Social Engineering

Silas A. Kraume

19. Juli 2024

INHALT

Zusammenfassung

Dieser Report bietet einen detaillierten Überblick über Social Engineering und seine Angriffsvektoren, sowie dessen Konsequenzen. Er stellt sich die Frage, wieso es keine effektiven Gegenmaßnahmen zu geben scheint um Social Engineering Angriffe effektik zu verhindern, beziehungsweise nachhaltig zu stoppen.

Kapitel 1

Einleitung

Social Engineering ist konträr zu seiner modernen Namensgebung sehrwohl bereits seit Menschengedenken existent. Es lassen sich Beispiele von Social Engineering in der Mythologie, Religion und Geschichte der Menschheit finden. Unter den prominentesten Beispielen ist das Trojanische Pferd[1] **[11, 1]**.

Social Engineering Angriffe dienen also seit Langem als Grundlage für die unterschiedlichsten Betrugsmaschen, aber nehmen im digitalen Zeitalter quantitativ kontinuierlich zu. Sie zielen darauf ab, durch Manipulation an sensible oder wertvolle Daten zu gelangen und richten damit immensen Schaden an **[17, 23, 3]**.

In 2016 erklärte Cyence, ein Cybersicherheitsanalyseunternehmen, dass Deutschland nach den Vereinigten Staaten das Land ist, mit den meisten Social Engineering Angriffen; doch dem U.S. Department of Justice zu Folge stellt dies sogar eine der weltweit bedeutsamsten Gefahren dar. In demselben Jahr (2016) wurde die Bangladesch Bank gehackt, was zu einem immensen finanziellen Verlust führte. Der Angriff wurde langwierig geplant und begannt bereits ein Jahr zuvor. Es gelang den Cyber-Kriminellen in das *SWIFT* Bank Netzwerk einzudringen, welches für Geldüberweisungen genutzt wird. Bei diesem Angriff wurden verschiedenste Social Engineering Methoden angewandt. Insgesamt sollten 1 Milliarden US-Dollar transferiert werden, wobei es den Angreifern letztendlich nur möglich war, 81 Millionen US-Dollar zu stehlen.

Mit der Entwicklung heutiger ICT[2] entwickeln sich auch Social Engineering Taktiken beständig weiter und mit neuen technologischen Möglichkeiten werden auch konsequent neue Formen des Social Engineering ermöglicht. So gelang es 2019 Hackern erfolgreich einen Social Engineering Angriff auf ein unbenanntes Energieunternehmen durchzuführen, indem mit deepfake Technologie der CEO der Firma imitiert wurde.

[1] Es wird erzählt, dass die Griechen den Krieg gegen Troja gewannen, indem sich Odysseus die Social Engingeering Taktik ausdachte, das hölzerne Pferd zu bauen, und die Trojaner zu manipulieren, dieses in die eigene Stadt zu bringen.

[2] Informationen and Communication Technology

Die Audiodaten waren ausreichend authentisch, sodass die Angreifer einen Angestellten davon überzeugen konnten eine Überweisung in Höhe von 243.000 Dollar zu tätigen **[10]**.

Heutzutage verwenden die meisten Cyber-Angriffe eine Form des Social Engineerings **[13, 6]**. Genauer setzen etwa 98% aller Angriffe auf den Menschen als Schwachstelle **[12]**. Diese Form von Cyber-Angriffen richtet sich nicht nur gegen Unternehmen und Regierungsinstitutionen, sondern auch gegen Individuen (insbesondere bezüglich Identitätsdiebstahl) **[26, 28]**.

Social Engineering stellt also eine allgemeine Gefahr für jeden dar, weshalb sich jeder über dieses Thema informieren sollte, um sich entsprechend schützen zu können.

Insbesondere aufgrund dessen, dass Social Engineering ein gesellschaftliches Phänomen ist, welches bereits schon lange existiert, analysiert dieser Report das Thema hinsichtlich der Frage, wieso es keine konsequent effektiven Methoden gibt, um Social Engineering Angriffen entgegenzuwirken. In Kapitel 2 wird ein grundlegender Überblick bezüglich Social Engineering und seinen Angriffsmethoden verschafft. Kapitel 3 beschäftigt sich mit validen Gegenmaßnahmen zu Social Engineering. Darauffolgend analysieren Kapitel 4 und Kapitel 5 Social Engineering hinsichtlich der Forschungsfrage auf sowohl technische und psychologische Weise. Zuletzt wird eine Konklusion genannt.

Kapitel 2

Social Engineering

2.1 Definition

Nach einer groben Definition des Wortes 'Social Engineering' (engl. 'soziale Manipulation') handelt es sich um eine zwischenmenschliche Beeinflussung durch diverse psychologische Tricks zweckgemäß konkrete Verhaltensmuster hervorzurufen. Social Engineering ist also ein Werkzeug, das nicht inhärent gut oder schlecht ist, sondern vielmehr durch seine Anwendung spezifiziert wird.

Geläufiger ist eine Definition im Sinne der Manipulation von Menschen, unrechtmäßig Informationen preiszugeben oder Aktionen auszuführen. Unter derartige Aktionen fallen beispielsweise das Aushebeln von Sicherheitsfunktionen, das Tätigen von Überweisungen oder das Installieren von Schadsoftware **[13, 3]**.

Das Bundeskriminalamt legt in einer Forschungsstudie die offizielle Definition des Verfassungsschutzes Brandenburg zugrunde: „Social Engineering ist der Versuch, unter Ausnutzung menschlicher Eigenschaften Zugang zu Know-how zu erhalten. Der Angreifer nutzt dabei Dankbarkeit, Hilfsbereitschaft, Stolz, Karrierestreben, Geltungssucht, Bequemlichkeit oder Konfliktvermeidung aus. Dabei bieten häufig soziale Netzwerke oder auch Firmenwebseiten Möglichkeiten, um sich auf sein Opfer gründlich vorzubereiten. Zu diesen 'Vorfeldermittlungen' können auch Anrufe im Unternehmen gehören. Professionelle Angreifer versuchen dabei nicht, mit einem Anruf alle gewünschten Informationen zu erlangen, dies könnte misstrauisch stimmen. Der Angerufene wird dabei im Gespräch nach vermeintlich nebensächlich erscheinenden Informationen gefragt.“

In der Kurzfassung: Social Engineering ist eine zwischenmenschliche Manipulation, bei der ein Unbefugter unter Vortäuschung falscher Tatsachen versucht, unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen **[5]**.

