Social Engineering

Silas A. Kraume

22. Juni 2024

Inhaltsverzeichnis

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 prominäntesten Beispielen ist das Trojanische Pferd[1][8, 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 [12, 16, 4].

In 2016 erklärte Cyence, ein Cybersicherheits-Analyseunternehmen, 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 Bangladesh 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 Geld-überweisungen 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

[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

Energieunternehmen durchzuführen, indem mit deepfake Technlogie der CEO der Firma imitiert wurde. Die Audiodaten waren ausreichend authentisch, sodass die Angreifer einen Angestellten davon überzeugen konten eine Überweisung in Höhe von 243.000 Dollar zu tätigen.

Heutzutage verwenden die meisten Cyber-Angriffe eine Form des Social Engineerings [9, 5]. Diese Form von Cyber Angriffen richtet sich nicht nur gegen Unternehmen und Regierungsinstitutionen, sondern auch gegen Individuen (insbesondere bezüglich Identitätsdiebstahl) [19, 21].

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 Überblich 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 Defintion des Wortes 'Social Engineering' (engl. 'soziale Manipulation') handelt es sich um eine zwischenmenschliche Beeinflussung durch diverse psychologische Tricks zwecksgemäß 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 [9, 4].

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 [3].

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

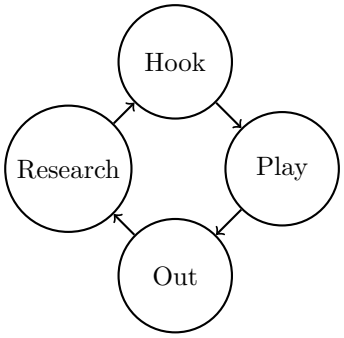
konkreter als 'Social Hacking' definiert [6, 15].

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



[16, 14, 11]

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 [16, 14, 11].

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 100ms[1] aus, um über Attraktivität, Sympathie, Vertrauenswürdigkeit, Kompetenz und Aggressivität zu urteilen [23], weshalb der erste Eindruck bei gewissen Social Engineering Taktiken elementar ist [16, 14, 11].

[1] Millisekunden

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, oder eine sicherheitskritische Aktion auszuführen [16, 14, 11].

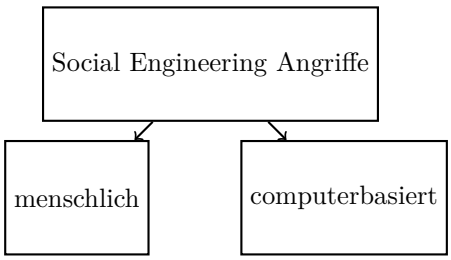
Out

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 [16, 14, 11].

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:

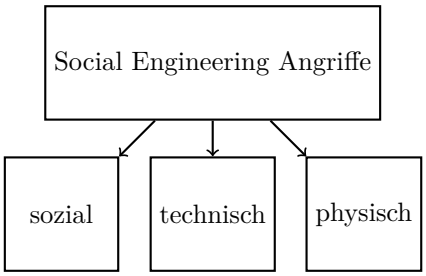
- 1) menschlich
- 2) computerbasiert



[9, 16]

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

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



[16]

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

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 [16, 9].

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 potentiellen Opfern in kürzester Zeit zu erreichen [16, 9].

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 [16, 12]. „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“[4].

soziale Angriffe

Bei sozialen Angriffen wird 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 [16].

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 [16].

2.2.3 Techniken

Es ist nahezu unmöglich einen vollständigen Überblich 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:

[3] darunter zählen auch Smartphones oder anderweitige computerähnliche Geräte

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 dem Namen eines Elternteils oder Haustieres. Solche Informationen sind oft unscheinbar, können allerdings ein immenses Sicherheitsrisiko darstellen, etwa im Kontext von Sicherheitsfragen beim Login in einen Account. Die am weitesten verbreitete Methode des Phishings ist das simple Verschicken vorgefertigter E-Mails an zahlreiche Individuen [16, 13].

