



Technische  
Hochschule  
Nürnberg

Fakultät Informatik

# Gefahren im Metaverse: Social Engineering als Grundlage für Angriffe im Metaverse

Bachelorarbeit im Studiengang Wirtschaftsinformatik

vorgelegt von

Andre Schindler

Matrikelnummer 327 2457

Erstgutachter: Prof. Dr. Ronald Petrlic

Zweitgutachter: Prof. Dr. Peter Rausch

Dieses Werk einschließlich seiner Teile ist **urheberrechtlich geschützt**. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Autors unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen sowie die Einspeicherung und Verarbeitung in elektronischen Systemen.

Hinweis: Diese Erklärung ist in alle Exemplare der Abschlussarbeit fest einzubinden. (Keine Spiralbindung)

## Prüfungsrechtliche Erklärung der/des Studierenden

Angaben des bzw. der Studierenden:

Name:

Vorname:

Matrikel-Nr.:

Fakultät:

Studiengang:

Semester:

### Titel der Abschlussarbeit:

Ich versichere, dass ich die Arbeit selbständig verfasst, nicht anderweitig für Prüfungszwecke vorgelegt, alle benutzten Quellen und Hilfsmittel angegeben sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

---

Ort, Datum, Unterschrift Studierende/Studierender

### Erklärung der/des Studierenden zur Veröffentlichung der vorstehend bezeichneten Abschlussarbeit

Die Entscheidung über die vollständige oder auszugsweise Veröffentlichung der Abschlussarbeit liegt grundsätzlich erst einmal allein in der Zuständigkeit der/des studentischen Verfasserin/Verfassers. Nach dem Urheberrechtsgesetz (UrhG) erwirbt die Verfasserin/der Verfasser einer Abschlussarbeit mit Anfertigung ihrer/seiner Arbeit das alleinige Urheberrecht und grundsätzlich auch die hieraus resultierenden Nutzungsrechte wie z.B. Erstveröffentlichung (§ 12 UrhG), Verbreitung (§ 17 UrhG), Vervielfältigung (§ 16 UrhG), Online-Nutzung usw., also alle Rechte, die die nicht-kommerzielle oder kommerzielle Verwertung betreffen.

Die Hochschule und deren Beschäftigte werden Abschlussarbeiten oder Teile davon nicht ohne Zustimmung der/des studentischen Verfasserin/Verfassers veröffentlichen, insbesondere nicht öffentlich zugänglich in die Bibliothek der Hochschule einstellen.

Hiermit  genehmige ich, wenn und soweit keine entgegenstehenden Vereinbarungen mit Dritten getroffen worden sind,  
 genehmige ich nicht,

dass die oben genannte Abschlussarbeit durch die Technische Hochschule Nürnberg Georg Simon Ohm, ggf. nach Ablauf einer mittels eines auf der Abschlussarbeit aufgebrachten Sperrvermerks kenntlich gemachten Sperrfrist

von Jahren (0 - 5 Jahren ab Datum der Abgabe der Arbeit),

der Öffentlichkeit zugänglich gemacht wird. Im Falle der Genehmigung erfolgt diese unwiderruflich; hierzu wird der Abschlussarbeit ein Exemplar im digitalisierten PDF-Format auf einem Datenträger beigefügt. Bestimmungen der jeweils geltenden Studien- und Prüfungsordnung über Art und Umfang der im Rahmen der Arbeit abzugebenden Exemplare und Materialien werden hierdurch nicht berührt.

---

Ort, Datum, Unterschrift Studierende/Studierender

**Datenschutz:** Die Antragstellung ist regelmäßig mit der Speicherung und Verarbeitung der von Ihnen mitgeteilten Daten durch die Technische Hochschule Nürnberg Georg Simon Ohm verbunden. Weitere Informationen zum Umgang der Technischen Hochschule Nürnberg mit Ihren personenbezogenen Daten sind unter nachfolgendem Link abrufbar: <https://www.th-nuernberg.de/datenschutz/>



# Anleitungen und Tests

## 1 Anleitungen

„Elizitieren“

**Glossar** Glossar erstellen <https://www.lektorat-bachelorarbeit.de/glossar-erstellen/#:~:text=In%20einem%20Glossar%20sammelt%20man, die%20Erstellung%2C%20beantwortet%20dieser%20Text>.

It is possible to reference glossary entries as Immersion as an example.