In Bezug zu IT-Systemen und digitalen Daten wird Social Engineering auch konkreter

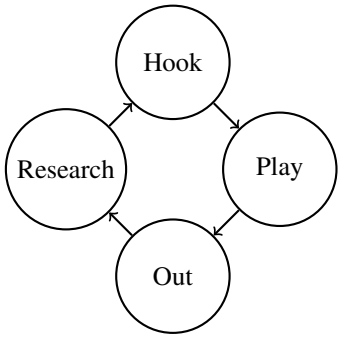
als 'Social Hacking' definiert **[7, 22]**.

2.2 Angriffsvektoren

2.2.1 Methodik

Obgleich unterschiedliche Social Engineering Angriffe fundamental verschieden ablaufen, so haben sie dennoch eine grundlegende Struktur gemeinsam. Diese Struktur lässt sich in vier Phasen einteilen:

- 1) Research
- 2) Hook
- 3) Play
- 4) Out



[23, 20, 16]

Research

In der ersten Phase sucht der Angreifer sein Opfer aus und sammelt alle erwerblichen Informationen im Zusammenhang mit dieser Person. Anhand dessen kann ein möglicher Angriffsvektor etabliert werden. Der Erfolg eines Angriffes ist oft abhängig von ausführlicher Recherche, weshalb ein Großteil des zeitlichen Aufwandes in dieser Phase steckt **[23, 20, 16]**.

Hook

In der 'Hook' Phase baut der Angreifer eine Beziehung mit dem Opfer auf. Die Qualität dieser Beziehung bestimmt die folgende Kooperation des Opfers. Abhängig von dem exakten Angriffsvektor kann diese Phase beispielsweise eine langwierige Beziehung durch etwa Social Media darstellen. In anderen Angriffen definiert diese Phase den ersten Eindruck im Affekt einer Situation, etwa durch freundliche Gestik oder Mimik. Es reichen für die meisten Menschen bereits 100 ms[1] aus, um über Attraktivität, Sympathie, Vertrauenswürdigkeit, Kompetenz und Aggressivität zu urteilen **[31]**, weshalb der erste Eindruck bei gewissen Social Engineering Taktiken elementar ist **[23, 20, 16]**.

Play

In der dritten Phase nutzt der Angreifer die zuvor erlangten Informationen und die Beziehung zum Opfer aus, um dieses dazu zu bewegen, sensible Daten preiszugeben

[1] Millisekunden

oder eine sicherheitskritische Aktion auszuführen **[23, 20, 16]**.

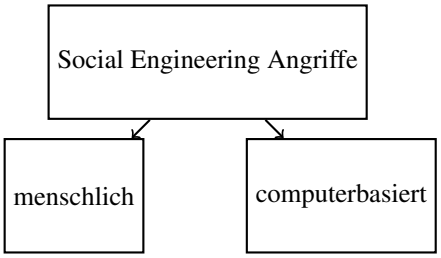
Out

Zuletzt zieht sich der Angreifer in der letzten Phase zurück, ohne jegliche Beweise eines Angriffes zurückzulassen. Zum Beispiel werden digitale Fußabdrücke gelöscht, sodass der Angriff gegebenenfalls nicht auffällt, die Identität des Angreifers anonym bleibt und die Möglichkeit besteht, zukünftig erneut Kontakt aufzunehmen **[23, 20, 16]**.

2.2.2 Klassifikation

Social Engineering Angriffe können hinsichtlich verschiedener Aspekte klassifiziert werden[2]. Einerseits lassen sich verschiedene Angriffsvektoren nach dem verwendeten Medium unterscheiden. Auf diese Weise lassen sich die folgenden zwei Kategorien identifizieren:

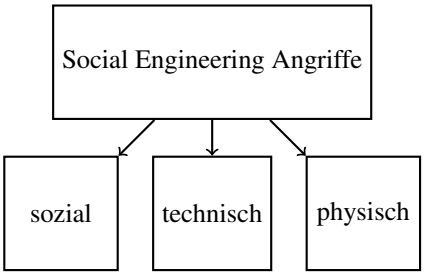
- 1) menschlich
- 2) computerbasiert



[13, 23]

Andererseits können Angriffsvektoren danach klassifiziert werden, wie die Angriffstechnik ausgeführt wird. Somit entstehen die folgenden drei Klassifikationen:

- 1) sozial
- 2) technisch
- 2) physisch



[23]

menschliche Angriffe

Im Falle von menschlichen Angriffen kommt es durch persönlichen Kontakt zu direkter Interaktion zwischen dem Angreifer und seinem Opfer. Diese Angriffe können durchaus auch digital ablaufen, etwa über beliebige Messaging-Plattformen, und verwenden gezielte psychologische Manipulation, die der Angreifer spezifisch auf sein Opfer abstimmt **[23, 13]**.

[2]Social Engineering Angriffe können gegebenenfalls mehrere dieser Aspekte kombinieren.

computerbasierte Angriffe

Computerbasierte Angriffe, oder auch softwarebasierte Angriffe, werden mithilfe von Computern[3] ausgeführt, um Informationen des Opfers zu sammeln. Diese Art von Angriff ist in der Lage, eine Vielzahl von potenziellen Opfern in kürzester Zeit zu erreichen **[23, 13]**.

technische Angriffe

Technische Angriffe zielen darauf ab, Information wie Passwörter oder Kreditkarteninformationen zu erlangen. Sie werden ausgeführt über das Internet durch die sozialen Medien, Webseiten oder anderweitigen online Diensten **[23, 17]**. „Die Kommunikation über digitale Kanäle wie E-Mail bietet ein besonders günstiges Umfeld für Social Engineering. Während der Täter sein Gegenüber in einer realen Gesprächssituation über alle Sinne hinweg täuschen muss, hat er es bei der technisch vermittelten Kommunikation deutlich einfacher“**[3]**.

soziale Angriffe

Bei sozialen Angriffen werden das psychologische Verhalten und die Emotionen des Opfers ausgenutzt. Diese Angriffe sind am gefährlichsten und in Relation zu ihrer Quantität am erfolgreichsten, da sie menschlichte Interaktion beinhalten **[23]**.

physische Angriffe

Physische Angriffe definieren diejenigen Aktionen, bei denen der Angreifer selbst materiellen Daten sammelt und nach Informationen sucht. Beispielsweise durchsucht der Angreifer Mülleimer, rekonstruiert zerstörte Dokumente oder begeht Diebstahl **[23]**.