Phishing Angriffe lassen sich in weitere Unterkategorien einteilen. Darunter liegen zum Beipsiel 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 [16].

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 [22].

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 Symphatie 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 Login 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 [9, 16].

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 erkären Angreifer selbstweusst, 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 [16].

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 Premien 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 infinzierten 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 [9, 16, 11] 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 ds 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 [9].

Reverse Social Engineering

Reverse Social Engineering Angriffe lassen ihre Opfer glauben, es gäbe ein (technisches) Problem, oder inszenieren einen tatsächlichen Schaden, wenn sie bei-

spielsweise 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 [16]. 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 potentielle 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 Antiviren Programm, welches im selbigen Pop-Up Fenster angeboten wird. Insgesamt lassen sich derartige Angriffe primär eingebunden in Webseiten finden, durch (Browser-) Plugins 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 ge-

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

sagt haben.

[16, 20]

Kapitel 3

Maßnahmen

”Proper identification and authentication processes, policies and trainings should be in place to circumvent such attacks.”[9] bzg Pretexting

SSecurity policies such as an air gap and the blocking of non-authorised software and hardware will thwart most attempts, though staff should also be reminded not to trust unknown sources.”[9] bzg Baiting

”Quid pro quo attacks are relatively easy to detect given the asymmetrical value of the information compared to the compensation, which is opposite for the attacker and the victim. In these cases the best countermeasure remains the victim integrity and ability to identify, ignore and report.”[9] bzg Quid pro quo

Äccess to non public areas should be controlled by access policies and/or the use of access control technologies, the more sensitive the area the stricter the combination. Th[e] obligation to wear a badge, the presence of a guard and actual anti-tailgating doors such as mantraps with RFID access control should be sufficient to deter most attackers.”[9] bzg Tailgating

3.1 Erkennung

”n order to detect and prevent these attacks, a number of techniques have been proposed. A list of defense procedures for social-engineering attacks include: encouraging security education and training, increasing social awareness of social-engineering attacks, providing the required tools to detect and avoid these attacks, learning how to keep confidential information safe, reporting any suspected activity to the security service, organizing security orientations for new employees, and advertising attacks’ risks to all employees by forwarding sensitization emails and known fraudulent emails [40].”[16]

3.2 Vorbeugung

Ïn order to detect attacks via phone calls, it is necessary to verify the source of calls using a recording contacts' list, being aware of unexpected and unsolicited calls, asking to call back, or asking questions with private answers to check the caller's identity. The most effective way to stop these attacks is by not answering these calls. For help desk attacks, assigning PINs to known callers prevents malicious calls [41]. The help desk is required to stick to the scope while performing a call request. For email-based attacks, some companies use the honeypot email addresses, also called spamtraps, to collect and publish the spams to employees. When an email is sent from one of the spamtraps list, the server considers it as malicious and bans it temporarily. Other procedures that can be done include: verifying emails' sources before clicking on a link or opening an attachment, examining the emails header, calling the known sender if suspicious, and discarding emails with quick rich or prize-winning announcements. For phishing attacks, anti-phishing tools have been proposed to blacklist and block phishing websites. Examples of these tools are McAfee anti-phishing filter, Microsoft phishing filter, and Web sense [42,43]. In [44], the authors proposed to teach students how the spear phishing attack is performed by learning by doing. They developed a framework in which students learn how phishing emails work by performing attacks on a virtual company. After gathering all the possible information from the company's website, the students launched phishing emails to simulated employees and then scanned all the received emails to decide about their nature. In [45], the authors proposed a detection technique based on machine learning algorithms. This technique is based on unsupervised learning, in which there is no past knowledge about the observed attacks. The authors compared the performance of six machine learning algorithms for detecting phishing attacks in terms of speed, reliability, and accuracy: support vector machine, biased support vector machine, artificial neural networks, scaled conjugate gradient, and self-organizing map. They showed that the support vector machine algorithm achieves better results compared to the other algorithms. In [22], the authors proposed a method to detect the credential spear phishing attacks in enterprise sittings. The proposed detection method, called anomaly detection (DAS), performs by analyzing the potential characteristics to the spear phishing attacks in order to derive a number of features used by the attacker. It is a non-parametric anomaly scoring method used for ranking alerts. For tailgating attacks, they may be prevented by training employees to never give access to someone without badge with no exceptions and requiring locks and IDs for all employees [35]. For shoulder surfing attacks, individuals are required to be more aware of what is around them, including persons or cameras when they enter sensitive information. For dumpster diving attacks, sensitive discarded documents and materials must be completely destroyed using shredders, memory devices must be secured or erased, and important files must be locked securely and not left for easy access. Trojan-based attacks may be prevented by refusing to let someone use other people personal or work computers, using an antivirus for USB scanning before opening it and following the antivi-