**Bilder einfügen** nach paragraph muss was was stehen bevor das bild kommt

Einführung	13	14	Einführung	15
Jahrzehnte altes Science-Fiction-Konzept, das Metaverse, das darauf hinzuweisen schien, dass die Zukunft wirklich angekommen war.			nehmen profitabler, ihre Kunden glücklicher und ihre Konkurrenten weniger bedrohlich machen würde. Vor dem Börsengang von Roblox im Oktober 2020 tauchte der Begriff „Metaverse“ nur fünfmal in den Unterlagen der US-Börsenaufsichtsbehörde auf. <sup>3</sup> Ein Jahr später wurde er bereits mehr als 260 Mal erwähnt. Im selben Jahr verzehnte Bloomberg, ein Softwareunternehmen, die Finanzdaten und -informationen für Investoren bereitstellt, mehr als tausend Berichte, in denen das Wort „Metaverse“ vorkam. Im gesamten Jahrzehnt davor waren es nur sieben.	
In Juli 2021 sagte der Gründer und CEO von Facebook, Mark Zuckerberg, „In dem nächsten Kapitel unseres Unternehmens werden wir uns von einem Unternehmen, das in erster Linie als soziales Medium wahrgesehen wird, zu einem Unternehmen des Metaversums wandeln. Und natürlich werden gesammelte Avatare, die wir uns und mit den App-leisten, die die Menschen für uns nutzen, direkt zu diesen Vierern haben.“ <sup>4</sup> Kurz darauf kündigte Zuckerberg öffentlich eine Abteilung in seinem Unternehmen an, die sich auf das Metaverse konzentriert, und ernannte den Leiter der Facebook Reality Lab – einer Abteilung, die an verschiedenen futuristischen Projekten wie Oculus VR (virtuelle Realität), AR-Brillen (erweiterte Realität) und Brain-to-Machine-Schnittstellen arbeitet – zum Chief Technology Officer. Im Oktober 2021 verkündete Zuckerberg, dass Facebook seinen Namen in Meta Platforms <sup>5</sup> ändern würde, der den Wandel zu diesem „Metaverse“ widerspiegeln sollte. Zur Überraschung vieler Facebook-Aktiengäste erklärte Zuckerberg ebenfalls, dass seine Investitionen in das Metaverse von über 10 Milliarden Dollar allein im Jahr 2021 das Betriebsergebnis belasten werden, wobei gleichzeitig davor gewarnt wurde, dass diese Investitionen noch mehrere Jahre lang steigen werden.		Das Interesse am Metaverse war dabei nicht auf westliche Nationen und Unternehmen beschränkt. Im Mai 2021 beschrieb Chinas größtes Unternehmen, der Internet-Gaming-Riese Tencent, öffentlich seine Vision des Metaverse und nannte es „Hyper Digital Reality“. Nur einen Tag später gab das südkoreanische Ministerium für Wissenschaft und IKT (Informations- und Kommunikationstechnologie) die (südkoreanische) Metaverse-Allianz <sup>6</sup> bekannt, die über 450 Unternehmen umfasst, darunter SK Telecom, Woori Bank und Hyundai Motor. Anfang August schloss der südkoreanische Spielegigant Krafton, Hersteller von <i>PlayerUnknown's Battlegrounds</i> (auch bekannt als PUBG), seinen Börsengang, den zweitgrößten in der Geschichte des Landes, ab. Die Investorenbanker von Krafton stellten sicher, dass sie den potenziellen Anlegern mitteilten, dass das Unternehmen auch im Metaverse weltweit führend sein würde. In den folgenden Monaten begannen sowohl der chinesische Internetriese Alibaba als auch ByteDance, die Muttergesellschaft des sozialen Netzwerks TikTok, verschiedene Metaverse-Marken zu registrieren und VR- und 3D-bezogene Start-ups zu erwerben. Krafton verpflichtete sich unterdessen öffentlich, ein „PUBG-Metaverse“ zu starten.	laut Bloomberg auf „Bereiche wie die Erhöhung des Einkommens der Armen, die Verbesserung der medizinischen Versorgung, die Förderung der wirtschaftlichen Effizienz in ländlichen Gebieten und die Subventionierung von Bildungsunternehmen“ konzentriert würden. <sup>4</sup> Alibaba, Chinas zweitgrößtes Unternehmen, sagte nur zwei Wochen später einen ähnlich hohen Betrag zu. Die Botschaft Chinas Kommunistischer Partei war klar: Schaut auf eure Landsleute, nicht auf virtuelle Avatare.	
Zuckerbergs kühne Äußerungen erregten zwar große Aufmerksamkeit, aber viele seiner Kollegen und Konkurrenten hatten in den Monaten zuvor schon ähnliche Initiativen gestartet und vergleichbare Ankündigungen gemacht. Im Mai 2021 sprach der CEO von Microsoft, Satya Nadella, von einem von Microsoft geführten „Unternehmens-Metaverse“. Ebenso hatte Jensen Huang, CEO und Gründer des Computer- und Halbleiterriesen Nvidia, den Investoren mitgeteilt, dass „die Wirtschaft im Metaverse ... größer sein [wird] als die Wirtschaft in der physischen Welt“ <sup>**</sup> und dass die Plattformen und Prozessoren seines Unternehmens dabei im Mittelpunkt stehen werden. <sup>7</sup> Im vierten Quartal 2020 und im ersten Quartal 2021 erlebte die Spieleindustrie mit Unity Technologies und Roblox Corporation zwei ihrer bisher größten Börsengänge, die beide ihre Unternehmensgeschichte und ihre Ambitionen in Metaverse-bezogene Narrative verpackten.			Das Metaverse hat mehr als nur die Fantasie der Techno-Kapitalisten und Science-Fiction-Fans angefuehrt. Nicht lange, nachdem Tencent seine Vision der hyperdigitalen Realität öffentlich vorgestellt hatte, begann die Kommunistische Partei China (KPC) mit dem bisherto scharfsten Durchschlag gegen die heimische Spieleindustrie. Zu den neuen Maßnahmen gehörte ein Verbot für Mindestlöhne, von Montag bis Donnerstag Videospiele zu spielen, und eine Begrenzung der Spielzeit von 20 bis 21 Uhr am Freitag-, Samstag- und Sonntagabend – mit anderen Worten: es war für jeden Minderjährigen unmöglich, mehr als drei Stunden pro Woche ein Videospiel zu spielen. Darüber hinaus wurden Unternehmen wie Tencent ihre Gesichtserkennungssoftware und die nationale ID eines Spielers verwenden, um regelmäßig sicherzustellen, dass diese Regeln nicht von einem Spieler umgangen werden, der sich das Gerät eines älteren Nutzers ausleihen. Tencent sagte außerdem 15 Milliarden Dollar für „nachhaltige soziale Werte“ zu, die sich	Die Besorgnis der KPC über die wachsende Bedeutung von Spiel-inhalten und Plattformen im öffentlichen Leben wurde im August noch deutlicher, als die staatliche Wirtschaftszeitung <i>Security Times</i> ihre Leser warnte, dass das Metaverse ein „großartiges und illusionäres Konzept“ sei und dass „eine blinde Investition [darin] letztendlich auf einen selbst zurückfallen wird“. <sup>**</sup> Einige Kommentatoren interpretierten die verschiedenen Warnungen, Verbote und Steuern Chinas als Bestätigung für die Bedeutung des Metaverse. Für ein kommunistisches und zentral gesteuertes Land, das von einer einzigen Partei regiert wird, ist das Potenzial einer Parallelwelt für mehr Zusammenarbeit und Kommunikation eine Bedrohung, unabhängig davon, ob sie von einem einzigen Unternehmen oder dezentralen Gemeinschaften betrieben wird.
Für den Rest des Jahres 2021 wurde der Begriff „Metaverse“ fast zu einer Pointe, da jedes Unternehmen und seine Führungskräfte sich zu überspielen schienen, um ihn als etwas zu erwähnen, das ihr Unter-			Doch China war mit seinen Sorgen nicht allein. Im Oktober 2021 begannen auch Mitglieder des Europäischen Parlaments, ihre Bedenken zu äußern. Eine besonders wichtige Stimme war die von Christel Schaldemose, die als Chefunternehmerin für die Europäische Union tätig war, als diese an ihrer bisher größten Überarbeitung der Vorschriften für das digitale Zeitalter arbeitete (von denen die meisten die Macht der sogenannten großen Tech-Giganten wie Facebook, Amazon und Google einschränken sollten). Im Oktober sagte sie der dänischen Zeitung <i>Politiken</i> , dass „die Pläne für das Metaversum zutiefst besorgniserregend sind und dass die Union „ihnen Rechnung tragen muss“. <sup>**</sup>	
* Aus Gründen der Klarheit wird in diesem Buch Meta Platforms als Facebook bezeichnet. Das Metaverse und seine verschiedenen Plattformen zu erklären und gleichzeitig einen frischen Marktführer im Metaverse zu diskutieren, der Meta Platforms heißt, würde wahrscheinlich nur Verwirrung stiften.			Viellesch handelt es sich ja bei den vielen Ankündigungen, Kritiken und Warnungen zum Metaverse nur um eine Echokammer der realen Welt über eine virtuelle Fantasie – oder es geht eher darum, neue Narrative, Produkteinführungen und Marketing voranzutreiben als um etwas Lebensveränderndes. Denn schließlich hat die Technologiebranche eine lange Geschichte mit Buzzwords, die viel länger gehypt werden, als sie letztendlich auf den Markt bestehen. Denke wir nur an den 3D-Fernseher, VR-Kopfhörer oder virtuelle Assistanten. Trotzdem ist es bemerkenswert und erstaunlich, dass sich die größten Unternehmen der Welt in einem frühen Stadium öffentlich an solchen Ideen orientieren	
** Im Jahr 2021 betrug das weltweite BIP etwa 96 Billionen US-Dollar.			Die <i>Security Times</i> zitierte den Autor dieses Buches bei der Beschreibung des Metaverse.	

