Social Engineering

Silas A. Kraume

June 19, 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 prominäntesten Beispielen ist das Trojanische Pferd[1] **[8, 2]**.

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 **[11, 13, 5]**. Diese Form von Angriffen richtet sich nicht nur gegen Unternehmen und Regierungsinstitutionen, sondern auch gegen Individuen (insbesondere bezüglich Identitätsdiebstahl) **[16, 17]**.

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. Heutzutage verwenden die meisten Cyber-Angriffe eine Form des Social Engineerings **[9, 6]**.

Social Engineering stellt also eine allgemeine Gefahr für jeden dar, welshalb 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 untermauert die Vehemenz des Themas, indem die Konsequenzen erfolgreicher Angriffe

[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

vermittelt werden. Darauffolgend analysieren *Kapitel* 4 und *Kapitel* 5 Social Engineering hinsichtlich der Forschungsfrage auf sowohl technische und psychologische Weise, und 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, 5]**.

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 **[4]**.

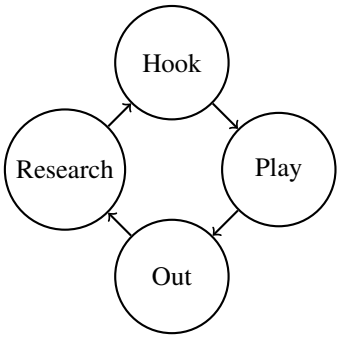
In Bezug zu IT-Systemen und digitalen Daten wird Social Engineering auch konkreter als ”Social Hacking” definiert **[7, 12]**.

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



[13, 1, 10]

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 **[13, 1, 10]**.

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 **[19]**, weshalb der erste Eindruck bei gewissen Social Engineering Taktiken elementar ist **[13, 1, 10]**.

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 **[13, 1, 10]**.

[1] Millisekunden

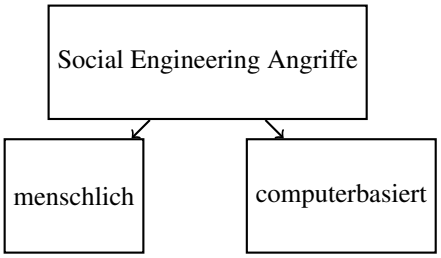
Out

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 **[13, 1, 10]**.

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:

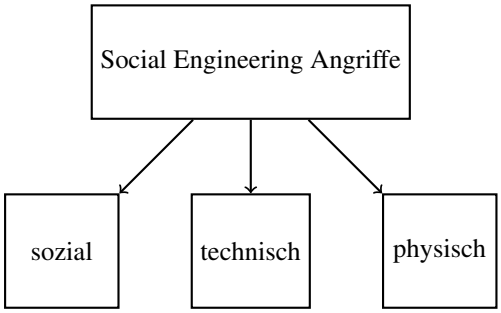
- 1) menschlich
- 2) computerbasiert



[9, 13]

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

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



[13]

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 **[13, 9]**.

[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 potentiellen Opfern in kürzester Zeit zu erreichen **[13, 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 **[13, 11]**. "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"**[5]**.

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 **[13]**.

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 **[13]**.

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:

"Pretexting This technique involves the use of a pretext - a false justification for a specific course of action - to gain trust and trick the victim. Example: the attacker claims to work for IT support and requests the target's password for maintenance purposes."[9]

"Pretexting Attacks Pretexting attacks consist of inventing fake and convincing scenarios in order to steal a victim's personal information. They are based on pretexts that make the victim believe and trust the attacker [27]. The attack is performed via phone calls, emails, or physical media. Attackers use publishing information on phone books, public web pages, or conferences where collaborators in the same field meet to carry out their attack. The pretext may be an offer to perform a service or to get a job, asking

[3] darunter zählen auch Smartphones oder anderweitige computerähnliche Geräte

about personal information, helping a friend to get access to something, or winning a lottery."[13]

"Baiting Baiting involves luring the victim into performing a specific task by providing easy access to something the victim wants. Example: a USB flash drive infected with a keylogger and labelled "My private pics" left on the victim's doorstep."[9]