2.2.3 Techniken

Es ist nahezu unmöglich, einen vollständigen Überblick über alle existenten Angriffsvektoren im Bereich des Social Engineering zu liefern. Wie zuvor in Kapitel 1 erwähnt, sind diverse Social Engineering Techniken mit aktuellen ICT konstant im Wandel. Etwaige Angriffsmethoden sind wie folgt:

Phishing

Phishing ist eine der üblichsten Angriffsmethoden des Social Engineering. Es handelt sich um semantische Angriffe durch elektronische Kommunikationswege (wie etwa E-Mails, HTTP, SMS, VoIP), um manipulative Nachrichten zu übermitteln, die das Opfer dahingehend beeinflussen sollen, konkrete Aktionen auszuführen. Diese Aktionen beinhalten etwa das Klicken von illegitimen Links oder das Eingeben von (Anmelde-) Informationen. Die Daten, auf die es ein Angreifer abgesehen hat, erstrecken sich von Kreditkarteninformationen und explizit sensiblen Daten bishin zu Informationen wie

[3] darunter zählen auch Smartphones oder anderweitige computerähnliche Geräte

dem Namen eines Elternteils oder Haustieres. Solche Informationen sind oft unscheinbar, können allerdings ein immenses Sicherheitsrisiko darstellen, etwa im Kontext von Sicherheitsfragen beim Log-in in einen Account. Die am weitesten verbreitete Methode des Phishings ist das simple Verschicken vorgefertigter E-Mails an zahlreiche Individuen **[23, 18]**.

Phishing Angriffe lassen sich in weitere Unterkategorien einteilen. Darunter liegen zum Beispiel Spear Phishing und Whaling. Spear Phishing bezieht sich auf Phishing Angriffe, die auf spezifische Individuen oder ausgewählte Gruppen abzielen. Diese Angriffe sammeln im Vorfeld Informationen, um den Angriff präziser auf ihre Opfer maßzuschneidern. Insofern diese ausgewählten Angriffsziele hochrangige Persönlichkeiten verkörpern, die als 'Big Fishes' oder 'Whales' bezeichnet werden, handelt es sich um Whaling Angriffe **[23]**.

Phishing wird im großflächigeren Raum auch als *ishing dargestellt, da die Namensgebung bei dieser Form des Social Engineering abhängig von der technischen Angriffsmethode ist. So sind beispielsweise Vishing (Voice-Phishing, das Phishing über Telefon), Smishing (SMS-Phishing), Quishing (QR-Code-Phishing) oder Tishing (Microsoft-Teams-Phishing) definiert **[30]**.

Pretexting

Diese Technik verwendet einen Vorwand (engl. 'Pretext'), also eine falsche Rechtfertigung für eine bestimmte Vorgehensweise, um das Vertrauen des Opfers zu gewinnen und dieses zur Kooperation zu manipulieren. Pretexting zielt auf die Emotionen des Opfers ab, um neben Vertrauen ein Gefühl von Dringlichkeit oder Sympathie zu erzeugen. Das Hauptmerkmal dieses Angriffes ist seine kreative Komponente. Oftmals täuschen Cyber-Kriminelle eine Autoritätsperson vor, wie etwa einen Investor, und legen sogar fälschliche online Persona mitsamt Webseiten und Bewertungen an, um seriös zu wirken. Populär ist auch das Ausgeben als IT support mit der Anfrage auf Log-in Daten, welche angeblich zu Wartungszwecken gebraucht werden. Andere Methoden enthalten Romance-Scams, in denen der Betrüger ein Interesse an einer romantischen Beziehung vorspielt, oder Nachahmung, wobei der Angreifer sich zum Beispiel als Firmenkollege ausgibt und das Opfer um „dringende Hilfe“ bittet **[13, 23]**.

Tailgaiting

Unter Tailgating versteht man das physische Eindringen eines Social Engineers in unbefugte Areale. Dies wird erreicht, indem der Kriminelle Personen mit Sicherheitsbefugnis dicht folgt, Sperrzonen bewusst umgeht oder Pretexting (Abschnitt 2.2.3) verwendet. Beispielsweise erklären Angreifer selbstbewusst, dass sie ID Karte verloren oder vergessen haben. In vielen Szenarien wird die Befugnis durch das äußere Erscheinungsbild, wie zum Beispiel dem Tragen von Warnwesten oder dem Dresscode eines Unternehmens vorgetäuscht oder die Hilfsbereitschaft anderer ausgenutzt, indem der Angreifer zum Beispiel schwere/viele Boxen trägt. Insofern im Prozess des Angriffes die Erlaubnis von befugtem Personal erlangt wird, handelt es sich um sogenanntes Piggybacking **[23]**.

Baiting

Baiting ist eine Social Engineering Methode, die sich die Neugierde der Menschen zunutze macht. Sie zeichnet sich dadurch aus, bewusst einfachen Zugang zu einem Köder zu bieten, welcher darauf abzielt, eine konkrete Handlung des Opfers auszulösen. Im Kontext der Phishing Angriffe lädt eine Baiting E-Mail etwa dazu ein, auf einen Link zu klicken, der beispielsweise kostenlose Prämien verspricht. Unter Baiting Angriffe fallen ebenfalls sogenannte Media-Drops. Beispielsweise werden bei USB-Drops absichtlich USB-Sticks platziert, die darauf abzielen, gefunden zu werden, und bei Verwendung den Computer infizieren. Eine weitere Möglichkeit ist es, die infizierten Medien wie CDs oder anderweitige beliebige Datenträger vor Firmengeländen als Werbegeschenke zu verteilen. Bei erfolgreicher Infektion eines Computers haben die Akteure bereits die Möglichkeit, Informationen zu stehlen oder anderweitige Malware zu installieren; beliebt sind Trojaner zu langzeitlichen Kontrolle eines Systems, Ransomware als Form der Erpressung **[13, 23, 16]** oder Spyware zur kontinuierlichen Informationssammlung.

Quid Pro Quo

Quid pro quo (lateinisch für 'dies für das') funktioniert auf eine ähnliche Weise wie Baiting Angriffe, wobei dieser Angriffsvektor nicht Neugierde, sondern Vertrauen ausnutzt. Es handelt sich um eine Anfrage nach persönlichen oder geschäftlichen Informationen im Austausch gegen Kompensation. Angreifer bieten zumeist einen Service an, der für das Opfer verlockend oder hilfreich ist. Quid Pro Quo wird oftmals in gezielten Spear Phishing Angriffen (Abschnitt 2.2.3) verwendet. Möglich ist auch, dass der Angreifer eine Studie oder ein Experiment vortäuscht, was bei Teilnahme Kontaktdaten benötigt und im Gegenzug eine Geldsumme verspricht **[13]**.