Abbildung 1: Das Metaverse und wie es alles revolutionieren wird  
[Ball 22a]

## Tests

Definitionen Metaverse [[Ball 22a](#)]

Definitionen Metaverse [[Ball 22b](#)]

Definitionen Metaverse [[Andr 22](#)]

Seite 46 gegen wen Kämpfen wir [[Hyp 22](#)]

Psychologie hinter SocialEngineering [?]

URL einfügen <https://arxiv.labs.arxiv.org/html/2401.05569>

You can also write footnotes.<sup>1</sup>

ääö

---

<sup>1</sup>Footnotes will be positioned automatically.

## **Kurzdarstellung**

### **1.1 Was ist zu tun**

Kurze Zusammenfassung der Arbeit, höchstens halbe Seite. Nenne die Zielsetzung, die Problemstellung und die Forschungsfragen. Wenn deiner Abschlussarbeit bestimmte Hypothesen zugrunde liegen, erwähne diese auch.

<https://www.scribbr.de/aufbau-und-gliederung/abstract-schreiben/>

### **1.2 Kurzdarstellung**

Das Ziel in der vorliegenden Arbeit ist es, zu klären, durch welche...



# Inhaltsverzeichnis

<b>Anleitungen und Tests</b> . . . . .	<b>v</b>
1 Anleitungen . . . . .	v
1.1 Was ist zu tun . . . . .	vii
1.2 Kurzdarstellung . . . . .	vii
<b>1 Einleitung</b> . . . . .	<b>1</b>
1.1 Problemstellung . . . . .	1
1.2 Zielsetzung der Arbeit . . . . .	2
<b>2 Das Metaverse</b> . . . . .	<b>3</b>
2.1 Definition und Entwicklung . . . . .	4
2.2 Technologien im Metaverse . . . . .	4
2.2.1 Virtuelle Realität . . . . .	4
2.2.2 Augmented Realität . . . . .	4
2.2.3 Digitale Zwillinge . . . . .	4
2.2.4 Künstliche Intelligenz . . . . .	4
2.2.5 LED und Hologramme . . . . .	4
2.2.6 Kryptowährungen . . . . .	4
2.2.7 Smart-Contracts . . . . .	4
2.3 Beispiele . . . . .	4
2.3.1 Meta . . . . .	4
2.3.2 Sandbox . . . . .	4
2.3.3 Roblox . . . . .	4
2.3.4 Fortnite . . . . .	4
2.3.5 Warframe . . . . .	4
<b>3 Social Engineering</b> . . . . .	<b>5</b>
3.1 Was ist Social Engineering? . . . . .	5
3.2 Geschichte des Social Engineering . . . . .	6
3.3 Grundformen des Sozial Engineering . . . . .	8
3.3.1 Phishing . . . . .	8
3.3.2 Elizitieren per Telefon . . . . .	10
3.3.3 Identitätsbetrug . . . . .	11