rus instructions and warning, examining any unexpected mailing packages, and not picking up and using found digital medias. To prevent fake software attacks, individuals need to check carefully the screen and verify if the software window is legitimate as real websites have always something special than the fake ones. Anti-virus may be limited by human unawareness; they may catch these attacks and send warnings, which most users ignore by closing the window and move on. Other preventions can be considered including verifying if the website has the https logo, not click before examining the URL, and update regularly the computer's operating system and security software. Some security organizations encourage companies to adopt the defense in depth strategy to monitor their network and prepared themselves for possible attacks while neglecting the human aspect. In [46], the authors proposed to identify the requirements of an anti-social engineering attacks framework capable of analyzing and mitigating attack risks. They developed a new layered defense technique named Social Engineering Centered Risk Assessment (SERA). SERA starts by identifying the critical assets to evaluate the company's information for the next step. Then, each asset is placed in a container and the corresponding social engineering attack vectors are identified. Probability of attack realization is driven by local security experts and the risk analysis is obtained. In [47], the authors proposed a flow whitelisting approach to enhance the network security inside companies. The flow whitelisting approach aims at identifying legitimate traffic from malicious traffic coming to the company's network. Four properties are used to identify these whitelists: address of the client, address of the server, port number of the server, and the protocol used for the traffic transport. The proposed approach is performed by capturing the network's traffic at a predefined period of time and aggregating that traffic into flows when that traffic is identified as legitimate. It is based on learning to distinguish legitimate traffic from malicious traffic and generating alarms in case of an observed malicious traffic. In [34], the authors proposed a new approach called TabShots to distinguish between legitimate pages from malicious pages. The TabShots is an extension installed in the browser that compares the appearance of the webpages and highlights any observed changes to excite the attention of the user before proceeding. In [48], the authors discussed the problem of formalizing actions that are a result of social engineering attacks. They proposed to model these actions through probabilities and graphical models such as Bayesian models. They analyzed the user's profile to estimate its vulnerabilities and psychological features. Estimating the protection of a user profile against an attack is obtained through four elements: psychological features (F), critical vulnerabilities (V), attack's actions (A), and user's accountability at successful attacks (C). In [49], the authors proposed to analyze the human's behaviors and perceptions to cope with social engineering attacks. They aim at understanding human weaknesses in being deceived easily by attackers and defining factors and features that influence the human abilities to detect attacks. They also aim at identifying vulnerable users by building a user profile that focuses on security education and training programs. In [50], the authors evaluated the susceptibility to cybersecurity attacks in cooperative organizations in order to assess the consciousness of social engineering attacks

of employees. By performing an attack against the organization based on the available information on the organization's website, employees reacted to the attack in different ways with different awareness degrees. These results were then benchmarked to establish the organization awareness in terms of ignoring the attack and being tricked or recognizing the attack and appropriately responding to it. Attack victims were then directed to intensive training. In [51], a social engineering awareness program (SEAP) was developed for schools aiming at increasing students' awareness by providing significant education and training in early age."[16]

