass sie ausgenutzt wurden und zu einem erfolgreichen Angriff beigetragen haben. Die oder der Social Engineer bleibt im Verborgenen und kann die zum Opfer etablierte Beziehung gegebenenfalls sogar erneut ausnutzen.

3.1.3 Social Engineering-Ontologie

Der typische Ablauf eines Social Engineering-Angriffs erfolgt in vier Phasen. Welche Arten von Angriffen es gibt, welche Methoden und Techniken Social Engineers dabei einsetzen und welche Motive sie verfolgen, beschreibt eine Ontologie für Social Engineering. Das von Mouton et al. (2014) vorgeschlagene ontologische Modell ermöglicht die systematische Beschreibung und Analyse von Social Engineering-Angriffen. Ein erweitertes und detaillierteres ontologisches Modell findet sich in (Wang et al., 2021).

Gemäß Mouton et al. (2014) besteht ein Social Engineering-Angriff aus folgenden Komponenten: „A Social Engineering attack employs either direct communication or indirect communication, and has a social engineer, a target, a medium, a goal, one or more compliance principles and one or more techniques." (Vgl. Bild 3.2) Einige der Komponenten sind selbsterklärend, z. B. dass es sich beim Ziel oder Opfer um ein Individuum oder um eine Organisation handeln kann. Daher soll im Folgenden nur kurz auf einige Komponenten der Ontologie eingegangen werden. Beispiele für die Anwendung der Ontologie auf konkrete Angriffe finden sich in Abschnitt 3.2. Die „Compliance Principles" werden ausführlich in Abschnitt 3.3 dargestellt.

Von direkter Kommunikation spricht man, wenn angreifende Person und Opfer direkt miteinander kommunizieren. Direkte Kommunikation kann entweder bidirektional (z. B. per E-Mail, im Gespräch, per Telefon) oder unidirektional erfolgen. Einseitige Kommunikation erfolgt meist von der angreifenden Person zum Opfer, z. B. beim Phishing. Indirekte Kommunikation erfolgt über ein Medium, z. B. einen USB-Stick oder eine Webseite, ohne direkte Interaktion zwischen den Beteiligten.

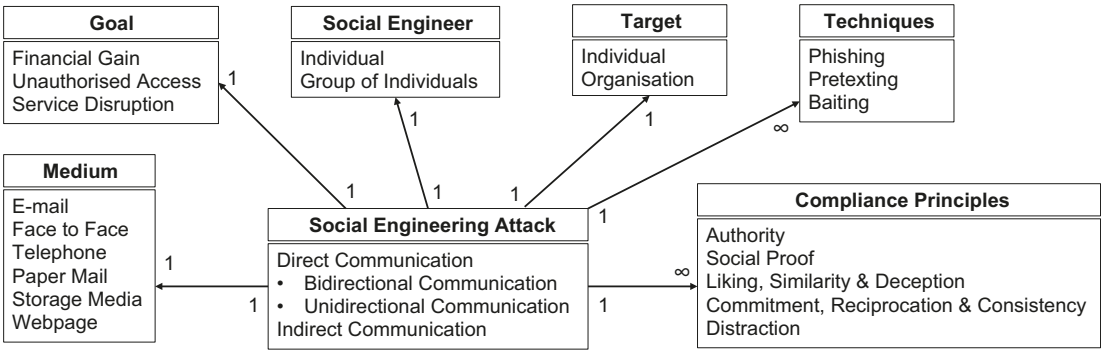


Bild 3.2 Ontologisches Modell eines Social Engineering-Angriffs (in Anlehnung an Mouton et al., 2014)

Die Liste der Techniken, welche Social Engineers nutzen, ist nahezu endlos und wird stetig erweitert. Die Techniken kommen in den verschiedenen Phasen eines Angriffs vor und werden auch miteinander kombiniert. Beim **Impersonating** (auf Deutsch etwa „jemanden imitieren oder nachahmen“) täuscht die angreifende Person vor, jemand anderes zu sein (s. Hadnagy & Wozniak, 2018, S. 241 ff.). Bei physischen Interaktionen, z. B. mit dem Ziel, in einen abgesperrten Bereich vorzudringen, sind Verkleidungen als Technikpersonal, IT-Dienstleister, Support für Verkaufsautomaten, Polizei oder Lieferdienst üblich. Impersonating wird in allen Formen des Phishings eingesetzt, weil die absendende Person immer vorgibt, eine andere Person (Chefin, Kollege, Freundin, nigerianischer Prinz ...) oder Institution (Bank, Kunde, Verein ...) zu sein. Diese Technik ist eng mit Pretexting verbunden.

Beim **Tailgating** oder **Piggybacking** (deutsch in etwa „sich an jemanden dranhängen“) lässt eine berechtigte Person die nicht autorisierte Person in einen nicht öffentlich zugänglichen Bereich hinein. Das Opfer hält z. B. einem sehr freundlich lächelnden vermeintlichen Kollegen aus Höflichkeit die Tür zum Bürogebäude offen. Vor allem in größeren Organisationen kennen sich nicht alle untereinander, und wenn das Erscheinungsbild des Social Engineers passend ist (auch hier wieder Impersonating), besteht eine große Wahrscheinlichkeit, dass diese Technik funktioniert.

Die Technik **Baiting** (deutsch „ködern“) wird beim Trick mit dem USB-Stick eingesetzt. Die angreifende Person hinterlässt einen manipulierten USB-Stick an einem Ort, an dem er von den Opfern wahrscheinlich gefunden wird, z. B. auf dem Parkplatz. Der USB-Stick ist mit dem Logo des Zielunternehmens oder anderen attraktiven Elementen versehen, um die Opfer dazu zu verleiten, den Stick mitzunehmen und in den Computer zu stecken. Nach dem Einstecken wird der bösartige Code automatisch ausgeführt. Andere typische Techniken wie Shoulder Surfing, Dumpster Diving und Pretexting wurden bereits erläutert. In Abschnitt 3.2 wird auf weitere Social Engineering-Techniken eingegangen, wie z. B. Phishing.

Das Modell von (Wang et al., 2021) unterscheidet präziser zwischen dem Ziel des Angriffs und der Motivation der Social Engineers (vgl. Bild 3.3). Mögliche Ziele eines Angriffs sind: Unterbrechung von IT-Dienstleistungen, Denial of Service, unerlaubter Zugriff auf Daten oder Systeme oder das Zerstören von Daten. Die dahinter liegenden Motive der Social Engineers können zahlreich sein: z. B. finanzielle oder Wettbewerbsvorteile erlangen, der Spaß an der intellektuellen Herausforderung, jemandem einen Streich spielen, Rache, externer Druck (z. B. durch Familienmitglieder oder das organisierte Verbrechen), politische oder religiöse

Hintergründe (Terrorismus, Fanatismus, Krieg, Spionage ...) oder das Image des Opfers beschädigen. Die Social Engineers können auch im eigenen Interesse handeln, um eigene Daten oder die von Bekannten zu ändern (vgl. Allen, 2006). Beispielsweise könnten Studierende versuchen, auf diesem Wege ihre Noten zu verbessern. Einige dieser Motive werden im Zusammenhang mit Insider Threats näher erläutert (vgl. Abschnitt 2.2.3).

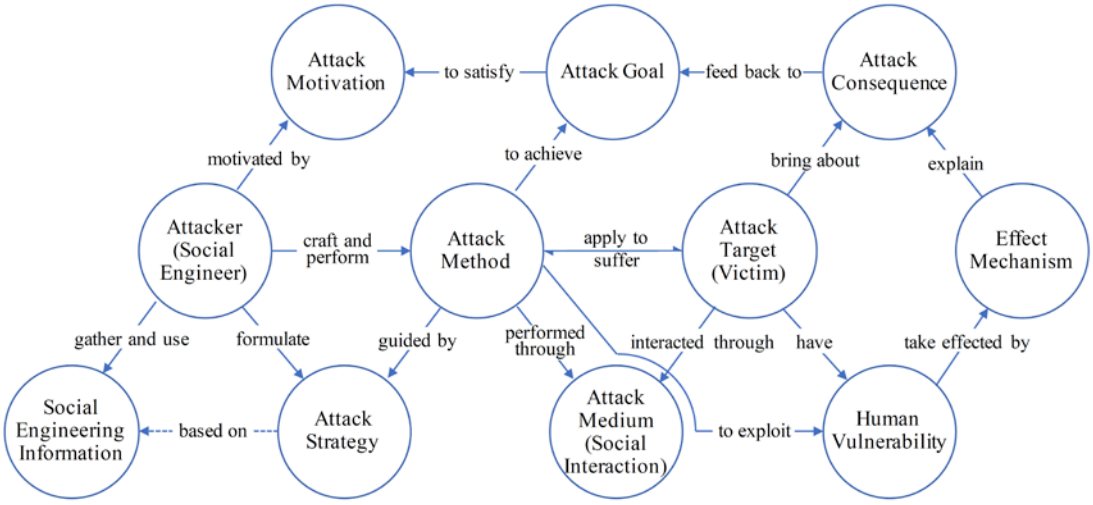


Bild 3.3 Die Social Engineering-Domänen-Ontologie (Wang et al., 2021, S. 11)

3.2 Die Methoden der Social Engineers

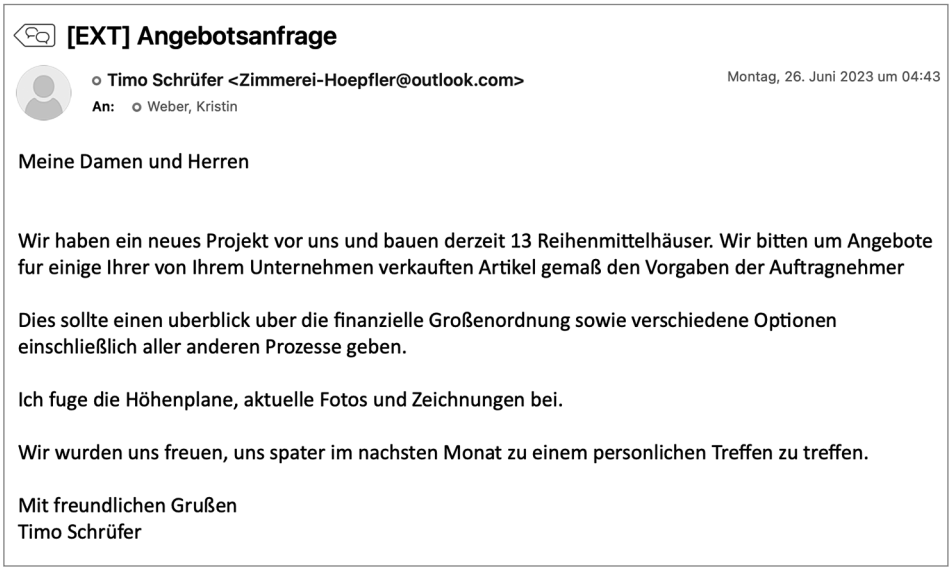
Social Engineers nutzen zahlreiche Instrumente, Techniken und Methoden in den verschiedenen Phasen ihrer Angriffe. Phishing, also das „Angeln" nach sensiblen Informationen wie Passwörtern, ist die Technik, die beim Social Engineering am häufigsten eingesetzt wird. Phishing gibt es in verschiedenen Formen – neben dem klassischen E-Mail-Phishing auch per Telefon oder SMS – und in verschiedenen Schwierigkeitsstufen. Zahlreiche weitere Angriffsszenarien und Methoden wie Pretexting, Reverse Social Engineering und Watering Hole Attacks, können dem Social Engineering zugeordnet werden. Diese und weitere Instrumente sollen im Folgenden vorgestellt werden.