3.4 weitere Angriffsvektoren . . . . .	13
3.4.1 Dumpster diving . . . . .	13
3.4.2 Watering Hole . . . . .	13
3.4.3 Ködern . . . . .	13
3.4.4 Honigtopf . . . . .	13
3.4.5 USB Drop . . . . .	13
3.5 Psychologische Prinzipien hinter Social Engineering . . . . .	13
3.5.1 6 Prinzipien der Beeinflussung . . . . .	13
<b>4 Social Engineering im Metaverse . . . . .</b>	<b>17</b>
4.1 Das Metaverse als Ziel für Social Engineering . . . . .	17
4.1.1 Was macht das Metaverse interessant für Social Engineering . . . . .	17
4.1.2 Gefahren für Minderjährige im Metaverse . . . . .	17
4.2 Anwendungsmöglichkeiten von Social Engineering im Metaverse . . . . .	17
4.2.1 Deep Fakes . . . . .	17
4.2.2 Manipulation durch Gamification-Elemente . . . . .	17
4.2.3 Biometrische Hacks . . . . .	17
4.3 Auswirkungen des Social Engineering im Metaverse . . . . .	18
4.3.1 persönliche Auswirkungen . . . . .	18
4.3.2 soziale Auswirkungen . . . . .	18
4.3.3 wirtschaftliche Auswirkungen . . . . .	18
4.4 Fallbeispiel . . . . .	18
<b>5 Schutzmechanismen und Abwehrstrategien . . . . .</b>	<b>21</b>
5.1 Technische Sicherheitsmaßnahmen . . . . .	21
5.2 Aufklärung und Bewusstseinsbildung . . . . .	21
<b>6 Fazit und Ausblick . . . . .</b>	<b>23</b>
<b>Literaturverzeichnis . . . . .</b>	<b>25</b>
<b>Abbildungsverzeichnis . . . . .</b>	<b>29</b>
<b>Glossar . . . . .</b>	<b>31</b>

# **Kapitel 1**

## **Einleitung**

Das Metaverse, ein umfassender virtueller Raum, der durch die Kombination physischer und virtueller Realität entsteht, hat in den letzten Jahren erhebliche Aufmerksamkeit auf sich gezogen. Es wird als die nächste große Entwicklung des Internets angesehen, die eine völlig neue Dimension der Interaktion und des Erlebens ermöglicht. Mit Technologien wie Virtual Reality (VR), Augmented Reality (AR) und Künstlicher Intelligenz (KI) schafft das Metaverse immersive Umgebungen, in denen Nutzer arbeiten, spielen und soziale Kontakte pflegen können (Lee et al., 2021). Facebooks Umbenennung in Meta im Jahr 2021 und die damit verbundene Investition in die Entwicklung des Metaverse verdeutlichen die Bedeutung und das Potenzial dieser Technologie (Meta, 2021).

Jedoch bringt diese neue digitale Welt auch zahlreiche Herausforderungen und Risiken mit sich. Eine besonders bedrohliche Form der Cyberkriminalität im Metaverse ist das Social Engineering. Social Engineering bezieht sich auf die Manipulation von Menschen, um vertrauliche Informationen zu erlangen oder sie zu Handlungen zu bewegen, die ihre Sicherheit gefährden (Hadnagy, 2010). Im Metaverse, wo die Grenzen zwischen Realität und Virtualität verschwimmen, können Angreifer besonders raffinierte Methoden einsetzen, um ihre Ziele zu erreichen (Smith, 2023).

### **1.1 Problemstellung**

Die Problemstellung dieser Arbeit ergibt sich aus der zunehmenden Verbreitung und Nutzung des Metaverse, welche neue Angriffsvektoren für Social Engineering eröffnet. Angreifer können die immersive Natur des Metaverse ausnutzen, um Vertrauen zu gewinnen und Nutzer zu täuschen. Die Anonymität und die komplexen sozialen Interaktionen im Metaverse erleichtern es den Angreifern, sich als vertrauenswürdige Personen oder Organisationen auszugeben. Dies führt zu erheblichen Risiken für die Privatsphäre und Sicherheit der Nutzer (Wilson, 2022).

Ein Beispiel für die Gefahr von Social Engineering im Metaverse ist die Nutzung von Deep Fakes, um gefälschte, aber äußerst realistische Avatare oder Videos zu erstellen. Diese können

verwendet werden, um Nutzer zu täuschen und sie dazu zu bringen, sensible Informationen preiszugeben oder schädliche Aktionen durchzuführen (Chesney und Citron, 2019). Darüber hinaus können durch Gamification-Elemente im Metaverse Nutzer manipuliert und zu bestimmten Verhaltensweisen verleitet werden, ohne dass sie sich der Manipulation bewusst sind (Bec, 2022).

## 1.2 Zielsetzung der Arbeit

Ziel dieser Arbeit ist es, die Gefahren des Social Engineerings im Kontext des Metaverse umfassend zu analysieren und mögliche Schutzmaßnahmen zu erörtern. Dabei sollen folgende Forschungsfragen im Fokus stehen:

- Welche spezifischen Social Engineering-Techniken werden im Metaverse eingesetzt?
- Welche Sicherheitslücken und Schwachstellen machen das Metaverse anfällig für Social Engineering-Angriffe?
- Welche Maßnahmen können ergriffen werden, um die Nutzer und Systeme im Metaverse besser zu schützen?

Um diese Fragen zu beantworten, wird eine Kombination aus Literaturrecherche und Fallstudien verwendet. Die Arbeit soll einen fundierten Überblick über die aktuellen Bedrohungen und möglichen Lösungsansätze geben und dabei sowohl technische als auch organisatorische und psychologische Aspekte berücksichtigen.