"Baiting Attacks Baiting attacks, also called road apples, are phishing attacks that invite users to click on a link to get free stuff. They act like trojan horses where the attack is performed by exploiting unsecured computer materials such as storage media or USB drives containing malware in a coffee shop to be found by victims. When the victims plug the USB drive into their computers, the drive acts like a real world trojan horse and attacks the computer. This attack performs malicious actions in the background without being noticed by the victims. In [7], the authors described a baiting attack named controller area network (CANDY) to be launched as a trojan horse in the infotainment system of automotive systems. This attack impacts the security capabilities of the vehicle by manipulating the communication between the driver and the vehicle. It is performed by recording the driver's voice which lets the attacker remotely access the victim's vehicle via back door, collect information about the vehicle circulation, and control the operation of the vehicle."[13]

"Quid pro quo Quid Pro Quo, "something for something" in Latin, involves a request for information in exchange for a compensation. Example: the attacker asks the victim's password claiming to be a researcher doing an experiment, in exchange for money."[9]

piggybacking: "Tailgating Tailgating is the act of following an authorised person into a restricted area or system. Example: the attacker, dressed as an employee, carries a large box and convinces the victim, who is an authorised employee entering at the same time, to open the door of the data-centre using the victim's RFID pass."[9]

"Tailgating Attacks Tailgating attacks, also called piggybacking or physical access, consist of accessing an area or building by following someone who has the security clearance to that place. They allow attackers access unauthorized buildings. For example, attackers ask a victim to hold the door open because they forgot their company' ID card or RFID (radio-frequency identification) card. They can als borrow a computer or cellphone to perform malicious activities such as installing malware software [14]. For instance, RFID cards attacks are one of the most used attacks to access forbidden spaces for malicious purposes. Due to their wide utilization and low cost, RFID systems are considered as the most emerging technology used by companies to control the access to their facilities. Despite their advantages, they have vulnerabilities that can be exploited to cause serious security issues to companies. RFID attacks can be performed over several layers of the interconnection system model (ISO) [28]. For instance, at the physical layer, the RFID devices and the physical interface are targeted to manipulate an RFID communication. These attacks can cause temporary or permanent damage of the RFID cards. At the network layer level, the attacker manipulates the RFID network such as the communication between the RFID entities and data exchange between these

entities."[13]

"Reverse Social Engineering Attacks Reverse social engineering attackers claim to solve a network's problem. This involves three main steps: causing a problem such as crashing the network; advertising that the attacker is the only person to fix that problem; solving the problem while getting the desired information and leaving without being detected"[13]

Pop-Up Windows Pop-up window attacks refer to windows appearing on the victim's screen informing the connection is lost [35]. The user reacts by re-entering the login information which runs a malicious program already installed with the window appearance. This program remotely forwards back the login information to the attacker. For instance, pop-ups can be alert messages showing up randomly for online advertising to lure the victim in clicking on that window. Pop-ups also can be fake messages alerting about a virus detection in the victim's computer. The pop up will prompt the victim to download and install the suggested anti-virus software to protect the computer. They can also be fake alerts stating that the computer storage is full and that it needs to be scanned and cleaned to save more space [35]. The victim panics and reacts quickly in order to fix the problem, which activates the malware software carried in the pop-up window."[13]

"Phone/Email Scams Attacks For this type of attacks, the attacker contacts the victim via phone or email seeking specific information or promising a prize or free merchandise. They aim at influencing the victim to break the security rules or to provide personal information. Moreover, cellphone-based attacks can be performed via calls and via short messaging services (SMS) or text messages, which are known as SMSishing attacks [35]. SMSishing attacks consist of sending fraudulent messages and texts via cell phones to victims to influence them. They are similar to phishing attacks but they are performed in different ways. The efficiency of the SMSishing attacks resides in the fact that victims can carry their cellphones anywhere and anytime. A received text message can include a malware even if it was sent from trusted and known transmitter. The malware works as a background process installing backdoors for attackers to have access to information such as contact list, messages, personal email, photos, notes, applications, and calendar. The scammer can install a root kit to control the cellphone completely [20]."[13]