3.2.1 Phishing

Die bekannteste und erfolgreichste Social Engineering-Technik ist Phishing. Phishing ist ein Versuch, unbefugten Zugang zu sensiblen Informationen zu erhalten. Oder die Phishing-Opfer sollen Handlungen durchführen, welche die Sicherheit ihrer Systeme gefährden, wie z. B. Dateien öffnen, um Schadsoftware zu installieren.

Ein gängiger Ansatz für Phishing-Angriffe ist das Versenden von E-Mails an mehr oder weniger zufällige E-Mail-Adressen. Die betrügerische E-Mail enthält einen Link zu einer gefälschten Webseite und einen Text, in dem die Opfer aufgefordert werden, dem Link zu folgen. Geben die Opfer ihre persönlichen Daten in das Formular auf der Webseite ein, haben die Angreifenden Zugriff auf die eingegebenen Informationen. Handelt es sich bei der gefälschten Webseite um eine exakte Kopie des Originals, wird die Person niemals vermuten, dass sie Opfer von Phishing geworden ist. Bei einer weiteren typischen Phishing-Variante enthält die E-Mail ein Dokument im Anhang, welches einen Schadcode enthält. Beim Öffnen des Dokuments installiert sich die Schadsoftware auf dem Rechner des Opfers. Es kann sich beispielsweise um einen Keylogger handeln, der alle auf dem Rechner eingegebenen Daten protokolliert und an die Angreifenden sendet.

Phishing-Nachrichten unterscheiden sich hinsichtlich ihrer Erkennbarkeit (vgl. Volkamer et al., 2020). Sehr einfach zu erkennende Phishing-Nachrichten enthalten meist einen eher kurzen Text mit Rechtschreib- und Grammatikfehlern und keine oder eine unpersönliche Anrede (vgl. Bild 3.4). Diese Nachrichten adressieren eine unbekannte Masse an Personen und werden in großer Anzahl verschickt. Schwer zu erkennende Nachrichten können inhaltlich, in ihrer Darstellung und aufgrund der Absendeadresse plausibel sein. Sehr schwer zu erkennende Phishing-Nachrichten werden von gehackten E-Mail-Konten aus verschickt und beziehen sich auf reale frühere Konversation, was sie fast ununterscheidbar von legitimen Nachrichten macht. Die letzten beiden Formen werden gezielt an eine kleine Anzahl von Personen geschickt.


[EXT] Angebotsanfrage

Timo Schrüfer <Zimmerei-Hoepfler@outlook.com>
An: Weber, Kristin

Montag, 26. Juni 2023 um 04:43

Meine Damen und Herren

Wir haben ein neues Projekt vor uns und bauen derzeit 13 Reihenmittelhäuser. Wir bitten um Angebote fur einige Ihrer von Ihrem Unternehmen verkauften Artikel gemaß den Vorgaben der Auftragnehmer

Dies sollte einen uberblick uber die finanzielle Großenordnung sowie verschiedene Optionen einschließlich aller anderen Prozesse geben.

Ich fuge die Höhenplane, aktuelle Fotos und Zeichnungen bei.

Wir wurden uns freuen, uns spater im nachsten Monat zu einem personlichen Treffen zu treffen.

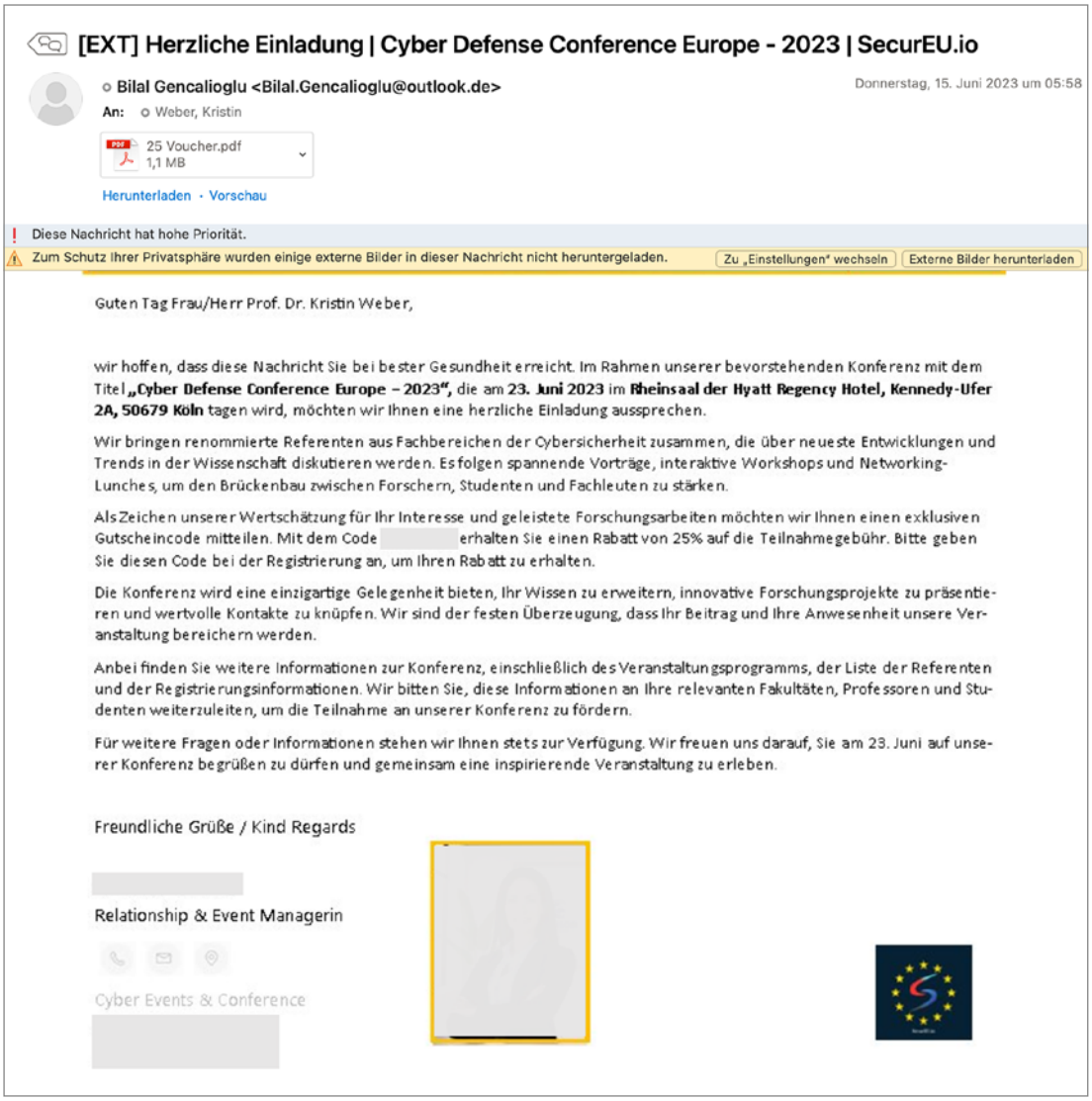
Mit freundlichen Grußen
Timo Schrüfer

Bild 3.4 Beispiel für einfache Phishing-Mail mit vielen Rechtschreibfehlern und falschem Kontext

Phishing-Nachrichten werden nicht nur klassisch per E-Mail, sondern auch über andere Kanäle verschickt, z. B. Social Media, Messenger-Dienste und SMS. Daneben gibt es Phishing auch per Telefon. Je nach Kanal und/oder verwendeter Strategie – eher breit angelegt oder eher gezielt – nimmt Phishing verschiedene Formen an, die im Folgenden kurz vorgestellt werden.

Spear Phishing & Whaling

Spear Phishing nimmt gezielt bestimmte Personen oder eine bestimmte Organisation ins Visier (vgl. das Beispiel im Kasten und in Abschnitt 3.1.2). Für die Vorbereitung eines solchen Angriffs ist intensives Information Gathering notwendig. Die Angreifenden nutzen in der Phishing-Nachricht dann die gefundenen Informationen, wie z. B. Anrede, Absendeadresse, Kontext, hierarchische Beziehungen, vermeintliche Insiderinformationen. Dadurch werden die Nachrichten deutlich glaubhafter und sind schwerer zu erkennen. Bild 3.5 zeigt eine Spear Phishing-Nachricht mit (fast) richtiger Anrede und mit der Einladung zu einer Cyber-Sicherheitskonferenz auch in passendem Kontext.



[EXT] Herzliche Einladung | Cyber Defense Conference Europe - 2023 | SecurEU.io

Bilal Gencalioglu <Bilal.Gencalioglu@outlook.de> Donnerstag, 15. Juni 2023 um 05:58

An: Weber, Kristin

25 Voucher.pdf
1,1 MB

Herunterladen · Vorschau

Diese Nachricht hat hohe Priorität.

Zum Schutz Ihrer Privatsphäre wurden einige externe Bilder in dieser Nachricht nicht heruntergeladen. Zu „Einstellungen" wechseln Externe Bilder herunterladen

Guten Tag Frau/Herr Prof. Dr. Kristin Weber,

wir hoffen, dass diese Nachricht Sie bei bester Gesundheit erreicht. Im Rahmen unserer bevorstehenden Konferenz mit dem Titel **„Cyber Defense Conference Europe – 2023"**, die am **23. Juni 2023** im **Rheinsaal der Hyatt Regency Hotel, Kennedy-Ufer 2A, 50679 Köln** tagen wird, möchten wir Ihnen eine herzliche Einladung aussprechen.