Ein weiterer Schwerpunkt der Arbeit liegt auf der Untersuchung der Auswirkungen von Social Engineering-Angriffen im Metaverse. Dies umfasst die persönlichen, sozialen und wirtschaftlichen Folgen für die Betroffenen sowie die gesellschaftlichen Implikationen (Naughton, 2021). Darüber hinaus sollen Empfehlungen für die Entwicklung und Implementierung effektiver Schutzmaßnahmen gegeben werden, um die Sicherheit im Metaverse zu erhöhen und das Bewusstsein für die Risiken zu schärfen.



## **Kapitel 2**

### **Das Metaverse**

#### **2.1 Definition und Entwicklung**

#### **2.2 Technologien im Metaverse**

##### **2.2.1 Virtuelle Realität**

##### **2.2.2 Augmented Realität**

##### **2.2.3 Digitale Zwillinge**

##### **2.2.4 Künstliche Intelligenz**

##### **2.2.5 LED und Hologramme**

##### **2.2.6 Kryptowährungen**

##### **2.2.7 Smart-Contracts**

#### **2.3 Beispiele**

##### **2.3.1 Meta**

##### **2.3.2 Sandbox**

##### **2.3.3 Roblox**

##### **2.3.4 Fortnite**

##### **2.3.5 Warframe**

# Kapitel 3

## Social Engineering

### 3.1 Was ist Social Engineering?

Auch zum Thema Social Engineering lassen sich mehrere Definitionen finden, die in vielen Punkten übereinstimmen aber sich auch in wesentlichen Punkten unterscheiden.

»Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyber-Kriminelle verleiten das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.«[\[BSI 24b\]](#)

»Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen.«[\[Kevi 11a\]](#)

Diese Definitionen betrachten Social Engineering durchweg als negativ, da es zum Schaden anderer und zum eigenen Vorteil eingesetzt wird. In anderen Quellen werden jedoch auch Definitionen dargestellt die aufzeigen dass Sozial Engineering auch zum Vorteil der Zielperson genutzt werden kann.

»Social Engineering [...] nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.

Gleichzeitig steht Social Engineering für eine Praxis der politischen und gesellschaftlichen Steuerung bzw. Beeinflussung von Gesellschaften mittels Kommunikation und kann sowohl als positiv als auch als negativ wahrgenommene Ergebnisse erzielen. Die stark negative Begriffsvariante dominiert jedoch aktuell das Begriffsbild [...]«[\[Wiki 24b\]](#)

»Akt der Manipulation einer Person, eine Handlung auszuführen, die vielleicht im besten Interesse der »Zielperson« liegt - oder auch nicht.«[\[Hadn 11a\]](#)

Die verschiedenen Definitionen stimmen darin überein, dass Social Engineering die Manipulation und/oder Beeinflussung von Personen umfasst, mit dem Ziel, diese zu bestimmten Handlungen zu veranlassen.

Social Engineering wird von verschiedenen Akteuren, darunter Einzelpersonen und Institutionen, zu unterschiedlichen Zwecken eingesetzt.

»Ärzte Psychologen und Therapeuten nutzen beispielsweise oft Elemente des Social Engineering um ihre Patienten zu bestimmten Handlungen zu manipulieren. Trickbetrüger hingegen nutzen Elemente des Social Engineering um ihre Zielperson zu Aktivitäten zu bringen die zu einem Verlust führen.« [\[Hadn 11a\]](#)

Methoden des Social Engineering finden ebenfalls Anwendung im Vertrieb, wo Verkäufer Kunden Produkte aufdrängen, die diese möglicherweise gar nicht benötigen. Ähnliche Techniken werden auch von Personalrekrutierern, Regierungen und Spionen genutzt, jeweils angepasst an ihre spezifischen Ziele und Kontexte. (Vgl. [\[Ozka 18\]](#)) Auch verärgerte Angestellte können Methoden des Social Engineering nutzen um dem eigenen Unternehmen zu schaden. (Vgl. [\[Hadn 11b\]](#)) Ebenso wie unterschiedliche Akteure die Social Engineering betreiben sind auch die Motivationen für einen Angriff unterschiedlich. Die einen tun es aus Spaß, für das Machtgefühl oder Rache während es für andere um Politik, Spionage oder Industriespionage geht. (vgl. [\[Schu 11a\]](#))

## 3.2 Geschichte des Social Engineering

Social Engineering ist ein Phänomen, das es bereits seit Anbeginn der Menschheit gibt, auch wenn es nicht immer unter diesem Begriff bekannt war. Schon kleine Kinder weinen absichtlich, um bei ihren Eltern ihren Willen durchzusetzen, oder nutzen nonverbale Kommunikation, um Dinge zu erreichen, die sie sonst nicht bekämen. Dieses Verhalten zeigt, dass die Manipulation anderer durch gezielte Handlungen tief in der menschlichen Natur verankert ist. (vgl. [\[Stir 21a\]](#))

Ein prominentes frühes Beispiel für Social Engineering ist das trojanische Pferd, das als der erste aufgezeichnete Social Engineering Angriff gilt. Diese Episode wurde in Homers "Ödyssee" niedergeschrieben. Im Jahr 1184 v. Chr. nutzten die Griechen eine Täuschung, um in Troja einzudringen. Sie bauten ein Holzpferd als Geschenk und täuschten ihren Rückzug vor. Nach der Verkündung dass das Pferd ein Weihegeschenk an die Göttin Athene sei und Unglück bringt sollte es zerstört werden. Außerdem wurde es so groß gebaut damit es nicht in Stadt gebracht werden kann da die Stadt sonst unter dem Schutz der Athene

stunde. Die Trojaner holten aufgrund dieser Manipulation das Pferd in die Stadt. Als die Trojaner schliefen, kletterten griechische Soldaten aus dem Holzpferd und öffneten die Tore von innen. (vgl. [MITN 24]).