"Robocalls Attacks Robocall attacks have recently emerged as massive calls coming from computers to targeted persons with known phone numbers. They target cellphones, residential, and work phones. A robocall is a device or computer program that automatically dials a list of phone numbers to deliver prerecorded messages. It is mainly based on voice over the internet protocol (VoIP) to ensure several VoIP functions such as interactive voice response and text to speech [36]. These calls can be about offering or selling services or solving problems. Helping to solve tax problems is a very known example of attack that has risen in intensity in recent years. In general, when a victim answers the call, the phone number is stored in the attacker's database. Even after blocking these calls, attackers' systems call from other numbers. Robocall attacks have become a serious problem in the USA and other countries. The only way

for people to stop these calls is by not answering unknown phone numbers."[13]

"51% of social engineering attacks are phishing"[3] "Microsoft is the most impersonated brand, used in 57% of phishing attacks"[3]

"That leads to a frightening finding: The median time for users to fall for phishing emails is less than 60 seconds. "[18]

Phishing, Baiting, Pretexting, Tailgating, Ransomware, impersonating on help desk, diversion theft, dumpster diving, shoulder surfing, quid pro quo, pup-up windows, robocalls, reverse social engineering, online social engineering, phone social engineering, stealing important documents, fake software, pharming, SMSishing, Whitelisting following ScareWare, Watering-Hole, honeytraps, whaling, smishing, quishing, tishing, vishing, wishing, pharming, snowshoeing, USB Drop

Kapitel 3

Konsequenzen

3.1 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 **[14]**. 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 global eine der 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. Insgesamt sollten 1 Milliarden US-Dollar transferiert werden, wobei es den Angreifern letztendlich nur möglich war, 81 Millionen US-Dollar zu stehlen.

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 **[15]**. 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 4

Maßnahmen

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

”Security 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

”Access 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

4.1 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].”[13]

4.2 Vorbeugung

”In 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 antivirus 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."[13]

”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]

”Use 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.”[3]

”Train staffers to recognize and report attacks. ”[3]

4.3 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.”[16]

”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.”[5]

”Geben Sie in privaten und beruflichen Sozialen Netzwerken keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit preis.”[5]

”Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon oder E-Mail mit. Banken und seriöse Firmen fordern ihre Kunden nie per E-Mail oder per Telefon zur Eingabe von vertraulichen Informationen auf.”[5]

”3-Sekunden-Sicherheits-Check.”[5] – ¿ ”Absender, Betreff und Anhang sind hierbei drei kritische Punkte, die vor dem Öffnen jeder E-Mail bedacht werden sollten.”

”Sollte 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.”[5]

Kapitel 5

Psychologie

”Es wurden 6 soziale Einfallstore und Mental Shortcuts identifiziert: o Hilfsbereitschaft o Leichtgläubigkeit o Neugier o (Wunsch nach) Anerkennung o Druck o Angst. ”[4]

”Der Mensch reagiert auf bestimmte Auslösemerkmale mit automatisiertem Sozialverhalten. Regeln mit solch hoher gesellschaftlicher Durchschlagkraft lassen sich leicht missbrauchen: 12 o Die Regel der Reziprozität (Wechselseitigkeit, d.h. wir müssen uns für erhaltene Gefälligkeiten, Geschenke etc. revanchieren. Auf Zugeständnisse müssen wir mit Zugeständnissen reagieren). Falls aber durch Bewusstheit/ Sensibilität erkannt wird, dass der Gefallen oder das Geschenk in Wirklichkeit nur ein Manöver war, um Vorteile zu erlangen, verliert die Reziprozitätsregel ihre Durchschlagskraft. o Das Kontrastprinzip (Kontraste erscheinen durch eine geschickte Präsentation größer als sie unter anderen Umständen erscheinen würden). o Die Regel des Commitments und der Konsistenz (d.h. den Menschen wohnt ein geradezu zwanghaftes Verhalten inne, in Konsistenz mit ihren früheren Handlungen zu erscheinen - also konsequent zu sein. Wurde eine Entscheidung getroffen, treten intra- und interpsychische Vorgänge in Kraft, die uns dazu drängen, konsistent zu bleiben. In der Sozialpsychologie und dem Marketing arbeitet man daher mit der sog. ”Fuß-in-der-Tür-Taktik”. Man beginnt mit einer kleinen Bitte und arbeitet sich dann zur großen vor oder verändert das Selbstbild des Gegenübers in die gewünscht Richtung. Hat man das Selbstbild einer Person erst einmal in eine neue Rolle manipuliert, tut die Person nahezu alles um mit dem neuen Selbstbild konsistent zu bleiben). Zumeist spürt der Mensch, dass er betrogen oder ausgenutzt werden soll, achtet aber nicht auf dieses ”Bauch-Gefühl”. Durch Awareness-Training kann hier, als Gegenmaßnahme, eingegriffen werden. o Das Prinzip der sozialen Bewährtheit (Das Verhalten anderer wird als richtig angenommen und gegebenenfalls kopiert bzw. adaptiert). o Sympathie (Uns sympathische Menschen können uns eher zu einem bestimmten Verhalten verleiten). Sympathie verstärkt alle anderen eingesetzten Überzeugungstricks. Dazu gehören auch Attraktivität, Ähnlichkeit, gleiche Herkunft, ähnliche Interessen, Schmeicheleien, Sympathiebekundungen, Flirts. o