Wir bringen renommierte Referenten aus Fachbereichen der Cybersicherheit zusammen, die über neueste Entwicklungen und Trends in der Wissenschaft diskutieren werden. Es folgen spannende Vorträge, interaktive Workshops und Networking-Lunches, um den Brückenbau zwischen Forschern, Studenten und Fachleuten zu stärken.

Als Zeichen unserer Wertschätzung für Ihr Interesse und geleistete Forschungsarbeiten möchten wir Ihnen einen exklusiven Gutscheincode mitteilen. Mit dem Code erhalten Sie einen Rabatt von 25% auf die Teilnahmegebühr. Bitte geben Sie diesen Code bei der Registrierung an, um Ihren Rabatt zu erhalten.

Die Konferenz wird eine einzigartige Gelegenheit bieten, Ihr Wissen zu erweitern, innovative Forschungsprojekte zu präsentieren und wertvolle Kontakte zu knüpfen. Wir sind der festen Überzeugung, dass Ihr Beitrag und Ihre Anwesenheit unsere Veranstaltung bereichern werden.

Anbei finden Sie weitere Informationen zur Konferenz, einschließlich des Veranstaltungsprogramms, der Liste der Referenten und der Registrierungsinformationen. Wir bitten Sie, diese Informationen an Ihre relevanten Fakultäten, Professoren und Studenten weiterzuleiten, um die Teilnahme an unserer Konferenz zu fördern.

Für weitere Fragen oder Informationen stehen wir Ihnen stets zur Verfügung. Wir freuen uns darauf, Sie am 23. Juni auf unserer Konferenz begrüßen zu dürfen und gemeinsam eine inspirierende Veranstaltung zu erleben.

Freundliche Grüße / Kind Regards

Relationship & Event Managerin

Cyber Events & Conference

Bild 3.5 Beispiel für eine Spear Phishing-E-Mail

Noch plausibler wird Spear Phishing, wenn die Angreifenden Zugang zu einem gehackten Konto innerhalb der Organisation haben und die Nachrichten als Antworten auf frühere legitime Nachrichten versenden. Bei der Mail in Bild 3.5 handelt es sich vermutlich sogar um eine Original-E-Mail, die hier allerdings als Bild in die Nachricht eingefügt wurde.

Spear Phishing-Beispiel

Der (entlassene) Angreifer findet über Texte, Bilder oder Videos in Social Media heraus, dass zwischen den Mitarbeitenden des Zielunternehmens ein gewisser Unmut herrscht. Er sendet über Social-Media-Plattformen Nachrichten oder E-Mails mit eingebettetem Schadcode an ausgewählte Ziele. Er behauptet, es handele sich um einen Hoax-Virus, der anonym an jemanden weitergeleitet werden kann, den man nicht mag. Dieses Vorgehen kann eine große Gruppe von Personen in der Zielorganisation gefährden. (Wang et al., 2021)

Ein Spear Phishing-Angriff, der speziell auf hochrangige Ziele einer Organisation wie leitende Angestellte, CEO oder CFO abzielt, wird **Whaling** genannt (von Whale-Phishing). Die Angreifenden gestalten beim Whaling E-Mails und Webseiten sehr individuell und personalisiert, indem sie den Namen der Zielperson, die Berufsbezeichnung, den Verantwortungsbereich, interne Telefonnummern, Logos, den E-Mail-Footer und andere richtige Informationen einbauen. Der Angriff ist in der Regel kontextabhängig, z. B. „... für die in Ihrem Terminkalender vorgesehene xxx-Geschäftsbesprechung müssen Sie sich anmelden und die Anmeldung mit der beigefügten Software bestätigen“. (Wang et al., 2021)

CEO Fraud

Beim CEO Fraud (auch Business E-Mail Compromise/Fake-President-Betrug) erhalten gezielt ausgewählte Mitarbeitende aus der Finanzabteilung eine E-Mail. Vermeintlich stammt diese Mail von einer hochrangigen Führungsperson. Die Nachricht fordert sie dazu auf, einen hohen Geldbetrag auf ein (angebliches) Bankkonto des Unternehmens, das sich typischerweise im Ausland befindet, zu überweisen. Aufgrund vorheriger Informationsbeschaffung sieht die Nachricht tatsächlich aus, als stamme sie von der Geschäftsleitung. Wird die darin enthaltene Anweisung ausgeführt, ist das Geld weg.

Mittels CEO Fraud können auch geheime Informationen angefordert werden (vgl. Beispiel im Kasten).

CEO Fraud per SMS

Der Angreifer blockiert das Handysignal der Ziel-CEO und sendet eine SMS-Nachricht an ihre Assistenz, indem er die Telefonnummer der CEO fälscht: „Ich bin in einer Besprechung in einer anderen Stadt und kann nicht telefonieren. Verschlüsseln Sie die Organisationsstrukturtabelle und eine Vertragsdatei zu einem Zip mit dem Schlüssel *** und senden Sie es sofort an xxx@xxx.xxx! Sonst geht uns ein wichtiges Geschäft durch die Lappen.“ (Wang et al., 2021)

Smishing & Social Media Phishing & Vishing

Immer häufiger werden Kurznachrichten auf Mobilgeräten für Angriffe von Social Engineers genutzt. Die sogenannten Smishing-Nachrichten (kurz für SMS-Phishing) sollen die Empfangenden zum Aufrufen eines schädlichen Links bewegen. Die Nachrichten verwenden oft Köder wie beispielsweise eine Sendungsverfolgung für ein bestelltes Paket oder ein Sonderangebot (vgl. Bild 3.6).

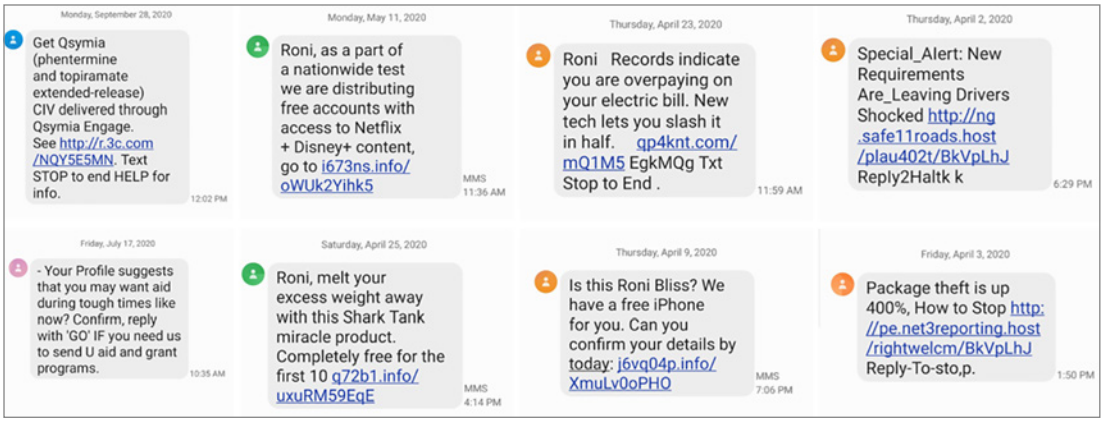


Bild 3.6 Beispiele für Smishing-Nachrichten (Crane, 2020)

Beim Öffnen der Links werden die Opfer aufgefordert, ein Sicherheitsupdate oder eine App herunterzuladen. In Wirklichkeit wird allerdings diverse Schadsoftware auf dem Smartphone installiert. Neben der Infektion des Geräts ist es häufig das Ziel des Angriffs, persönliche Daten zu stehlen. Hierfür werden die Opfer auf eine scheinbar legitime Internetseite weitergeleitet, auf der persönliche Angaben (z. B. Handynummer, Anschrift, Kontodaten) gemacht werden sollen.

Social-Media-Plattformen erleichtern Social Engineers die Arbeit erheblich. Viele User geben wissentlich oder unwissentlich persönliche Informationen auf Social Media weiter. Beim Social Media Phishing verwenden Angreifende Social-Media-Webseiten wie Facebook, Twitter und Instagram anstelle von E-Mails, um an persönliche Daten zu gelangen oder die User dazu zu bewegen, auf bösartige Links zu klicken (Chanti & Chithralekha, 2022, S. 454). Social Engineering in sozialen Medien kann auf folgende Weise erfolgen: durch verdächtige URLs oder Anhänge, über ein Bot-Konto, ein kompromittiertes Konto oder ein Spam-Konto.

Beim **Vishing** (von Phone Phishing) werden Social Engineering-Techniken eingesetzt, um per Telefon unbefugten Zugriff auf Daten zu erhalten (Chanti & Chithralekha, 2022, S. 454). Die Angreifenden nutzen Techniken wie Voice-over-IP, Spoofing der Anrufer-ID oder Interactive Voice Response, um das Opfer anzurufen. Die anrufende Person gibt sich als vertrauenswürdig aus, um persönliche Daten des Opfers zu erfragen, z. B. Kontonummern oder Log-in-Daten. Zwei Beispiele von Vishing finden sich im Kasten.

Die Angreiferin gibt sich als neue Mitarbeiterin aus und überzeugt die Zielperson davon, einer Bitte nachzukommen. Sie bittet z. B. den technischen Support (Paul), das Passwort ihres Kontos zurückzusetzen, damit sie eine sehr dringende Aufgabe erledigen kann, und bittet außerdem um einen VPN-Zugang von außen.

Die Angreiferin ruft einen Mitarbeiter des technischen Supports an, um ihm zu sagen, dass die CEO ihr erlaubt hat, einen VPN-Kanal für eine dringende virtuelle Projektpräsentation anzufordern, und erzählt ihm weiter, dass ein anderer Mitarbeiter (Paul) ihr früher bereits geholfen haben. (Wang et al., 2021)

3.2.2 Watering Hole Attack

Ein Watering Hole-Angriff ist ein einfacher, aber sehr erfolgreicher Social Engineering-Angriff. Der Name leitet sich vom Wasserloch ab, welches die Tiere der Savanne oder Wüste am Morgen aufsuchen, um Wasser zu trinken. Tierische Jäger warten dort gezielt auf die in großen Gruppen auftauchenden Tiere und haben unter ihren potenziellen Opfern quasi freie Auswahl.