"Nevertheless, the single most efficient countermeasure to social engineering attacks remains common sense. In this light, ENISA recommend the following:

frequent awareness campaigns: posters, presentations, emails, information notes; staff training and exercising; penetration tests to determine an organisation's susceptibility to social engineering attacks, reporting and acting upon the results."[9]

Üse multi-factor authentication. Multi-factor authentication, also called MFA, two-factor authentication, and two-step verification, provides an additional layer of security above and beyond username and password, such as an authentication code, thumb print, or retinal scan."[2]

"Train staffers to recognize and report attacks. "[2]

3.3 Milderung

"Human-based attacks are sophisticated and hard to detect, making their mitigation necessary. Mitigating techniques for social engineering attacks aim at decreasing the attacks' impact on the individuals or the companies [52]. They aim at saving what can be saved after a human is already attacked or a company's system is already hacked. The cyber security entity needs to minimize the loss as much as possible by defining security actions in case of emergency. For instance, building a corporate security culture among the company's employees is a mitigation technique against the attacks targeting companies or groups of individuals [53]. This positive culture helps the attack's victim not feel ashamed of being manipulated as the social engineer exploits the misplaced trust and not because the victim is unintelligent or foolish."[19]

"Gehen Sie verantwortungsvoll mit Sozialen Netzwerken um. Überlegen Sie genau, welche persönlichen Informationen Sie dort offenlegen, da diese von Kriminellen gesammelt und für Täuschungsversuche missbraucht werden können."[4]

"Geben Sie in privaten und beruflichen Sozialen Netzwerken keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit preis."[4]

"Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Te-

lefon oder E-Mail mit. Banken und seriöse Firmen fordern ihre Kunden nie per E-Mail oder per Telefon zur Eingabe von vertraulichen Informationen auf."[4]

"3-Sekunden-Sicherheits-Check."[4] – > Äbsender, Betreff und Anhang sind hierbei drei kritische Punkte, die vor dem Öffnen jeder E-Mail bedacht werden sollten."

SSollte eine Reaktion zwingend erforderlich sein, vergewissern Sie sich durch einen Anruf bei der Absenderin oder dem Absender, dass es sich um eine legitime E-Mail handelt."[4]

Kapitel 4

Konsequenzen

4.1 Motivation

Das primäre Motiv von Cyber-Kriminellen ist finanziell. 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 [17].

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 [18]. 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.

Kapitel 5

Psychologie

5.1 psychologische Grundlagen

Ës wurden 6 soziale Einfallstore und Mental Shortcuts identifiziert: o Hilfsbereitschaft o Leichtgläubigkeit o Neugier o (Wunsch nach) Anerkennung o Druck o Angst. "[3]

Ës gibt keinen Abwehrzauber gegen Social-Engineering, denn dabei handelt es sich um Verhalten, das in der Regel sozial erwünscht ist. Technische Maßnahmen sind nicht in der Lage, derartige Vorfälle zu verhindern, da es sich um ein soziales Problem handelt. Zur Abwehr wird die Fähigkeit benötigt, soziale Beziehungen und Kontexte zu deuten. Es ist notwendig, in Organisationen ein Sicherheitsbewusstsein im Rahmen einer Sicherheitskultur zu schaffen"[3]

"Prognostisch bleibt zu befürchten, dass SE-Fälle in Zukunft eher ansteigen als abnehmen werden und die Aufklärung problematisch bleibt. Gründe hierfür sind insbesondere:

Die Betrügereien werden weiterhin und zunehmend aus dem Ausland oder von nicht zu identifizierenden Rechnern oder Personen begangen. Dadurch sinkt das Entdeckungsrisiko. Scham oder die Angst vor Reputationsverlust kann die Anzeigebereitschaft hemmen. Die Aussicht auf immense (schwer abzuschöpfende) Gewinne erhöht den Tatanreiz. Die Verfügbarkeit relevanter offener Informationen, die für einen SE-Angriff genutzt werden können, wird eher ansteigen als abnehmen. Dadurch werden Manipulationen erleichtert. Der Druck auf einzelne Mitarbeiter in der heutigen Arbeitswelt steigt eher als dass er sinkt und der notwendige Rückhalt/ das Vertrauen in die Organisation, sich vermeintlichen Anweisungen zunächst zu widersetzen, ist nicht immer vorhanden. Die Ëuropäisierung des Betruges"wir nicht adäquat mit der Europäisierung der Strafverfolgung beantwortet und "die internationale Rechtshilfe ist in hohem Maße

defizitär”.”[3]

5.2 menschliche Beeinflussung

5.2.1 Einflussprinzipien

Ein Angreifer kann die Entscheidungsfähigkeit zu seinem Vorteil beeinflussen, denn Menschen reagieren oftmals mit automatisiertem Sozialverhalten [3]. Der Psychologe Robert Cialdini entwickelte die sechs Prinzipien der Überzeugung („Six Principles of Persuasion“), welche in weitreichenden Studien demonstiert wurden[1][19]. 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 Gefolgsamkeit bei Anderen [19, 10, 3].

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 [19, 10, 3].

Reciprocity

Das Prinzip der Gegenseitigkeit (engl 'Reciprocity') beruht auf der fundamentalen Tendenz, dass sich Menschen dazu verpflichtet fühlen, Gefallen oder Geschenke zu erwiedern. Dieses Prinzip ist derartig stark, dass die Erwiederung vehementer ausfallen kann, als den initial erhaltenen Gefallen [19, 10, 3].

Liking

Aufgrund des grundlegenden Motivs, soziale Beziehungen aufzubauen und aufrechtzuhalten, führen Menschen die Anfragen Anderer eher aus, wenn sie diese

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

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 [19, 10, 3].

Social Proof

Das Prinzip des sozialen Beweises (engl. 'social proof') ist ein Phänomen, dass in der Psychologie als 'informativer sozialer Einfluss' bekannt ist. Es geht um eine mächtige Überzeugungstaktik, die ausnutzt, dass Menschen eine natürliche (bzw. primitive) Tendenz haben, dem Beispiel Anderer folgen zu wollen, um sozial akzeptiert zu werden [19, 10, 3].

Scarcity

Das letzte Prinzip der Überzeugung ist die Knappheit (engl. 'scarcity'), und beschreibt die Tatsache, dass Menschen einer geringeneren 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 verfügbar sind. So wirken Informationen, die einem im Geheimen anvertraut werden, oft spektakulärer [19, 10, 3].

5.2.2 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. 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:

5.2.3 Anfälligkeit für Social Engineering

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

Tabelle 5.1: Charakteristiken der OCEAN-Modell Persönlichkeitseigenschaften [7]

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.

Kapitel 6

Konklusion

prognose hier ...

Literaturverzeichnis

[1] Madelyn Bacon and Linda Rosencrance. Social engineering, 5 2024.

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

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

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

[5] 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.

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

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

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

[9] ENISA. What is SSocial Engineering"? ENISA, Februar 2024.

[10] 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.

[11] 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.

[12] Rūdolfs Kalniņš, Jānis Puriņš, and Gundars Alksnis. Security evaluation of wireless network access points. Applied Computer Systems, 21(1):38–45, 2017.

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

[14] Amade Nyirak. The attack cycle - security through education, 1 2022.

[15] Ionos Redaktion. Social engineering, 11 2023.

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

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

[18] Marketing Team. The "Five Agonies" of Social Engineering Cyber Attacks | GRaphus, 9 2023.

[19] 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.

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

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

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

[23] 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.