Zum ersten Mal erwähnt wurde der Begriff Social Engineer in einem Zeitungsartikel der New York Times von 1887. T. Burnett Baldwin wurde darin als Social Engineer bezeichnet, der sichergestellt hat, dass seine Mitarbeiter das Karnevalsprogramm bis ins kleinste Detail ausführten.(vgl. [Time 87]) Im Jahr 1899 prägte William Tolman den Begriff Social Engineering und bezeichnete es als eine der neuesten Professionen. Tolman beschrieb in einem Artikel, wie eine Organisation ein leeres Grundstück in einen Erholungsbereich für die Familien der Mitarbeiter umwandelte, was zu einer verbesserten Beziehung zwischen den Mitarbeitern und dem Arbeitgeber führte.(vgl. [Time 99]) Dies zeigt, dass Social Engineering darauf zielt, auf eine Personengruppe Einfluss zu nehmen, um ihre Verbindung zu einer bestimmten Organisation zu intensivieren. (vgl. [Mout 18]).

In der Geschichte der Menschheit finden sich jedoch immer wieder Beispiele dafür, wie Methoden des Social Engineering eingesetzt wurden, um Menschen in eine bestimmte Richtung zu lenken. Durch religiöse Regeln wurden ganze Kulturen geformt, die nach bestimmten Normen und ethischen Grundsätzen handeln, da sie sich davon Vorteile im Jenseits erhoffen. Ein prominentes Beispiel dafür ist das Kastensystem in Indien, das tief in religiösen Überzeugungen und sozialen Strukturen verwurzelt ist und seit Jahrtausenden das Verhalten und die Interaktionen der Menschen bestimmt (vgl. [Mali 09]).

Ein weiteres Beispiel ist die Verwendung von Propaganda durch politische Regime, um die öffentliche Meinung zu beeinflussen und die Macht zu festigen. Während des Zweiten Weltkriegs nutzten verschiedene Länder intensiv Propaganda, um die Moral zu stärken und die Bevölkerung hinter den Kriegsanstrengungen zu vereinen (vgl. [Tayl 03]). Diese gezielte Beeinflussung der Massen zeigt, wie tiefgreifend und wirkungsvoll Social Engineering sein kann.

In modernen Zeiten hat sich Social Engineering weiterentwickelt und ist zu einem zentralen Thema im Bereich der Informationssicherheit geworden. Cyberkriminelle nutzen psychologische Manipulationstechniken, um Menschen dazu zu bringen, vertrauliche Informationen preiszugeben oder schädliche Software herunterzuladen. Dieses Phänomen zeigt, dass Social Engineering nicht nur ein historisches, sondern auch ein aktuelles und sich ständig weiterentwickelndes Thema ist (vgl. [Kevi 11b]).

### 3.3 Grundformen des Sozial Engineering

Es existieren diverse Methoden, wie Social Engineers Zugang zu ihren Zielobjekten erlangen, wobei sich die Vorgehensweisen in technische, physische und über soziale Medien vermittelte Ansätze unterteilen lassen.

Technisches Social Engineering umfasst Angriffe, die mithilfe von technischen Geräten wie Computern, Handys oder Telefonen durchgeführt werden. Hierbei werden oft komplexe technische Hilfsmittel eingesetzt, um Sicherheitsmaßnahmen zu umgehen und Zugang zu vertraulichen Informationen zu erlangen.

Physisches Social Engineering bezieht sich auf Situationen, in denen der Angreifer persönlich in Erscheinung tritt, um sein Ziel zu erreichen. Dies kann beispielsweise durch das Eindringen in gesicherte Gebäude unter falscher Identität oder durch direkte Interaktion mit dem Ziel unter einem Vorwand geschehen.

Bei Angriffen über soziale Medien nutzen Social Engineers ebenfalls technische Hilfsmittel, um zunächst Kontakt zur Zielperson aufzubauen. Die eigentliche Manipulation erfolgt jedoch durch persönliche Kommunikation über Plattformen wie Chats, Messenger-Dienste oder andere soziale Netzwerke. Hierbei wird oft eine Kombination aus technischem Know-how und psychologischen Fähigkeiten eingesetzt, um die Zielperson subtil zu beeinflussen.

Diese Kategorisierung verdeutlicht, wie vielseitig und angepasst Social Engineering-Methoden sein können, je nach Ziel und Kontext des Angriffs. (Vgl. [Alex 16])

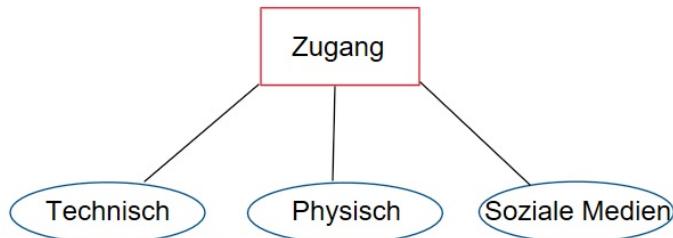


Abbildung 3.1: verschiedene Zugangsarten  
(eigene Darstellung)

Social Engineering in seiner schädlichen Ausprägung lässt sich typischerweise in drei Hauptkategorien einteilen: Phishing, Elizitieren per Telefon und Identitätsbetrug (vgl. [Chri 14a])

#### 3.3.1 Phishing

Phishing, ein Begriff, der sich aus den Worten "Passwort" und "Fishing" zusammensetzt, ist die am häufigsten auftretende Form des Social Engineering wie Abbildung 3.2 zeigt. (vgl. [BSI 24a])