Die Opfer eines Watering Hole-Angriffs sind meist bestimmte Gruppen mit ähnlichem Surfverhalten, wie Unternehmen, Branchen oder Regionen. Die Angreifenden ermitteln, welche Webseiten die Zielpersonen regelmäßig besuchen oder besuchen werden. Sie infizieren diese Webseiten dann mit bösartigem Code. Die Ziele werden kompromittiert, wenn sie die Webseite aufrufen, Software (Malware) herunterladen oder auf (bösartige) Links klicken.

Beispielsweise stellen die Angreifenden eine Software über eine Webseite zur Verfügung und geben vor, dass die Software das kostenlose Herunterladen und Anschauen von Pornobildern oder -videos ermöglicht (Wang et al., 2021). Sobald die Zielpersonen die Software installiert haben, ist ihr Computer kompromittiert.

Ein Hacker (oder eine Hacking-Organisation) namens **Harioboy** griff Hunderttausende von Privatrechnern an, indem er einen Watering Hole-Angriff durchführte (Zheng et al., 2019).

Harioboy stellte Anleitungsvideos auf Video-Webseiten (z. B. YouTube), die erklärten, wie man mit einem Hacker-Tool RC7 und Discord knackt. Das Tool, welches Schadcode enthielt, stellte er kostenlos zum Download bereit. Einige Gamer, Hacker und Cracker fanden die Videos und das Tool über Suchmaschinen. Sie luden das Tool herunter. Sobald das Hacker-Tool auf dem Computer des Opfers ausgeführt wurde, führte es den eingebetteten Schadcode von Harioboy aus und lud einen Trojaner herunter. Harioboy nutzte den Trojaner dann, um die Computer der Opfer zu überwachen, zu kontrollieren und sensible Daten wie Bankdaten, Spielkonten oder Bitcoins zu stehlen.

3.2.3 Impersonating/Pretexting

Social Engineers, die ihre Opfer vor Ort besuchen und mit ihnen direkt von Angesicht zu Angesicht interagieren, nutzen häufig die Technik Impersonating. Die angreifende Person gibt dabei vor, jemand anderes zu sein, und nutzt dazu eine passende Verkleidung. Beispielsweise gibt sich eine kriminelle Person als jemand aus, der die Identität des Opfers prüft. Unter dem Vorwand, sie benötige für die Überprüfung weitere persönliche Informationen, nennt das Opfer ihm diese (Bishnoi et al., 2023).

Allen (2006) zeigt zwei weitere typische Beispiele (vgl. auch Beispiel im Kasten):

- Der Angreifer gibt vor, ein Mitglied des Führungskreises mit einem wichtigen Termin zu sein. Er setzt die Mitarbeitenden im Helpdesk unter Druck, hilfreiche Informationen preiszugeben, wie z. B. die Art der verwendeten Fernzugriffssoftware, deren Konfigurationsmöglichkeiten, die zu wählenden Telefonnummern des Fernzugriffsservers und die Anmeldedaten für den Server. Mit diesen Informationen kann der Angreifer dann den Fernzugriff auf das Netz des Unternehmens einrichten. Er kann später anrufen, um zu erklären, dass er sein Passwort vergessen hat, und darum bitten, dass es zurückgesetzt wird.
- Die Angreiferin kann sich beispielsweise als IT-Administratorin ausgeben, die versucht, dem Benutzer bei einem Problem zu helfen. Dazu benötigt sie die Log-in-Daten inklusive Passwort des Benutzers, welches sie durch eine passende Geschichte und entsprechendes Auftreten eher erhält. Oder sie kann ihn überzeugen, eine als nützliches Tool getarnte Schadsoftware zu installieren.

Impersonating

Beispiel für die Anwendung der Social Engineering-Ontologie (vgl. Tabelle 3.1)

Der Social Engineer gibt vor, Teil der Organisation zu sein, kleidet sich entsprechend und schleicht sich dann hinter anderen Mitarbeitenden in das Gebäude. Im Gebäude versucht er, Zugang zu einem Computerterminal zu erhalten. Hat der Angreifer Zugang, installiert er eine Hintertür auf dem Computerterminal, über die er sich künftig von außen Zugang verschaffen kann. (Mouton et al., 2016, S. 190)

Tabelle 3.1 Merkmale des Social Engineering-Angriffs „Impersonating“

Communication Model and Medium Bidirektional, von Angesicht zu Angesicht	**Technik** Impersonating, Pretexting
Ziel/Opfer Das Ziel des Angriffs ist es, unbefugten Zugang zu einem Computerterminal innerhalb der Organisation zu erhalten.	
Social Engineer Einzelperson	
Compliance Principles Authority; Liking, Similarity & Deception; Commitment, Reciprocation & Consistency	

In der ersten Hype-Phase von Kryptowährungen (2017/2018) kam es zu einigen sehr erfolgreichen Social Engineering-Angriffen, die zu Verlusten in Millionenhöhe führten. So reagierten beispielsweise im November 2017 mehrere potenzielle Kaufende des Red Pulse-Tokens auf über Twitter-Konten verbreitete Fake News und gaben ihre Zugangsdaten auf einer Phishing-Website ein. Die verlorenen Token hatten einen Wert von mehr als 3 Millionen US-Dollar. Für viele User war die Blockchain-Technologie noch neu und das Verständnis für ihre Funktionsweise und vor allem ihre Sicherheitsmechanismen gering (Krombholz et al., 2017). Die User wollten die Technologie ausprobieren oder wurden angelockt von schnellen und hohen Gewinnen. In (Weber et al., 2020) haben wir fünf dieser Angriffe auf Basis der Ontologie von (Mouton et al., 2014) analysiert. Ein Beispiel, in dem Pretexting verwendet wurde, findet sich im Kasten.

Falsche Twitter-Konten (Morse, 2018)

Twitter (heutiger Name „X“) ist eine beliebte Social-Media-Plattform innerhalb der Kryptowährungs-Community, wenn es um die Bekanntgabe von Neuigkeiten und den Austausch von Ideen geht. Alle wichtigen Blockchain-Akteure haben ein Twitter-Konto. Anfang 2018 kopierten die Betrügenden das Konto des berühmten Unternehmers und Investors Elon Musk, indem sie „Elon Musk“ als Anzeigename wählten und sein Profilbild verwendeten. Als Benutzungsnamen wählten sie „@elonlmusk“, ähnlich dem eigentlichen Namen „@elonmusk“. Die Betrügenden erlangten die Aufmerksamkeit der Twitter-Nutzenden, indem sie einen Beitrag des ursprünglichen Elon Musk kommentierten. In ihrem Kommentar gaben sie an, dass sie 5.000 ETH an Elons Follower verschenken. Um teilzunehmen, sollten die Follower 0,5 bis 1 ETH an seine Adresse schicken und würden 5 bis 10 ETH zurückbekommen. Die Betrügenden nutzten auch andere gefälschte Konten, um das Angebot scheinbar zu bestätigen. Sie kommentierten über die Konten, dass sie die angebotenen ETH erhalten hätten. Mehrere Follower überwiesen einen Teil ihrer ETH an die gefälschten Adressen. Die Betrügenden erhielten 172,57 ETH aus 282 verschiedenen Wallets. Diese Betrugsmasche wurde danach vielfach angewandt mit unberechenbaren Folgen.

Tabelle 3.2 beschreibt die Merkmale dieses Angriffs gemäß dem ontologischen Modell.

Tabelle 3.2 Merkmale des Social Engineering-Angriffs „Falsche Twitter-Konten“

Communication Model and Medium Indirekte Kommunikation via Twitter	**Technik** Pretexting
Ziel/Opfer User mit Interesse an Kryptowährungen, die einer Blockchain-Berühmtheit auf Twitter folgen	
Social Engineer unbekannt; jeder könnte ein gefälschtes Konto einrichten, um sich als prominente Person auszugeben, und den richtigen Moment abwarten, um einen Twitter-Beitrag zu kommentieren	
Compliance Principles Authority; Social Proof; Liking, Similarity & Deception; Commitment, Reciprocation & Consistency; Distraction	

3.2.4 Reverse Social Engineering

Beim Reverse Social Engineering wird das Opfer dazu verleitet, von sich aus Kontakt mit den Angreifenden aufzunehmen. Die Social Engineers bieten beispielsweise Unterstützung bei der Behebung eines Problems an, die das Opfer dankbar annimmt. Die Support-Funktion gibt den Social Engineers einen scheinbar legitimen Grund, dem Opfer alle möglichen Fragen zu stellen. Diese Art von Angriff ist besonders glaubhaft, weil das Opfer kaum Anlass hat, an der Legitimität der Angreifenden zu zweifeln, da es selbst den Kontakt gesucht hat (Bishnoi et al., 2023). Ebenfalls wird ein psychologischer Trick namens **Quidproquo** ausgenutzt (vgl. Abschnitt 3.3.5). Die Angreifenden bieten ihre Hilfe an, und die Opfer fühlen sich verpflichtet, eine Gegenleistung anzubieten. In diesem Fall sind es sensible Informationen (s. auch Beispiel im Kasten).

Ein typischer Reverse Social Engineering-Angriff läuft in drei Schritten ab (Allen, 2006), wobei die Reihenfolge der Schritte 1 und 2 abweichen kann. Zunächst bieten die Social Engineers ihre Hilfe an, falls es zu Problemen kommen sollte. Das tun sie z. B., indem sie ihre Visitenkarte beim Opfer hinterlassen oder ihre Kontaktdaten in der Fehlermeldung angeben. Dann verursachen sie absichtlich die bereits angekündigten Probleme, indem sie beispielsweise den Anschein erwecken, dass ein System beschädigt ist und nicht richtig funktioniert. Das Opfer entdeckt das Problem. Im letzten Schritt meldet sich das Opfer bei den Social Engineers, die dann bei der Behebung des vermeintlichen Problems helfen. Dabei installieren sie eine Schadsoftware auf dem Rechner des Opfers oder erfragen vertrauliche Informationen. Ein konkretes Beispiel beschreibt der folgende Kasten.