Autorität (Autoritätssymbole: Titel, Uniform, Luxus). o Knappheit (je knapper eine Ware ist, desto mehr gewinnt sie an Wert). ”[4]

”Es 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”[4]

”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 ”Europäisierung des Betruges” wir nicht adäquat mit der Europäisierung der Strafverfolgung beantwortet und ”die internationale Rechtshilfe ist in hohem Maße defizitär”.”[4]

”The Dual Process Model of Persuasion [19] defines two different ways how we process information: the peripheral route or heuristic processing via intuition (system 1) and the central route via reasoning (system 2) (cf. [18]). Attackers can target both systems.”[16]

”six principles of influence”:[16]

”Authority Most people comply to authorities (cf. Milgram experiments [24]), even if they persuade them to act against their beliefs and ethics. It also works for symbols of authority, e.g. uniforms, badges, and titles or in telephone conversations where authority can easily be claimed. Two types of authority exist: one based on expertise and one relying on the relative hierarchical position in an organisation or society [19].

Commitment & Consistency Commitment is an act of stating what one person thinks he is and does, while consistency makes that same person behave consistently according to his or her commitments and beliefs revealing a a highly successful influence principle [19].

Reciprocity A strong social norm that obliges us to repay others for what we have received from them. Relationships rely and societies are built on it. Reciprocity helps establishing trust with others and refers to our need for equity. The power of reci-

procity can be so high that the target would return an even greater favour than what was received.

Liking 'If you make it plain you like people, it's hard for them to resist liking you back" [25]. We prefer to comply with requests from people we know and like due to the fundamental motive to create and maintain social relationships. Perceived similarity enhances compliance as it can originate from a potential friend. These can be as superficial as shared names or birthdays.

Social Proof Besides adapting beliefs and behaviour of people around in order to become socially "accepted", social proof also implies higher trust levels towards people who share alike opinions, especially in ambiguous situations.

Scarcity We assign more value to less available opportunities due to a short-cut from availability to quality. Moreover, if something becomes scarce, we sense losing freedoms. Reactance Theory [26] suggests that we respond to scarcity by wanting to have what has become rare more than before. Even information with limited access persuades better."[16]

"In psychology, personality is defined as a person's relatively stable feelings, thoughts, and behavioural patterns. These are predominantly determined by inheritance, social and environmental influence, and experience, and are therefore unique for every individual [27]."[16]

"The FFM consists of five broad, empirically derived personality dimensions or traits, which split in several subtraits and are used across research areas with high validity: these traits are defined as Conscientiousness which focus on competence, self-discipline, self-control, persistence, and dutifulness as well as following standards and rules. Extraversion comprises positive emotions, sociability, dominance, ambition, and excitement seeking. Agreeableness includes compassion, cooperation, belief in the goodness of mankind, trustfulness, helpfulness, compliance, and straightforwardness. Openness to experience encompasses as a preference for creativity, flexibility' fantasy as well as an appreciation of new experiences and different ideas and beliefs. Neuroticism describes the tendency to experience negative emotions, anxiety, pessimism, impulsiveness, vulnerability to stress, and personal insecurity."[16]

Kapitel 6

Konklusion

prognose hier ...

Quellenverzeichnis

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

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

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

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

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

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

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

[10] 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.

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

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

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

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

[15] Marketing Team. The “Five Agonies” of Social Engineering Cyber Attacks — GRaphus, 9 2023.

[16] 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.

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

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

[19] 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.