Reverse Social Engineering

Reverse Social Engineering Angriffe lassen ihre Opfer glauben, es gäbe ein (technisches) Problem oder inszenieren einen tatsächlichen Schaden, wenn sie beispielsweise ein Netzwerk zum Absturz bringen. Im Folgenden überzeugen sie ihre Opfer auf verschiedenste Weise, dass sie alleine das Problem beheben können. Während sie das Problem lösen, erlangen sie die gewünschten Informationen und ziehen sich abschließend zurück, ohne jemals ihre Identität preiszugeben **[23]**. Im Gegensatz zu anderen Social Engineering Angriffen sind es nicht die Angreifer, die auf ihre Opfer zugehen, sondern die Opfer, die gutgläubig Hilfe bei den Angreifern suchern.

Pop-Up Windows

Es existieren zwei verschiedene Grundstrukturen im Aufbau von Pop-up Fenstern als Social Engineering Taktik. Erstere verwendet eine Methodik ähnlich zum Baiting (Abschnitt 2.2.3). Hierbei wird zum Beispiel vorgetäuscht, das potenzielle Opfer habe in einer Verlosung oder der Lotterie gewonnen. Zweitere verwendet elementar die Taktik von Scareware; es wird also Panik beim Opfer ausgelöst, mit dem Ziel, dieses verängstigt in unüberlegte Handlungen zu bewegen. Die hierbei dargestellte Gefahr wirkt

bedrohlich, ist allerdings lediglich simuliert und nicht existent. Unter den populärsten Pop-up-Windows sind fälschliche Nachrichten, die davon überzeugen sollen, der Computer habe bereits Malware installiert und benötige nun ein Antivirenprogramm, welches im selbigen Pop-Up Fenster angeboten wird. Insgesamt lassen sich derartige Angriffe primär eingebunden in Webseiten finden, durch (Browser-) Plug-ins oder zuvor installierten Programmen. Das Ziel dieser Fenster ist es, dazu zu bewegen, Informationen einzugeben, auf Links zu klicken oder Fake Software[4] herunterzuladen.

Weiteres

Es gibt viele weitere Arten von Angriffsvektoren. Einige davon lassen sich wie folgt zusammenfassen:

- Impersonation/Masquerading: Eine Form des Identitätsdiebstahles, bei der der Angreifer vorgibt jemand anderes zu sein.
- Eavesdropping: Das unbemerkte Mithören, oder Lesen, von der Kommunikation Anderer, ohne deren Erlaubnis.
- Shoulder surfing: Das Beobachten von Personen, während diese sensible Daten, wie Passwörter, eingeben.
- Dumpster diving: Der Angreifer sammelt sensible Informationen, wie (geschredderte) Dokumente, in dem Mülleimern seines Ziels.
- Diversion Theft: Ein Transportunternehmen, oder -vehikel, wird mit falschen Anweisungen beauftragt, ein Paket an einen vom Kriminellen gewünschten Ort zu bringen.
- Pharming: Der Datenverkehr einer Webseite wird auf eine andere, bösartige Webseite umgeleitet.
- Deepfake: Medien, die künstlich verändert oder generiert werden, um den fälschlichen Anschein zu erwecken, dass Individuen etwas getan oder gesagt haben.

[23, 27]

[4]Fake Software enthält oft zu teilen legitime Software, welche der Social Engineer neu verpackt

Kapitel 3

Maßnahmen

3.1 Erkennung & Vorbeugung

Um verschiedene Angriffe zu erkennen und damit präventiv zu verhindern, werden verschiedene Techniken vorgeschlagen. Eine Liste von Abwehrverfahren gegen Social Engineering umfasst Förderung von Sicherheitsschulungen und Steigerung des allgemeinen Bewusstseins für Angriffsvektoren durch entsprechende Aufklärung; die beste Methode gegen eine soziale Form des Angriffes ist ein soziales Bewusstsein, angegriffen zu werden **[23]**. Derartige Schulungen sollten erklären, wie die Sicherheit kritischer Informationen gewährleistet werden kann und stetig auf aktuelle Angriffsmuster aufmerksam machen, wie etwa bekannte Phishing Kampagnen **[23]**. Regelmäßige Poster, Präsentationen, E-Mails und Informationsschreiben können weiter dazu beitragen, das Bewusstsein zu verbreiten. Es wird zudem empfohlen, dass Organisationen Penetrationstests ausführen, um die Anfälligkeit für Social Engineering zu ermitteln **[13]**.

Viele Angriffe verlieren an Wirksamkeit, wenn ausreichende Identifizierungs- und Authentifizierungsprozesse vorhanden sind. Beispielsweise bietet Mehr-Faktor-Authentifizierung eine zusätzliche Sicherheitsebene zu Benutzername und Passwort. Hierbei stehen Optionen wie ein Authentifizierungscode, ein Daumenabdruck oder ein Netzhautscan zur Verfügung. Es sollten verschiedene Anmeldedaten für unterschiedliche Plattformen eingesetzt werden **[13, 2]**. Um physischen Angriffen wie Tailgating (Abschnitt 2.2.3) entgegenzusetzen, sollte der Zugang zu nicht öffentlichen Bereichen durch Zugangsrichtlinien und/oder den Einsatz von Zugangskontrolltechnologien kontrolliert werden. Die Pflicht, einen Ausweis zu tragen, die Anwesenheit von Sicherheitspersonal und explizite Türen zum Schutz vor Tailgating, wie Schleusen mit RFID-Zugangskontrolle[1] reichen häufig aus, um die meisten Angreifer abzuschrecken **[13]**.

Oftmals werden persönliche Informationen, die freiwillig offen gelegt wurden, von Kriminellen missbraucht, weshalb bereits der verantwortungsvolle Umgang mit den

[1] RFID (Radio Frequency Identification signals) verwendet elektromagnetische Ausweise

sozialen Netzwerken eine hilfreiche Gegenmaßnahme darstellen kann. Unter keinen Umständen sollten private oder berufliche Informationen öffentlich preisgegeben werden.