Beispiel für einen Reverse Social Engineering-Angriff

Die Angreiferin sendet eine E-Mail mit einer gefälschten Adresse vom IT-Support an einen neuen Mitarbeiter. Die E-Mail informiert ihn darüber, dass „in Kürze ein Netzwerktest durchgeführt wird und er sich bei einem Netzausfall bitte an xxx wenden soll“. Die Angreiferin verursacht nun eine Netzwerkstörung und wartet auf die Anfrage des neuen Mitarbeiters. Nachdem sie dem Opfer geholfen hat, das Problem zu beheben, entwickelt sich folgender Dialog:

„Würden Sie uns einen Gefallen tun, nur eine Minute, und eine Umfrage ausfüllen, die für die Entwicklung eines Schulungsprogramms zur Security Awareness für neue Mitarbeitende verwendet wird? Fast 80 % der Mitarbeitenden haben dies bereits getan.“

„Okay, mit Vergnügen.“

„Sind Sie eigentlich mit unseren E-Mail-Richtlinien vertraut? … Es kann gefährlich sein, unaufgeforderte Anhänge zu öffnen … Wir müssen Ihr Passwort wissen, um die Security Awareness neuer Mitarbeitender zu bewerten. Es ist eine Angelegenheit der Unternehmenssicherheit.“

„Okay, es ist …“ (Wang et al., 2021)

Nach einem ähnlichen Prinzip funktioniert **Scareware**. Den Nutzenden wird beim Surfen im Internet suggeriert, dass ein Problem mit ihren Computern besteht, beispielsweise eine

Schadsoftware-Infektion oder eine Fehlfunktion des Betriebssystems. Oder es wird mit einem wichtigen Sicherheits-Update geworben. Vertrauen die Anwendenden diesen Meldungen, installieren sie die angebotene Software und infizieren dadurch selbst das System mit einer Schadsoftware.

3.3 Menschen manipulieren

„In general, it is difficult for people to recognize a lie. ... humans are predisposed to trust others."

(Bullée & Junger, 2019, S. 13)

Gute Social Engineers sind – ob es ihnen bewusst ist oder nicht – Spezialist:innen in Psychologie. Sie verstehen, wie Menschen „funktionieren", und sind in der Lage, sie zu ihren Gunsten zu beeinflussen.

Menschen zeigen typische Verhaltensweisen, die sich im Laufe der Evolution als vorteilhaft herausgebildet haben und die in der Vergangenheit das Überleben der Menschheit sicherten. Dazu gehört, dass Menschen Autoritätspersonen fast blind vertrauen und deren Entscheidungen nicht hinterfragen. Social Engineers nutzen diese antrainierten Verhaltensweisen gezielt aus. Die Opfer bemerken diese Manipulation meist nicht und haben während und nach der Manipulation auch kein schlechtes Gefühl dabei.

Der folgende Abschnitt beschreibt fünf typische „Compliance Principles" oder psychologische Tricks, die Social Engineers bei ihren Angriffen einsetzen. Zuvor wird noch kurz erklärt, warum diese Prinzipien so gut funktionieren.

3.3.1 Thinking, Fast and Slow

Cialdini (2007) erklärt am Anfang seines Buches „Influence", warum wir Menschen so leicht zu manipulieren sind, anhand eines Experiments (in sehr anschaulicher und humorvoller Form auch von Brushwood (2011) präsentiert). In dem Experiment wurde untersucht, wie hilfsbereit Personen sind, wenn sie um einen Gefallen gebeten werden. Wesentliches Ergebnis: Wenn die bittende Person einen Grund nennen kann, warum sie den Gefallen benötigt, lag die Hilfsbereitschaft bei fast 100 %. Erstaunlich war, dass es egal war, was für einen Grund die bittende Person nannte. Auch wenn dieser Grund völliger Nonsens war, wurde ihrer Bitte stattgegeben. Als Erklärung gab die Autorin des Experiments an, dass es nur auf das Wörtchen „weil" ankommt und nicht auf den konkret danach genannten Grund. Sie erklärt, dass „weil" eine Art Trigger ist, der ein vorbestimmtes Muster – hilfsbereites Verhalten – auslöst.

Von diesen Triggern, die bei Menschen ein bestimmtes Verhalten auslösen, gibt es einige. Sie haben sich im Laufe der Evolution gebildet, weil sie sich in unserer Historie als vorteilhaft erwiesen haben und z. B. das soziale Miteinander regeln und dadurch erleichtern. Auch heute

noch reagieren wir in bestimmten Situationen ganz automatisch. Beispielsweise erwidern wir gerne Gefallen oder sind eben hilfsbereit. Diese Trigger sind also grundsätzlich etwas Gutes.

Social Engineers nutzen die typischen menschlichen Verhaltensmuster jedoch als Schwachstellen aus, neben dem Wunsch, zu helfen, auch die Tendenz, anderen Menschen zu vertrauen, und die Angst, in Schwierigkeiten zu geraten. In ihrer Studie, in der untersucht wurde, ob Personen USB-Sticks, die sie finden, wirklich in ihre Computer einstecken, fanden Tischer et al. (2016) heraus, dass mindestens 45 % der von ihnen „verlorenen" USB-Sticks tatsächlich benutzt worden waren. Die Opfer gaben zwei Gründe an: die altruistische Absicht, den USB-Stick der besitzenden Person zurückzugeben, und Neugierde.

Nobelpreisträger Kahnemann (2011) erklärt dieses automatische Verhalten damit, dass wir in zwei verschiedenen Systemen denken. System 1 arbeitet automatisch und schnell, weitgehend mühelos und ohne willentliche Steuerung („thinking fast"). System 2 lenkt die Aufmerksamkeit auf die anstrengenden mentalen Aktivitäten, die auf bewusstes Denken angewiesen sind, z. B. komplexe Berechnungen („thinking slow"). Der Großteil unseres Denkens findet in System 1 statt. Alles andere wäre zu anstrengend. Beispiele sind das Wahrnehmen von Größenunterschieden, einfache Berechnungen wie 1 + 1 oder das Lesen einer Werbebotschaft. In System 2 hingegen konzentrieren wir uns nicht nur, wir können auch bewusst (und frei) entscheiden.

Social Engineers versuchen, Menschen zu manipulieren, indem sie die bestimmten Trigger setzen und damit automatische Handlungen und Reaktionen auslösen. Sie verknüpfen ihre Botschaft mit fest verankerten menschlichen Beweggründen und nutzen damit das System 1 aus. Die Opfer können nicht willentlich entscheiden und denken nicht rational. Gegen Social Engineering-Angriffe hilft demnach bereits, zu wissen, dass es diese Trigger gibt, und deren gezielten Einsatz durch Social Engineers zu erkennen. Wird der Manipulationsversuch erkannt, wird System 2 eingeschaltet und hilft beim besonnenen Reagieren.

Im Folgenden sollen fünf dieser psychologischen Prinzipien näher vorgestellt werden: Autorität (Authority), Soziale Bewährtheit (Social Proof), Sympathie, Ähnlichkeit und Täuschung (Liking, Similarity & Deception), Verpflichtung, Gegenseitigkeit & Konsistenz (Commitment, Reciprocation & Consistency) sowie Ablenkung (Distraction). Die Auswahl der Prinzipien basiert auf (Cialdini, 2007; Ferreira et al., 2015; Stajano & Wilson, 2011; Weber et al., 2020).

3.3.2 Autorität

Das Prinzip Autorität ist einfach: Menschen folgen Anweisungen von Autoritäten und stellen diese nicht infrage. Als Autoritätspersonen gelten bestimmte Personengruppen wie z. B. Lehrer:innen, Eltern, Polizist:innen, Ärzt:innen, Richter:innen, prominente Persönlichkeiten oder Führungskräfte. Das Prinzip ist in allen hierarchischen Beziehungen sichtbar. Autorität kann bei Personen aber auch durch Titel, Kleidung (vor allem Uniformen) oder Statussymbole wie teure Autos und Uhren ausgedrückt werden. In Werbung für Gesundheitsprodukte werden beispielsweise gerne Doktor:innen oder Professor:innen gezeigt – mit Namensschildern, die sie als „Prof. Dr. XXX" benennen. Gewisse Institutionen werden auch als Autorität gesehen, wie Regierungsinstitutionen, Kirchen, Banken, Fernsehsender, aber auch bekannte Unternehmen wie Apple, Amazon etc. Bei Institutionen kann Autorität z. B. auch durch wichtig aussehende Logos oder Zertifikate hergestellt werden.

Autorität kann also leicht gefälscht werden, indem die Symbole für Autorität verwendet werden. In einem Experiment beobachteten Forschende das Verhalten von wartenden Personen an einer Ampelkreuzung (zitiert in Cialdini, 2007, S. 227). Sie ließen einen Mann mehrfach bei Rot die Ampel überqueren. In der Hälfte der Fälle trug er dabei normale Straßenkleidung (T-Shirt und Hose). Bei den anderen Fällen war er sehr ordentlich mit Anzug und Krawatte gekleidet. Wenn der Mann einen Anzug trug, liefen mehr als dreimal so viele Personen hinter ihm bei Rot über die Straße als in den Fällen, in denen er normal gekleidet war. Die gleiche Person wurde also durch den Anzug als Autorität wahrgenommen und ihr wurde gefolgt, obwohl sie eine Ordnungswidrigkeit beging.

Auch durch „Name Dropping" kann Autorität hergestellt werden. Eine Person gibt vor, eine andere Autoritätsperson (z. B. eine prominente Person) gut zu kennen, und wird dadurch selbst auch als Autorität wahrgenommen. Damit das Prinzip Autorität funktioniert, reicht es, dass die Opfer glauben, dass es sich bei der anfragenden Person oder Institution um eine Autorität handelt.

Im Social Engineering wird dieses Prinzip auf verschiedene Arten ausgenutzt (vgl. Tabelle 3.3). Ganz deutlich ist es beim CEO Fraud. Die Angestellten in der Finanzabteilung bekommen vermeintlich von einem hochrangigen Mitglied des Führungskreises (= Autorität) eine E-Mail und sollen eine hohe Summe Geld überweisen. Das Prinzip besagt, dass sie die Anweisung nicht hinterfragen, sondern das Geld überweisen. Eine Anfrage von ganz oben hat mehr Aussicht auf Erfolg, weshalb sich Social Engineers als Pretext gerne eine Führungskraft aussuchen. Informationsanfragen, die von oben und nicht von unten kommen, erregen weniger Aufsehen.