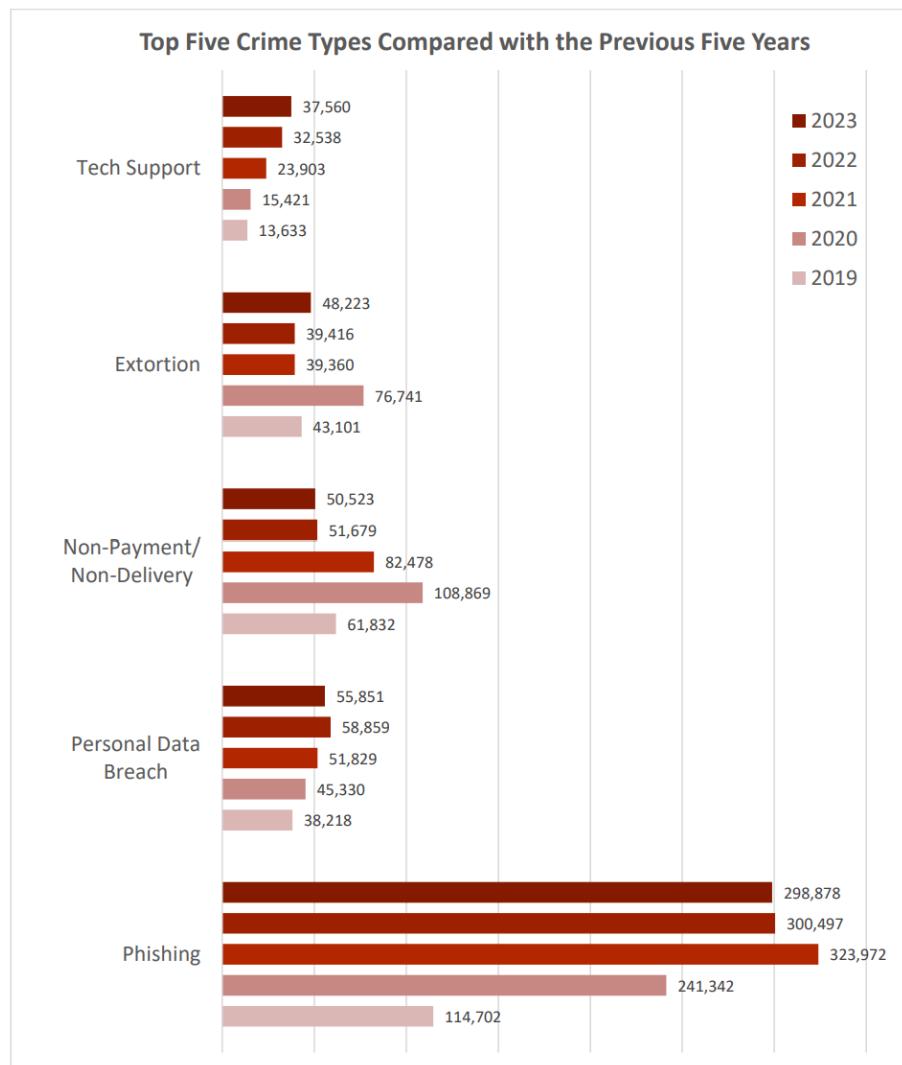


Abbildung 3.2: Die fünf häufigsten Kriminalitätsarten im Vergleich zu den letzten fünf Jahren

[Inve 24]

Phishing gehört zum technischen Social Engineering. Bei dieser Methode senden Angreifer massenhaft E-Mails, die gezielt Emotionen wie Angst und Neugier oder das Konzept der Autorität ausnutzen. Diese E-Mails enthalten schädliche Dateien, Links oder Anweisungen. Das Anklicken, Öffnen oder Befolgen dieser Inhalte kann zu Datenverlust, Sicherheitsverletzungen oder anderen nachteiligen Konsequenzen für die Zielperson führen (Vgl. [Chri 14b]). Abbildung 3.3 zeigt eine solche E-mail.

Die Befürchtung, dass das eigene Konto kompromittiert und Geld gestohlen wurde, kann ausreichen, um einen Menschen dazu zu bewegen, auf einen Link zu klicken und sich schnell ins Konto einzuloggen, um die Situation zu überprüfen. Genau diese Reaktion intendiert der Angreifer. Häufig werden die Zugangsdaten dann von einer gefälschten Webseite oder durch einen manipulierten Login-Prozess mittels kleiner Skripte abgefangen. Sobald der Angreifer



Abbildung 3.3: gefälschte E-Mail von PayPal

[Chri 14a]

diese Daten in seinem Besitz hat, nutzt er sie, um sich einzuloggen und genau jene Handlung auszuführen, vor der das Opfer Angst hatte: das Geld wird gestohlen. (Vgl. [Chri 14b]) Da es sich hierbei um Massen-E-Mails handelt ist die Anrede immer unpersönlich.

Wenn solche Angriffe durch persönlich angepasste E-Mails ausgeführt werden, die bereits detaillierte Informationen, wie Vorlieben oder Abneigungen, des Empfängers enthalten, bezeichnet man dies als »Spear-Phishing«. Dieser Begriff leitet sich vom Speer ab, der als Symbol für die gezielte Ausrichtung auf ein spezifisches Ziel steht. (Vgl. [Stir 21b],[Chri 14b]) Eine Spezialform des Spear-Phishing ist das »Whaling«, auch bekannt als »CEO-Fraud« oder »Business E-Mail Compromise (BEC)«. Whaling leitet sich von Wal ab und umschreibt das Spear-Phishing auf ein hochrangiges Individuum, wie z.B. den CEO einer Firma. »Allein im Jahr 2023 erhielt das IC3 des FBI 21.489 BEC-Beschwerden, wobei die angepassten Verluste über 2,9 Milliarden Dollar betrugen.« [Inve 24, frei übersetzt]

### 3.3.2 Elizitieren per Telefon

Das „Elizitieren“ am Telefon ist die zweithäufigste Methode des Social Engineering.[Stir 21c] „In Schulungsunterlagen definiert die National Security Agency der USA Elizitieren als ‚subtile Extraktion von Informationen während einer offenbar normalen und harmlosen Unterhaltung‘“. [Hadn 11c]

Beim Elizitieren per Telefon kontaktiert der Angreifer die Zielperson telefonisch und stellt unauffällige Fragen, um relevante aber bedeutungslos wirkende Informationen zu sammeln. Diese Informationen nutzt er häufig, um bei der nächsten Zielperson vertrauenswürdig zu erscheinen und so Zugang zu sensibleren Daten zu erhalten.