Angriffen wie Baiting (Abschnitt 2.2.3) kann entgegengewirkt werden, wenn entsprechende Systeme installiert sind, welche unautorisierte Software und Hardware blockieren. Grundsätzlich gilt, keinen unbekannten Kontaktaufnahmen zu vertrauen **[13]** und die Legitimität von Anrufen und E-Mails (oder anderweitigen Quellen) ausreichend zu prüfen. Insbesondere sollten bei E-Mails die drei kritischen Punkte Absender, Betreff und Anhang vor dem Öffnen bedacht und überprüft werden **[3]**. Links sollten nicht geöffnet werden, bevor diese verifiziert wurden. Beispielsweise lässt sich die URL eines Links bereits durch das Bewegen des Mauszeigers über den Link inspizieren, bevor dieser angeklickt wurde. Merkmale, auf die hierbei geachtet werden sollte, sind, ob die URL semantisch unseriös wirkt und/oder mit 'http' anstelle von 'https' beginnt.

3.2 Juristik

Die strafrechtlichen Folgen von Social Engineering haben im digitalen Zeitalter beständig angepasst und verbessert werden müssen. Wie zuvor etabliert ist Social Engineering zudem umfangreich in seinen Möglichkeiten, weshalb Tatbestände detailreich und sachbezogen behandelt werden müssen. Es folgt keine vollständige strafrechtliche Beurteilung, vielmehr ein grundlegender Überblick über die essenziellsten juristischen Grundlagen. Des Weiteren ist die Handhabung von Social Engineering als Straftat nicht uniform sondern variiert in unterschiedlichen Ländern.

In Österreich wird Social Engineering beispielsweise juristisch zumeist nur mit Geldbußen bestraft. „Da sich der Angreifer Zugang zu einem Computersystem verschafft, über das er nicht oder nicht alleine verfügen darf, ist ein Teil des objektiven Tatbestandes des §118a StGB erfüllt. Dieser erfordert jedoch [zusätzlich], dass die Zugangsverschaffung durch die Verletzung einer Sicherheitsvorkehrung erfolgt, die sich 'im Computersystem' befindet. Da sich die durch Social Engineering Angriffe verletzte Sicherheitsvorkehrung Mensch jedoch nicht 'im Computersystem' befindet, ist der objektive Tatbestand des §118a StGB idR nicht erfüllt.“**[14]** Die Fassung von §118a StGB wurde in den Jahren 2007, 2015 und 2023 neu aufgelegt, enthält in jeder dieser Auflagen jedoch dieselbe Formulieren bezüglich der Verletzung von Sicherheitsvorkehrungen. Social Engineering ist hier rechtlich gesehen somit allenfalls eine Täuschung **[14]**.

In Deutschland fällt Social Engineering zumeist unter die 'Verletzung des persönlichen Lebens- und Geheimbereichs', insbesondere §202a[2], §202b[3] und §202c[4]. Nach §202a Abs 1 StGB gilt: „Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“ Für technische Angriffsvektoren (Abschnitt 2.2.2) gilt

[2] Ausspähen von Daten
[3] Abfangen von Daten
[4] Vorbereiten des Ausspähens und Abfangens von Daten

zudem explizit §202b, welches das unbefugte Verschaffen von nichtöffentlichen Daten unter Anwendung technischer Mittel behandelt. §202c beschreibt das Vorbereiten der in §202a und §202b erklärten Tatbestände, etwa durch den Besitz von „Computerprogramme[n], deren Zweck die Begehung einer solchen Tat ist“.

Social Engineering kann ebenfalls eine Straftat gegen die öffentliche Ordnung darstellen, wenn eine Gefährdung der Verbreitung personenbezogener Daten (§126a) vorliegt. Insofern bei einem Social Engineering Angriff beispielsweise ein Passwort erlangt wird, muss geprüft werden, ob die Entwendung ein konkretes Individualrecht verletzt. Dies ist der Fall, insofern das Passwort eine personenbezogene Informationen darstellt, also die Identität einer Person in Zusammenhang des öffentlich bekannten Benutzernamen bestimmbar ist. Ist das Passwort hingegen für einen administrativen Account eines unpersönlichen Computersystems, so liegen bei der Entwendung keine personenbezogenen Daten vor.

Bei dem Straftatbestand des Datendiebstahls sowie der Datenhehlerei (§202d) handelt es sich um ein sogenanntes Antragsdelikt, sodass die Polizei erst nach einer entsprechenden Strafanzeige ein Ermittlungsverfahren eröffnen kann **[19]**.

Selbstverständlich ist die typische Folge eines gelungenen Social Engineering Angriffes oftmals eine weitere Straftat wie Identitätsdiebstahl, Verbraucherbetrug oder Diebstahl. Diese werden als eigenständige Tatbestände behandelt **[21]**.

Kapitel 4

Auswirkungen

4.1 Prävalenz

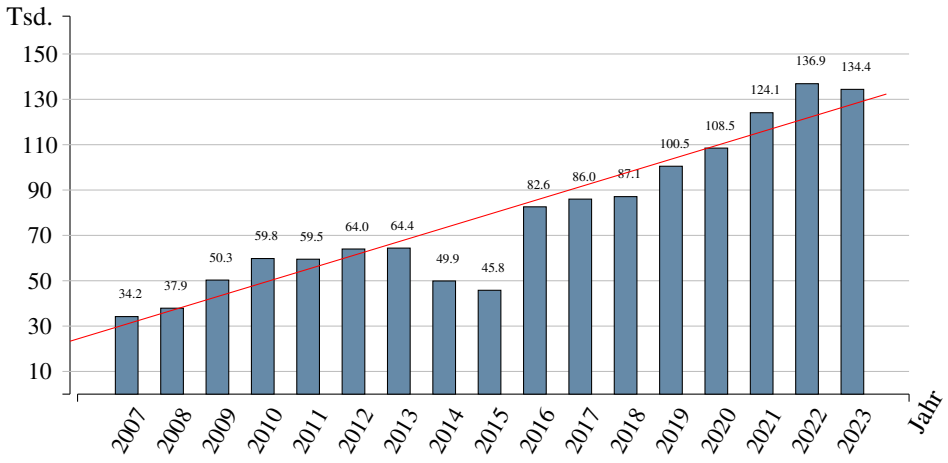


Abbildung 4.1: Von der polizeilichen Kriminalstatistik (PKS) registrierte Straftaten im Bereich Cybercrime von den Jahren 2007 bis 2023. Zusammengetragene Werte aus den jährlich veröffentlichten Bundeslagebildern des Bundeskriminalamtes **[4]**. Die in rot dargestellte Trendkurve wurde anhand der ungerundeten Werte kalkuliert und weist einen linearen Korrelationskoeffizienten von 0.9304 auf.