Tabelle 3.3 Zusammenfassung des Prinzips „Autorität"

Prinzip	Menschen sind darauf trainiert, Autoritäten nicht zu hinterfragen. In der Regel folgen sie den Aufforderungen oder Befehlen von jemandem, den sie für eine Autorität halten.
Techniken/Instrumente	Titel, Logos, Namedropping, Kleidung (Uniformen), Statussymbole
Anwendung	CEO Fraud, (Spear) Phishing, Pretext/Impersonating, Vishing

Auch Phishing-E-Mails, in denen die Adressierten von ihrer Bank aufgefordert werden, zur Legitimationsprüfung auf einer Webseite ihre Log-in-Daten einzugeben, nutzen dieses Prinzip (vgl. Bild 3.7). In Phishing-Mails ist Autorität das am meisten genutzte Prinzip von allen (Ferreira et al., 2015). Hierin wird Autorität auch häufig durch die Art und Weise der Ansprache der Opfer hergestellt, indem die Imperativform in Aufforderungen oder Befehlen verwendet wird.

Bei Anwendung des Autoritätsprinzips ist es weniger wahrscheinlich, dass die Opfer die Gültigkeit einer Anfrage (oder eines Angebots) infrage stellen. Einen starken Effekt zeigte das Autoritätsprinzip bei dem Beispiel mit den gefälschten Twitter-Konten (vgl. Abschnitt 3.2.3). Die Kriminellen kopierten den Online-Auftritt und den Namen des Prominenten Elon Musk und boten der Community in seinem Namen kostenlose Token an. Die Nachahmung eines Prominenten ließ die Kriminellen vertrauenswürdig erscheinen, wodurch die Wahrscheinlichkeit groß war, dass ihre Opfer dem Angebot folgen und auf den Trick hereinfallen würden.

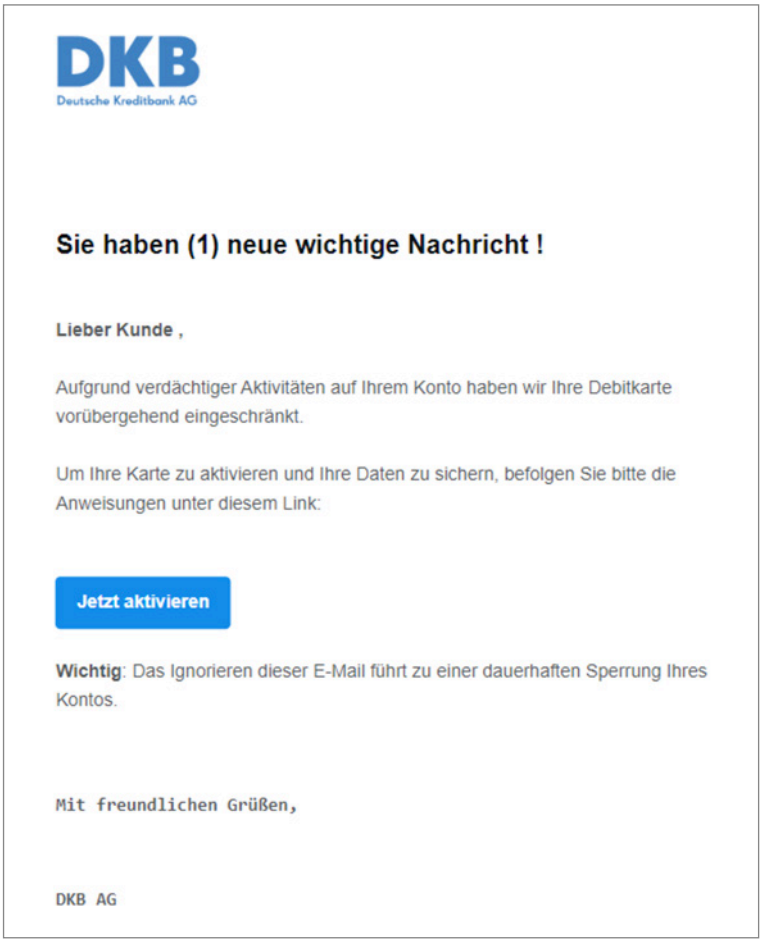


Bild 3.7 Phishing-Nachricht von einer Bank

3.3.3 Soziale Bewährtheit

Besonders in unbekannten Situationen tendieren Menschen dazu, das Verhalten von anderen zu imitieren. Auf diese Weise reduzieren sie das Risiko, durch unangemessenes Verhalten (unangenehm) aufzufallen. Zudem fühlen sie sich so nicht allein verantwortlich für ihre Taten. Sie tun nur das, was die anderen auch tun.

Im Alltag kann man dieses Prinzip vielerorts beobachten. In ein leeres Geschäft oder in ein leeres Restaurant geht niemand gern als Erste/r hinein. In Restaurants, wo schon fast alle Tische besetzt sind, muss das Essen gut sein. Auch wenn irgendwo eine Schlange ist, stellen wir uns an – da muss es doch etwas Gutes geben. In Cafés liegen im Glas für das Trinkgeld immer schon ein paar Münzen drin. Die Mützen oder Gitarrenkoffer von Straßenmusizierenden sind auch nie leer. Dies suggeriert, dass schon anderen die Musik gefallen hat und sie etwas Geld gegeben haben. Somit steigt die Wahrscheinlichkeit, dass weitere Vorübergehende

ebenfalls spenden werden. Auch das künstliche Lachen in Comedyserien funktioniert. Obwohl alle wissen, dass die Lacher nur eingespielt werden, um die Zuschauenden zum Lachen zu animieren, werden Serien mit Lachkonserven als lustiger empfunden und führen dazu, dass die Zuschauenden tatsächlich mehr lachen (Cialdini, 2007, S. 114 f.).

Das folgende kleine Experiment kann jede/r selbst ausprobieren. In einer Gruppe von mindestens zwei Personen bleibt man z. B. in einer belebten Fußgängerzone stehen und schaut nach oben. Sofort werden andere ebenfalls stehen bleiben und dem Blick folgen.

Es gibt auch sehr negative Konsequenzen von sozialer Bewährtheit. In dem Moment, in dem sich viele Menschen eigentlich falsch verhalten, trauen sich andere nicht, richtig zu handeln. Beispielsweise bei unterlassener Hilfeleistung lässt sich dieses Phänomen immer wieder beobachten. Viele Personen beobachten ein Verbrechen oder einen Unfall, aber keiner unternimmt etwas. Auch die Personen nicht, die sich vielleicht trauen würden, dazwischenzugehen, tun es nicht, weil alle anderen nur herumstehen oder vorbeifahren. Sie würden aus der Masse herausstechen und auffallen, oder sie sind sich nicht mehr sicher, ob sie wirklich ein Verbrechen beobachten. Denn sonst würde doch jemand anderes auch eingreifen. Tailgating funktioniert u. a. nach diesem Prinzip. Da niemand die unbekannte Person anspricht, kann sie in das Gebäude problemlos eindringen, selbst wenn sie einigen Angestellten auffällt. Solange niemand den ersten Schritt tut und sich traut, etwas anderes als die Masse zu tun, bleibt die Person unbehelligt.

Soziale Bewährtheit (englisch Social Proof) zeigt sich nicht nur im Verhalten, sondern auch im Aussehen. Auf der Arbeit, in Schulen und Hochschulen, in einem Konzert o. Ä. imitieren sich die Anwesenden gegenseitig und tragen ähnliche Kleidung, Frisuren, Schmuck etc. Es fällt Menschen sehr schwer, dieser Erwartung oder diesem Druck zu widerstehen und beispielsweise als einzige Person jeden Tag im Anzug mit Krawatte zur Arbeit zu erscheinen, wenn alle anderen eher leger gekleidet sind.

In der Online-Welt gibt es viele Möglichkeiten, Social Proof herzustellen. Ratings, Empfehlungen, Likes, Follower, Ranglisten oder Rezensionen zeigen, dass etwas gut ist oder eben nicht, weil andere es als gut oder nicht gut empfunden haben. Aufgrund der Vielzahl an vergleichbaren Produkten, Urlaubszielen, Dienstleistungen oder Angeboten entscheiden sich viele für das, was andere auch gekauft haben.

Social Engineers nutzen soziale Bewährtheit, z. B. beim Phishing, insbesondere Social Media Phishing, um ihre Opfer von der Legitimität ihrer Anfrage zu überzeugen (vgl. Tabelle 3.4). Sie tun so, als ob bereits viele andere Personen, vor allem Freunde oder Kollegen, ihrem Anliegen bereits gefolgt sind. Beim Vishing-Beispiel in Abschnitt 3.2.1 erklärt die Angreiferin den Mitarbeitenden im IT-Support, dass ein Kollege von ihnen – Paul – ihr bereits früher geholfen hat. Dies lässt ihr Anliegen rechtmäßig erscheinen.

Tabelle 3.4 Zusammenfassung des Prinzips „Soziale Bewährtheit“

Prinzip	Menschen neigen dazu, sich so wie andere zu verhalten
Techniken/Instrumente	(gefälschte) Referenzen, Ratings, Empfehlungen, Social-Media-Profile
Anwendung	(Social Media) Phishing, Onlineshopping-Betrug, Pretext/Impersonating, Information Gathering, Tailgating

Oder Social Engineers nutzen soziale Bewährtheit, um Druck aufzubauen. Sie wissen, dass niemand gerne unangenehm auffallen möchte, und ermutigen ihre Opfer, „mit der Herde mitzugehen“. Mit einer Aussage wie „Alle anderen haben das Update schon installiert – Sie sind einer der Letzten, die noch die alte, unsichere Version nutzen, also handeln Sie noch heute.“ setzen sie sie zudem unter Zeitdruck (vgl. Abschnitt 3.3.6).

Der Betrug mit gefälschten Twitter-Konten nutzt ebenfalls das Prinzip Social Proof (vgl. Abschnitt 3.2.3). Die Social Engineers haben nicht nur das Konto von Elon Musk gefälscht, sondern auch weitere Twitter-Konten erstellt. Diese gefälschten Twitter-Konten reagierten auf das Angebot und „bestätigten“, dass sie tatsächlich einige der versprochenen kostenlosen Token erhalten haben. Nach dem Social Proof-Prinzip überzeugt dieser Trick einige bis dahin unsichere Follower. Sie imitierten das Verhalten der gefälschten Follower und überwiesen ihre ETH an die gefälschte Adresse.

3.3.4 Sympathie, Ähnlichkeit und Täuschung

Menschen gewähren Bitten, die von Bekannten und Freund:innen kommen, bereitwilliger als Bitten von fremden Personen. Wenn Annika die Mail mit der Einladung zur Faschingsparty nicht direkt vom Verein, sondern von einer angeblichen Freundin bekommen hätte, wäre die Aussicht auf Erfolg der Phishing-Mail vermutlich sogar noch höher gewesen (vgl. Beispiel in Kapitel 1).

Das Prinzip von Sympathie, Ähnlichkeit und Täuschung funktioniert aber auch, wenn die bittstellende Person den Opfern sympathisch, attraktiv oder ähnlich ist. Am Anfang des Kapitels wurde das Experiment erwähnt, in welchem Personen um einen Gefallen gebeten wurden und die Hilfsbereitschaft bei fast 100 % lag. In diesem Experiment war die Bittstellerin den Personen zwar unbekannt, aber sie wirkte sehr attraktiv auf viele Beteiligte.

Vor allem Ähnlichkeit lässt sich sehr schnell und bewusst herstellen. Es reichen oft kleine Gemeinsamkeiten, wie ein Lieblings-Urlaubsziel, das gleiche Hobby, ähnliche Interessen und der Geburts- oder Studienort, den man mit der anderen Person teilt. Auch ein bewusst gewählter Kleidungsstil kann Ähnlichkeit suggerieren. Sympathisch wird man anderen Personen eventuell schon, wenn man sie offen anlächelt, ihnen Komplimente macht, einen kleinen Gefallen tut oder versucht, attraktiv auf sie zu wirken.

Social Engineers versuchen, ihre Opfer so zu manipulieren, dass sie sie mögen und sich bei ihnen wohlfühlen (vgl. Tabelle 3.5). So ist es sehr viel wahrscheinlicher, dass sie mit ihren Forderungen erfolgreich sind. Im Fall der gefälschten Twitter-Konten folgen die Opfer dem berühmten Elon Musk, weil sie ihn wahrscheinlich mögen oder respektieren. Als sie die Chance bekamen, von ihrem Idol kostenlose Token zu erhalten, haben sie diese genutzt.

Tabelle 3.5 Zusammenfassung des Prinzips „Sympathie, Ähnlichkeit und Täuschung“

Prinzip	Menschen kommen Bitten von Bekannten eher nach.
Techniken/Instrumente	Komplimente, gemeinsame Interessen
Anwendung	Spear Phishing, Tailgating, Vishing, Information Gathering, um kleine Gefallen bitten

Ein Social Engineer kann ein Gespräch damit beginnen, dass er auf derselben Konferenz, demselben Musikkonzert oder demselben Restaurant wie seine Zielperson war. Derartige Anknüpfungspunkte sind über die vorherige Informationsrecherche z. B. in sozialen Netzwerken leicht herauszufinden. Die Informationen werden auch bei der Erstellung eines Pretexts entsprechend berücksichtigt. Vor allem in der Phase „Establish Relationship and Rapport" ist bei einigen Social Engineering-Angriffen entscheidend, dass die Angreifenden durch das Opfer als sympathisch und vertrauenswürdig wahrgenommen werden.

> *Astrid stellt sich in der Zigaretten- und Kaffeepause zu den anderen Angestellten. Sie tut so, als ob sie ebenfalls Beraterin für das Unternehmen ist, und beginnt ein Gespräch. Indem sie vermeintliche Insiderinformationen einflicht und über den furchtbaren Chef herzieht, wird sie sehr leicht wertvolle Informationen erhalten.*

Das Prinzip der Täuschung funktioniert deswegen so gut, weil Menschen per se anderen Menschen vertrauen (Bullée & Junger, 2019, S. 13). Grundsätzlich ist Vertrauen etwas Positives und sicherte evolutionär das Überleben, indem Kinder den Erwachsenen vertrauen und von ihnen lernen. Deswegen fällt es Menschen aber unglaublich schwer, Lügen und Lügende zu entlarven.

Ist die Beziehung zum Opfer hergestellt, können die Social Engineers nach Informationen fragen oder das Opfer um einen kleinen Gefallen bitten. Das Prinzip wird häufig nicht allein, sondern in Kombination mit anderen Prinzipien eingesetzt (vgl. Beispiel in Abschnitt 3.3.5).

3.3.5 Verpflichtung, Gegenseitigkeit & Konsistenz

Mögen Sie Tiere? Ist Ihnen die Gesundheit Ihrer Kinder wichtig? Finden Sie nicht auch, dass heute ein schöner Tag ist? – Personen, die auf diese oder ähnliche Fragen mit „Ja" antworten, haben eigentlich schon verloren. (Und wer würde bei diesen Fragen nicht mit „Ja" antworten?)

Das Problem ist das Prinzip der Konsistenz. Haben sich Menschen einmal für etwas entschieden, fühlen sie sich – sich selbst gegenüber – verpflichtet, ihre Entscheidung bis zum (bitteren) Ende zu folgen. Wird mit einer Person aufgrund der oben genannten Fragen ein Gespräch begonnen, und das auch noch mit dem positiven „Ja", so sagt die Konsistenz, dass weiter mit dieser Person gesprochen wird und auch mögliche Anfragen eher mit „Ja" beantwortet werden. Viele Verkaufsgespräche funktionieren so. Anfragen, die zu der ursprünglichen Entscheidung passen, wird bereitwillig gefolgt.

Ist es den Social Engineers also erst einmal gelungen, ihren Opfern eine noch so kleine Information zu entlocken, werden die Opfer auf weitere Nachfragen noch bereitwilliger antworten. Ein schönes Beispiel der Anwendung dieses Prinzips zeigt (Kimmel, 2015). Ein Interviewteam vom Fernsehen (= Autorität) fragt hier Personen nach ihren Passwörtern. Einige sind im ersten Moment nicht bereit, ihr Passwort zu nennen. Nach einigen scheinbar harmlosen Fragen geben sie dann aber ohne zu zögern Auskunft. Aus diesem Muster auszubrechen, erfordert enorme Willenskraft und mentale Anstrengung.

Ein anderes Verhaltensmuster ist die Reziprozität oder Gegenseitigkeit, die sich auf das Gefühl bezieht, einen Gefallen erwidern zu müssen. In einer Gesellschaft wird erwartet, dass man sich für etwas revanchiert, was man von einer anderen Person bekommen hat.

Wenn wir zum Beispiel von unserem Kollegen ein Geschenk zum Geburtstag bekommen, fühlen wir uns verpflichtet, ihm ebenfalls ein Geschenk zu seinem Geburtstag zu machen. Auch dieses Prinzip wird häufig im Verkauf angewendet. Durch kleine kostenlose Proben oder kleine Geschenke, die an die Kinder verteilt werden, fühlen sich die Kund:innen eher verpflichtet, etwas oder etwas mehr zu kaufen.

Reziprozität funktioniert aber auch beim Austausch von Information und Wissen. Ein Geschenk oder eine Gefälligkeit kann also auch mit einer Auskunft erwidert werden (vgl. Beispiel im Kasten).

Passwort gegen Schokolade

Happ et al. (2016) zeigen in ihrer Studie die Macht der Reziprozität. Sie führten kurze Interviews zum IT-Verhalten mit mehr als 1.100 Teilnehmenden. Während der Interviews wurden die Teilnehmenden gebeten, eines ihrer Passwörter preiszugeben. Insgesamt gaben 30 % der Teilnehmenden ihr Passwort preis. Einem Drittel der Teilnehmenden wurde direkt vor der Passwortfrage ein Stück Schokolade angeboten. Von diesen Teilnehmenden nannten sogar 48 % ihr Passwort. Aufgrund des Reziprozitätseffekts führte das kleine Geschenk (ein Stück Schokolade) dazu, dass sie den Gefallen erwiderten, indem sie einige persönliche Daten (das Passwort) preisgaben.

Das Ähnlichkeits- und Sympathieprinzip könnten beim Erfolg dieser Studie ebenfalls eine Rolle gespielt haben. Die Interviewenden waren alle zwischen 20 und 25 Jahre alt und trugen auf ihrer Tasche sichtbar das Logo der örtlichen Universität. Teilnehmende in ähnlichem Alter verrieten ihr Passwort häufiger als der Durchschnitt. Generell kann angenommen werden, dass die befragten Personen mit der örtlichen Universität sympathisieren, weil sie z. B. selbst dorthin gehen oder gegangen sind.

Beim Phishing wird häufig das Prinzip der Konsistenz ausgenutzt. Hat sich das Opfer dazu entschieden, auf den in der E-Mail enthaltenen Link zu klicken, wird es weitere konsistente Handlungen durchführen, wie die Eingabe von Log-in-Daten auf der gefälschten Webseite. Für Annika ist es konsistent, Karten für die jährliche Faschingsparty des Fußballvereins zu kaufen, da sie das seit vielen Jahren tut (vgl. Beispiel in Kapitel 1). Selbst wenn sie sich vielleicht wundert, warum die Anmeldeseite anders aussieht als in den letzten Jahren oder warum dieses Mal mehr Informationen abgefragt werden, die der Verein doch eigentlich haben müsste, wird sie die Angaben eintragen und abschicken.

Tabelle 3.6 Zusammenfassung des Prinzips „Verpflichtung, Gegenseitigkeit & Konsistenz“

Prinzip	Wer einmal eine Entscheidung getroffen hat, zieht sie bis zum Ende durch; Menschen fühlen sich verpflichtet, Gefälligkeiten zu erwidern.
Techniken/Instrumente	Geschenke, Zugeständnisse, harmlose Fragen
Anwendung	Quidproquo, Phishing, Information Gathering

3.3.6 Ablenkung

Menschen können nur begrenzt eingehende Informationen verarbeiten. Sie versuchen daher, sich auf die vermeintlich wichtigsten Fakten zu konzentrieren, und ignorieren alles andere. Ablenkung kann auf viele verschiedene Arten erfolgen: durch Zeitdruck, Angst, Gier, Neugier, Überraschungen, Sehnsüchte und Wünsche, zu viele Informationen oder Knappheit.

Durch die Konzentration auf die Ablenkung rutschen Menschen bei allen anderen Denkprozessen in System 1 (automatisch, ohne Nachdenken). Sie werden quasi blind für alles andere, was um sie herum passiert, und können nicht mehr logisch denken. Social Engineers nutzen das aus, indem sie ihre Opfer gezielt von ihrem eigentlichen Vorhaben ablenken. Typische Mittel zur Ablenkung sind vermeintliche Preisausschreiben oder Wettbewerbe, bei denen schnell reagiert werden muss, um etwas zu gewinnen, sowie generell zeitlich limitierte Angebote.