„Bei Cybercrime ist von einem sehr großen Dunkelfeld auszugehen. Das heißt, dass vermutlich nur ein kleiner Teil der Straftaten in diesem Bereich zur Anzeige gebracht wird bzw. der Polizei und/oder den Strafverfol- gungsbehörden bekannt ist. Bereits 2013 hatte eine in Niedersachsen durchgeführte Dunkelfeldstudie ein Dunkelfeld von 91 % aller Cyber- crimestraftaten errechnet04.“ BKA

4.2 Schaden

Das finanzielle Motiv im Cybercrime ist nicht nur das primäre Motiv von Cyber Kriminellen, sondern verdrängt alle anderen Motive nahezu vollständig. Neben einer finanziellen Motivation existieren beispielsweise Espionage und persönliche Motive, wobei Letztere statistisch außer Acht zu lassen sind. Waren 2022 noch 11% aller Data Breaches durch Espionage motiviert, so sind es 2023 gelegentlich 5%. Entsprechend stieg in diesen Jahren das finanzielle Motiv von 89% auf 95% an **[29, 30]**.

Im Durchschnitt richtet ein 'Data Breach' 4.45 Millionen US-Dollar an Schaden an, wobei Social Engineering als initialer Angriffsvektor noch über diesem Wert liegt **[24]**.

Der Verlust, nach erfolgreichen Social Engineering Angriffen, ist jedoch für Unternehmen weitreichender. Neben dem direkten finanziellen Verlust, durch den Diebstahl der Angreifer erleiden Unternehmen zusätzlich Wiederherstellungskosten, da etwaige Daten verloren gegangen sind, und Sicherheitslücken gefunden und repariert werden müssen. Des Weiteren entsteht eine Betriebsdisruption, was zu indirektem finanziellen Schaden, durch Verlust von Produktivität, führt. Zuletzt erleiden Unternehmen einen Reputationsschaden, was in vielen Fällen den verheerendsten Faktor ausmacht, insbesondere für kleinere Firmen **[25]**. Für Unternehmen können Cyber-Angriffe auch eine Form der Espionage darstellen, weshalb der Schaden eines Unternehmens zusätzlich einen kompetitiven Schaden in der Marktwirtschaft darstellen kann.

Individuen erleiden ebenfalls, neben finanziellen-, auch weitere Formen von Schäden. Nicht außer Acht zu lassen ist der emotionale Schaden, da Personen oft, in Folge einer erfolgreichen Manipulation, als naiv dargestellt werden.

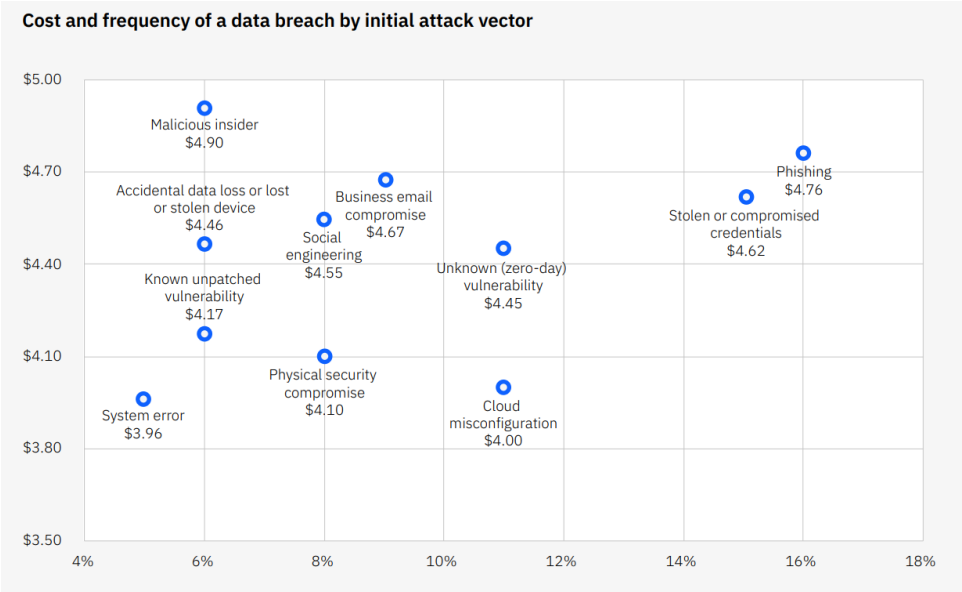


Abbildung 4.2: IBM - Measured in USD millions

Avg. Kosten pro Breach (2022)

Kapitel 5

Psychologie

Im Social Engineering werden verschiedene menschliche Eigenschaften ausgenutzt, um eine Person zu manipulieren. Das Bundeskriminalamt (BKA) hat 2015 in einer Studie „6 soziale Einfallstore [. . .] identifiziert:

- Hilfsbereitschaft
- Leichtgläubigkeit
- Neugier
- (Wunsch nach) Anerkennung
- Druck
- Angst.

“**[5]**

Selbiger Studie ist zu entnehmen, warum die sozialen Angriffsvektoren eine hohe Wirksamkeit erreichen, denn der Begriff selbst ist vielen unbekannt und wird sogar oftmals fälschlicherweise mit positiven Assoziationen verbunden.

Das bedeutet, dass durch fehlende Aufklärung Opfer nicht das nötige Bewusstsein haben, um eine Situation akkurat als Bedrohung zu identifizieren. Des Weiteren werden beim Social Engineering Verhaltensweisen ausgenutzt, die in der Regel sozial erwünscht sind, weswegen Maßnahmen nicht in der Lage sind, derartige Vorfälle zu verhindern **[5]**.

5.1 Einflussprinzipien

Ein Angreifer kann die Entscheidungsfähigkeit zu seinem Vorteil beeinflussen, denn Menschen reagieren oftmals mit automatisiertem Sozialverhalten **[5]**. Der Psychologe Robert Cialdini entwickelte die sechs Prinzipien der Überzeugung/Beeinflussung („Six

Principles of Persuasion“), welche in weitreichenden Studien demonstiert wurden[1] **[26, 8]**. Die sechs Prinzipien bestehen aus:

Authority

Die meisten Menschen neigen dazu, Autoritätspersonen beziehungsweise Personen mit Fachwissen oder ergiebigen Erfahrungen zu glauben, und gehorchen den Anweisungen eben jener. Autorität (engl. 'Authority') kann Menschen selbst dazu verleiten, gegen ihren Glauben oder ihre moralische Vorstellung zu handeln. Eine Person gilt als Autoritätssymbol, wenn sie als legitimer Experte wahrgenommen wird. Symbole der Autorität, wie etwa Titel, äußeres Erscheinungsbild oder Statussymbole wie luxuriöse Gegenstände, erhöhen die Folgsamkeit bei anderen **[26, 15, 5]**.