Ablenkung wird häufig in Kombination mit den anderen Prinzipien eingesetzt und ist häufig der Hauptgrund, warum die Anfragen der Social Engineers funktionieren (vgl. Tabelle 3.7). Die von den Social Engineers „verlorenen" USB-Sticks machen die Findenden neugierig. Sie wollen wissen, was sich darauf befindet. Oder sie wollen helfen und den Stick der besitzenden Person zurückgeben. Beim Baiting (USB-Stick als Köder) wird dieses Prinzip also besonders ausgenutzt.

Tabelle 3.7 Zusammenfassung des Prinzips „Ablenkung" (eigene Darstellung)

Prinzip	Menschen konzentrieren sich auf scheinbar wichtige Fakten oder Handlungen und ignorieren alles andere.
Techniken/Instrumente	Gewinnspiele, zeitlich begrenzte Angebote, Spendenaktionen, Hilferufe
Anwendung	Baiting, Nigerian Scam, Phishing, Vishing, CEO Fraud, Watering Hole

Bei vielen Phishing-Versuchen wird zeitlicher Druck auf die Opfer ausgeübt. Sie sollen z. B. schnell reagieren und ihr Passwort ändern, weil sie sonst nicht mehr auf ihr Nutzungskonto zugreifen können. Annika soll zügig ihre Tickets für die Faschingsparty kaufen, weil diese immer schnell ausverkauft sind. Auch beim CEO Fraud wird Zeitdruck aufgebaut. Das Geld muss unverzüglich überwiesen werden, sonst kann das wichtige Geschäft nicht zustande kommen. Der Betrug mit den gefälschten Twitter-Konten kombiniert den Wunsch der Opfer nach kostenlosen Token mit einem gefälschten Wettbewerb, bei dem nur die schnellsten Teilnehmer gewinnen konnten.

In Bild 3.8 wird sowohl zeitlich Druck aufgebaut als auch das Autoritätsprinzip genutzt, da der Footer suggeriert, dass die E-Mail von einer Regierungsorganisation kommt.

Beim Vishing kann Ablenkung sehr erfolgreich unterstützen, wie der Selbstversuch von Roose (2017) zeigt. In diesem Beispiel wird ein schreiendes Baby als Ablenkung eingesetzt und „zwingt" die Person am anderen Ende des Telefons, der verzweifelten Mutter schnell zu helfen, ohne groß nachzudenken.

Bild 3.8 Phishing-E-Mail mit Ablenkung und Autorität

Die vorhergehende Informationsbeschaffung ist bei der Wahl der richtigen Ablenkung ein Schlüssel zum Erfolg. Menschen lassen sich durch unterschiedliche Dinge ablenken, vor allem, wenn Sehnsüchte oder Wünsche angesprochen werden sollen (vgl. Haucke et al., 2018). Anfragen für ein Interview, einen Vortrag oder die Teilnahme an einer exklusiven Studie schmeicheln dem Ego von denen, die nach Anerkennung streben. Smishing-Nachrichten enthalten vermeintliche Hilferufe der eigenen Kinder, deren Handy angeblich gestohlen wurde oder verloren gegangen ist, und lösen bei vielen Eltern Angst und Hilfsbereitschaft aus. Bild 3.9 zeigt eine Phishing-Mail, welche die Gier im Menschen anspricht oder Menschen in finanzieller Notlage.

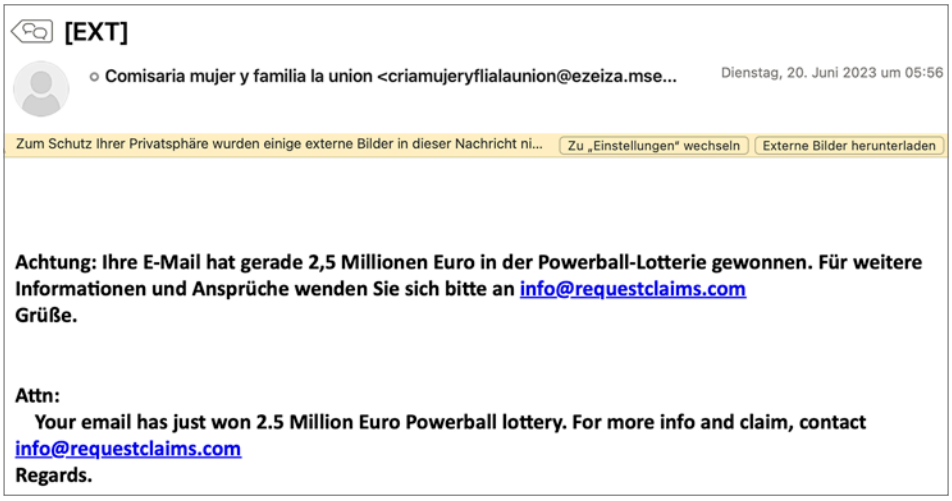


Bild 3.9 Phishing-E-Mail mit angeblichem Gewinn

Stichwortverzeichnis

A
Ablenkung 68
Accidental Insider 32
Agenda Setting Theory 134, 138, 171
Angreifende 9
Anwendende 9
Assoziative Netzwerktheorie 135, 136
Autorität 61, 68
Awareness-Kampagne 74, 84, 89, 99, 100, 139
Awareness-Maßnahmen 73, 76, 88, 94, 99
Awareness Training 73

B
Baiting 50, 68
Bedrohung 9, 19, 43
Behaviorismus 109, 160
Belohnungen 109, 119, 120, 122, 127, 145
Beobachtungen 123, 128, 153
Berichterstattung 119, 124, 138, 175
Betrug 37
Bildschirmsperre 21, 132, 147, 165, 173

C
CEO Fraud 54, 62, 68
Compliance Budget 27

D
Datendiebstahl 35
Dumpster Diving 47

E
Eavesdropping 47
Eigenverantwortung 129
Einstellungen 79, 116, 161
Evaluative Priming 164

F
Fähigkeiten 77, 105, 106
Faktenwissen *siehe* Wissen – deklarativ
Faktor Mensch 1, 2, 16, 91, 182
Feedback 100, 120, 126, 149, 155, 157
Fehlerquelle 10
Fishbein 163, 165
Fragebögen 97, 153, 160

G
Gamification 127
Gedächtnis 110, 135
Gewohnheiten 82, 140, 178
Gruppenzugehörigkeit 121

H
Habitualisierung 142, 144
HAIS-Q 153
Hilfsbereitschaft 28, 60, 69
Hinweisreize 82, 141
Humans as Solution 3, 181

I
Impersonating 50
Individualisierung 83
Informationsbeschaffung 45, 46
Information Security Awareness 5, 73, 77, 83
Informationssicherheit 7
– Gefährdungen 8
informationssicherheitskonform 19, 21, 25, 76
Insider 31
Insider Threat 32, 33
Integriertes Verhaltensmodell 75, 77
Interviews 29, 67, 96, 161, 167, 172
Involvement 134
Involvement Profile 173
ISMS 12
Ist-Analyse 85, 93, 151
IT-Sicherheit 7

K
Klassifikation 21

kognitive Dissonanz 119
Kognitivismus 109
Kommunikation 117
Konstruktivismus 109
Kontrollüberzeugungen 167
Kundschaft 11

L
Lernen 106
– formal 106, 108, 155
– informell 106
– sozial 106
Lernzieltaxonomie 108
Likert-Skala 162, 165, 167, 170, 178

M
Malicious Enabling 37
Malicious Insider 9, 30
Manipulation 44, 60
Marketing 132, 136
Medien 119, 124, 134, 176
Mediendidaktik 113
menschliche Fehlhandlungen 9
menschliche Verhaltensmuster 61
Messen 100, 151
Mindfulness 5, 77, 136
Motivation 121, 146

N
Negligent Insider 32
Non-Malicious Insider 32
Norm
– deskriptiv 120, 166
– injunktiv 120, 164
– wahrgenommen 80, 120, 164

O
Open Source Intelligence 46
Opfer 9, 43
Organisation *siehe* Unternehmen

P
Passwort 20, 21, 26, 29, 67, 118, 131
PDCA-Zyklus 12
persönliche Handlungsfähigkeit 80, 125, 167
Phishing 1, 22, 29, 48, 51, 62, 67, 127, 131, 137, 147, 160, 169
– Smishing 55, 69
– Spear Phishing 1, 53
– Vishing 55, 68
– Whaling 54
Phishing-Simulationen 16, 153
Pretexting 45, 47, 57, 58
Produktivität 27, 75, 132
Psychologie 60
– Sozialpsychologie 72
– Verhaltenspsychologie 77

Q
Quidproquo 59

R
Remote Work 22
Ressourcen 130, 167
Reverse Social Engineering 59
Richtlinien 24, 123
Risiko 14
Risikoorientierung 13
Risikoverständnis 87

S
Sabotage 36
Safety Science 2
Salience Bias 135
Salienz 82, 133, 171
Salienzindex 172
Scareware 59
Schulung 73, 78, 111, 118, 129, 155
Security Champions 10, 115, 121
Selbstvertrauen 126
Selbstwirksamkeitserwartung 125, 169
Self-Report Habit Index 178
semantisches Differenzial 162
Sensibilisierung 71, 73, 90
Sentiment-Analysen 176
Shoulder Surfing 47
Sicherheitsexpert:innen 10
Sicherheitsfaktor 11, 72
Sicherheitskultur 136, 147, 182
Sicherheitsvorfall melden 4, 23, 177
Social Engineering 4, 10, 44, 143
– Attack Cycle 45
– Ontologie 49
Soziale Bewährtheit 63, 65
Soziotechnisches System 2
Spionage 36
Sympathie 65, 67

T
Tailgating 50, 64, 129

Teilnahme 129
Themensalienz 119, 134
Tracking 176

U
Überzeugungen 117, 125
Umfragen 158, 174
Unternehmen 7, 73, 181
Unterstützende 10
Updates 23, 149
Usability 16, 26, 99
USB-Sticks 23, 27, 50, 61, 83, 135, 153

V
Verantwortliche 10
Verhaltensabsicht 78, 114, 160
Verhaltenskontrolle, wahrgenommene 130
Verhaltensweisen 94, 142
Verpflichtung 66
Vorbild 10, 109, 117, 122, 128
VPN 22, 24, 142

W
wahrgenommene Norm 80, 120, 164
wahrgenommene Verhaltenskontrolle 130
Watering Hole Attack 56
Whistleblowing 35
Wirtschaftlichkeit 15, 84
Wissen 77, 105, 130, 155
– deklarativ 105, 110, 155, 160
– explizit 105
– implizit 105
– prozedural 105, 110, 156

Z
Zielgruppen 85, 86, 94, 96, 97, 98, 100, 139