Commitment & Consistency

Konsistenz (engl. 'Consistency') sorgt dafür, dass Personen sich konsequent zu ihren Verpflichtungen (engl. 'Commitments') und Überzeugungen verhalten. Das menschliche Verlangen nach Konsistenz gegenüber eingegangenen Verpflichtungen kann das Verhalten einer Person langzeitlich beeinflussen. Beispielsweise lässt sich dieses Verhalten insofern feststellen, dass Personen, die eine kleine Petition unterschreiben, später wesentlich gewillter sind, sich auch anderweitig zu diesem Zweck zu engagieren **[26, 15, 5]**.

Reciprocity

Das Prinzip der Gegenseitigkeit (engl 'Reciprocity') beruht auf der fundamentalen Tendenz, dass sich Menschen dazu verpflichtet fühlen, Gefallen oder Geschenke zu erwidern. Dieses Prinzip ist derartig stark, dass die Erwiderung vehementer ausfallen kann als den initial erhaltenen Gefallen **[26, 15, 5]**.

Liking

Aufgrund des grundlegenden Motivs, soziale Beziehungen aufzubauen und aufrechtzuhalten, führen Menschen die Anfragen anderer eher aus, wenn sie diese Person kennen oder mögen (engl. 'like'). Wahrgenommene Ähnlichkeiten erhöhen die Fügsamkeit einer Person. Diese können durchaus oberflächlicher Natur sein, wie etwa ein gemeinsamer Geburtstag oder Name. Andere Faktoren, die dazu beitragen, von einer Person gemocht zu werden, sind physische Attraktivität und positive Assoziation, etwa durch Komplimente **[26, 15, 5]**.

Social Proof

Das Prinzip des sozialen Beweises (engl. 'social proof') ist ein Phänomen, das in der Psychologie als 'informativer sozialer Einfluss' bekannt ist. Es geht um eine mächtige Überzeugungstaktik, die ausnutzt, dass Menschen eine natürliche (bzw. primitive)

[1] Da in der Psychologie Situationsfaktoren und menschliche Emotionen immer eine Rolle spielen, ist der Erfolg bei Anwendung dieser Prinzipien nicht garantiert.

Tendenz haben, dem Beispiel anderer folgen zu wollen, um sozial akzeptiert zu werden **[26, 15, 5]**.

Scarcity

Das letzte Prinzip der Überzeugung ist die Knappheit (engl. 'scarcity') und beschreibt die Tatsache, dass Menschen einer geringeren Quantität eine höhere Qualität zuschreiben. Dieses Prinzip ist nicht ausschließlich auf Materielles anzuwenden, sondern gilt beispielsweise auch bei verhaltenstechnisch weniger verfügbaren Möglichkeiten oder bei Informationen, die nicht allgemein erhältlich sind. So wirken Informationen, die einem im Geheimen anvertraut werden, oft spektakulärer **[26, 15, 5]**.

5.2 Persönlichkeitsmerkmale

Das Fünf-Faktor-Modell ist ein Modell der Persönlichkeitspsychologie, welches fünf Kernaspekte der Persönlichkeit identifiziert und besagt, dass jeder Mensch sich auf den Skalen dieser Kernaspekte einordnen lässt. Die fünf Eigenschaften bieten also jeweilige Skalen im Wertebereich von 0 bis 100. Das Modell wird auch als OCEAN-Modell bezeichnet (nach den entsprechenden Anfangsbuchstaben Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism[2]). Die folgende Tabelle beschreibt knapp die verschiedenen Kerneigenschaften:

Eigenschaft	hoher Wert	niedriger Wert
Offenheit	intellektuell, fantasievoll, kontaktfreudik. Offen für Neues	praktisch, konventoniell, skeptisch, rational
Gewissenhaftigkeit	organisiert, eigenständig, gründlich, zuverlässig, aber kontrollierend	desorganisiert, nachlässig, kann anfällig für Sucht sein
Extraversion	aufgeschlossen, enthusiastisch, aktiv; sucht Neues	distanziert, ruhig, unabhängig; vorsichtig, zurückgezogen
Verträglichkeit	vertrauensvoll, unkompliziert, empathisch, nachgiebig, umgänglich	unkooperativ, feindselig; unempathisch
Neurotizismus	anfällig für Stress, Angst, Befangenheit, Launenhaftigkeit, Impulsivität	emotional stabil, ruhig und sicher.

Tabelle 5.1: Charakteristiken der OCEAN-Modell Persönlichkeitseigenschaften, entnommen aus **[9]**.

[2] zu Deutsch: Offenheit, Gewissenhaftigkeit, Extraversion, Verträglichkeit, Neurotizismus

5.3 Anfälligkeit für Social Engineering

Gewisse Persönlichkeitseigenschaften sind direkt korreliert mit der Anfälligkeit verschiedener Prinzipien der Beeinflussung und damit dem Social Engineering. Es gibt drei verschiedene Persönlichkeitsmodelle im Zusammenhang mit Social Engineering: FFM (Five-Factor Model), MBTI (Myers-Briggs Type Indicator), DT (Dark Triad Model). Die folgende Grafik verdeutlicht den Zusammenhang zwischen bestimmten Überzeugungsprinzipien und Persönlichkeitsmerkmalen, von denen aus psychologischer Sicht ausgegangen wird, nach dem FFM-Modell:

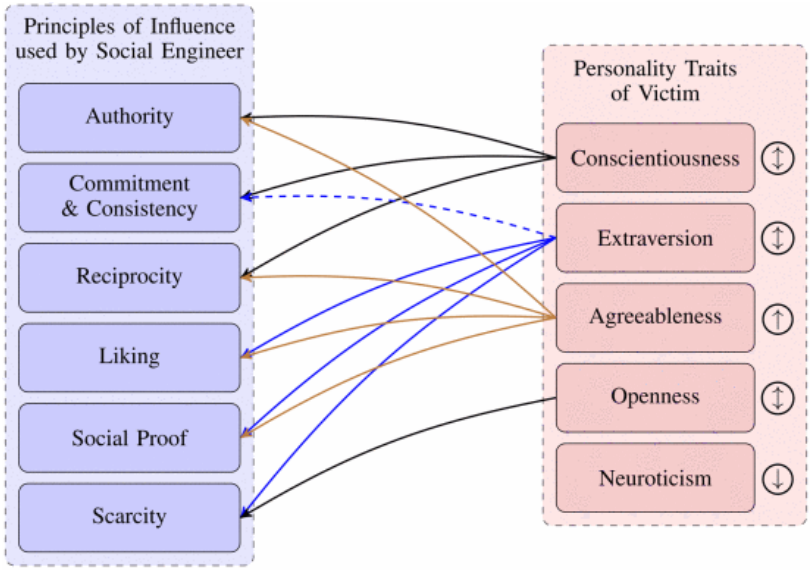


Abbildung 5.1: Anfälligkeit verschiedener Persönlichkeitseigenschaften durch die Prinzipien der Beeinflussung, welche von Social Engineers verwendet werden (die Färbung der Pfeile ist außer Acht zu lassen; gestrichelte Linien weisen auf eine negative Korrelation hin). Entnommen aus **[26]**.

Gewissenhaftigkeit erhöht die Empfänglichkeit für Autorität, Engagement/Konsistenz und Reziprozität. Extraversion erhöht die Empfänglichkeit für Sympathie und soziale Anerkennung (soziale Beweise) aufgrund ihrer Verbindung mit Geselligkeit. Hohe Grade der Verträglichkeit korrelieren mit der Tendenz, anderen zu vertrauen und erhöhen die Anfälligkeit für Social Engineering, da sie anfälliger für Überzeugung und Autorität sind und mehr Interesse an sozialer Bestätigung, Reziprozität und Sympathie haben. Offenheit ist mit erhöhter Anfälligkeit für Social Engineering Taktiken verbunden, da sie mit der sozialen Neigung einhergeht, Neues erleben zu wollen. Neurotizismus ist mit Stress und Angst verbunden, was wiederum die Anfälligkeit gegebenenfalls verringern kann **[8, 26]**.

Nach dem DT-Modell haben narzisstische (oder psychopathische) Tendenzen eine Korrelation dazu, den Angreifer einer Social Engineering Attacke zu repräsentieren. Nar-

zissmus zeichnet sich zumeist aus durch hohe Extraversion und hohen Neurotizismus sowie niedrige Verträglichkeit **[8]**.

Insgesamt ist also zu sehen, dass nahezu alle Persönlichkeiten auf gewisse Manipulationstechniken ansprechen. Daher ist also auch nahezu jede Person bei Verwendung eines spezifischen und passenden Prinzips der Beeinflussung manipulierbar.

Kapitel 6

Konklusion

prognose hier ...

Quellenverzeichnis

[1] Madelyn Bacon and Linda Rosencrance. Social engineering. *ComputerWeekly*, Mai 2024.

[2] Barracuda. Spear Phishing: Top Threats and Trends. Technical report, Barracuda, März 2022.

[3] BSI. Social Engineering - der Mensch als Schwachstelle. *BSI*, März 2024.

[4] Bundeskriminalamt. Bundeslagebild Cybercrime. Technical report, BKA, 2011-2023.

[5] Bundeskriminalamt. Social Engineering / CEO-fraud. Technical report, BKA, Oktober 2017.

[6] Fiona Carroll, John Ayooluwa Adejobi, and Reza Montasari. How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. *SN Computer science*, 3(2):170, 2022.

[7] Florian Cramer. Social Hacking, Revisited. *Retrieved Jan*, 20:2011, 2003.

[8] Irina CRISTESCU, Ella Magdalena CIUPERCĂ, and Carmen Elena CÎRNU. Exploiting personality traits in social engineering attacks. *Romanian Journal of Information Technology & Automatic Control/Revista Română de Informatică și Automatică*, 32(1), 2022.

[9] Brian Cusack and Kemi Adedokun. The impact of personality traits on user's susceptibility to social engineering attacks, 2018.

[10] Jesse Damiani. A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. *Forbes*, September 2019.

[11] Hiep Dang. The origins of social engineering. *McAfee security journal*, 1(1):4–9, 2008.

[12] Emeka Dr. Ejikeme and Ronald Brandon. Social Engineering: The Manipulated Insider, Januar 2024.

[13] ENISA. What is "Social Engineering"? *ENISA*, Februar 2024.

[14] Lukas Feiler. Threat Update: Social Engineering, September 2006.

[15] Ana Ferreira, Lynne Coventry, and Gabriele Lenzini. Principles of persuasion in social engineering and their use in phishing. In *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3*, pages 36–47. Springer, 2015.

[16] Pablo L. Gallegos-Segovia, Jack F. Bravo-Torres, Víctor M. Larios-Rosillo, Paúl E. Vintimilla-Tapia, Iván F. Yuquilima-Albarado, and Juan D. Jara-Saltos. Social engineering as an attack vector for ransomware. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, pages 1–6, 2017.

[17] Rūdolfs Kalniņš, Jānis Puriņš, and Gundars Alksnis. Security Evaluation of Wireless Network Access Points. *Applied Computer Systems*, 21(1):38–45, 2017.

[18] Mahmoud Khonji, Youssef Iraqi, and Andrew Jones. Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, 15(4):2091–2121, 2013.

[19] Kanzlei Kotz. Datendiebstahl und Datenhehlerei: Strafrechtliche Folgen und Handlungsmöglichkeiten.

[20] Amade Nyirak. The attack cycle - security through education, Januar 2022.

[21] ProofPoint. What is social Engineering? *ProofPoint US*, April 2024.

[22] Ionos Redaktion. Social engineering, November 2023.

[23] Fatima Salahdine and Naima Kaabouch. Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 2019.

[24] IBM Security. Cost of a Data Breach Report. Technical report, IBM Security, 2023.

[25] Marketing Team. The “Five Agonies” of Social Engineering Cyber Attacks | GRaphus, September 2023.

[26] Sven Uebelacker and Susanne Quiel. The Social Engineering Personality Framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust*, pages 24–30, Juli 2014.

[27] undergroundwires. Certified ethical hacker in bullet points, 2021.

[28] Verizon. 2012 Data Breach Investigations Report. Technical report, Verizon, 2012.

[29] Verizon. 2022 Data Breach Investigations Report. Technical report, Verizon,

2022.

[30] Verizon. 2024 Data Breach Investigations Report. Technical report, Verizon, 2024.

[31] Janine Willis and Alexander Todorov. First impressions: Making up your mind after a 100-ms exposure to a face. *Psychological science*, 17(7):592–598, 2006.