Typischerweise verwendet der Angreifer einen „Pretext“, indem er vorgibt, eine Person mit berechtigtem Interesse an den Informationen zu sein. (Vgl. [Chri 14c]) „Mit Pretexting bezeichnet man die Schaffung eines erfundenen Szenarios, um die Zielperson als Opfer dazu zu überreden, Informationen herauszurücken oder eine Aktion auszuführen.“ [Hadn 11d] Dies wird durch „Spoofing“unterstützt, wobei der Zielperson eine falsche Telefonnummer angezeigt wird, um den Eindruck zu erwecken, der Anruf stamme von einer vertrauenswürdigen Quelle(Vgl. [Chri 14d])

Die Effektivität des Elizitierens beruht auf der psychologischen Manipulation der Zielperson. Durch geschicktes Fragen und das Erzeugen eines Gefühls von Vertraulichkeit und Dringlichkeit gelingt es dem Angreifer, die Zielperson dazu zu bringen, Informationen preiszugeben, die sie unter normalen Umständen nicht teilen würde. Dies wird oft durch nonverbale Kommunikation wie Lächeln, Tonfall oder Sprechgeschwindigkeit unterstützt. Diese Technik erfordert sowohl Geduld als auch ein gutes Verständnis menschlicher Verhaltensweisen, um erfolgreich zu sein. (Vgl. [Hadn 11e])

Auch die Polizei warnt vermehrt vor Betrügern, die sich am Telefon als Polizisten ausgeben und mit gefälschter Telefonnummer warnen das ein Einbruch ins Anwesen des Opfers bevorsteht. Sie fordern das Opfer auf Barvermögen und Wertgegenstände zur Sicherheitsverwahrung an falsche Kollegen zu übergeben. Außerdem soll das Opfer mit niemanden darüber sprechen um angebliche Ermittlungen nicht zu gefährden. Siehe Abbildung 3.4 (Vgl. [Poli 24])

### 3.3.3 Identitätsbetrug

Beim Identitätsbetrug übernehmen die Angreifer eine fremde Identität, um die Zielperson zu unvorteilhaften Handlungen zu bewegen. Auch hier spielen Elizitieren und Pretexting eine wichtige Rolle. Im Gegensatz zu Phishing und telefonischem Elizitieren ist Identitätsbetrug eine physische Methode des Social Engineering. Daher kommt der nonverbalen Kommunikation eine besondere Bedeutung zu. Abhängig vom gewählten Pretext des Angreifers ist es entscheidend, die nonverbalen Signale der Zielperson richtig zu interpretieren und gleichzeitig selbst die passenden nonverbalen Zeichen auszusenden. (Vgl. [Chri 14e])

Eine Beliebte Methode des Identitätsbetrugs ist „Tailgating“. Hierbei folgt der Angreifer befugten Personen in einen Bereich zu dem er sonst keinen Zutritt hätte indem er sich als



Abbildung 3.4: Poster der Polizei Nordrhein-Westfalen  
[Poli 24]

jemand ausgibt, der berechtigt ist einzutreten. Indem er sich beispielsweise als Mitarbeiter ausgibt und im schwächer gesicherten Raucherberich aufhält um mit den Mitarbeitern anschließend das Gebäude zu betreten. Oft reicht es auch einen großen Karton zu tragen während man auf eine gesicherte Tür zuläuft, um von einem hilfsbereiten Mitarbeiter die Tür aufgehalten zu bekommen. Ein weiterer beliebter Trick ist es eine Kennkarte optisch zu kopieren. Nach mehreren Fehlversuchen besteht eine hohe Chance eingelassen zu werden. Diese Taktiken funktionieren besser, wenn sich der Angreifer gut vorbereitet hat und Verhaltensweisen, Körpersprache, Dialekte und Kleidungsstil der Angestellten erforscht und eingeübt hat. Auch hier hilft es im Vorfeld zu Elizitieren um an die notwendigen Informationen zu kommen. (Vgl. [Chri 14e])

Bei einem Identitätsbetrug wie in dem Fall der falschen Polizisten, benutzen die Angreifer falsche Uniformen um sich als Polizisten auszugeben. Hier müssen die Täter versuchen sowohl Vertrauen als auch Autorität auszustrahlen um die Opfer nicht misstrauisch zu machen.

## 3.4 weitere Angriffsvektoren

### 3.4.1 Dumpster diving

### 3.4.2 Watering Hole

### 3.4.3 Ködern

### 3.4.4 Honigtopf

### 3.4.5 USB Drop

## 3.5 Psychologische Prinzipien hinter Social Engineering

### 3.5.1 6 Prinzipien der Beeinflussung

Es gibt viele unterschiedliche Taktiken die Social Engineere nutzen um ihre Zielperson zu überzeugen. Die meisten davon haben ihren Kern in einem von sechs grundlegenden psychologischen Prinzipien (vgl. [Cial17a]). Diese Prinzipien werden im folgenden kurz vorgestellt und erklärt wie ein Angreifer diese nutzt um seine Zielperson zu beeinflussen.

#### 3.5.1.1 Reziprozität

„Nach Erkenntnissen von Soziologen und Anthropologen ist eine der verbreitetsten und grundlegendsten Normen der menschlichen Kultur die Reziprozitätsregel. Diese Regel besagt, dass Menschen versuchen sollen sich für das zu revanchieren, was sie von anderen bekommen.“ [Cial17b] Diese Regel wurde Menschen bereits in Kindertagen beigebracht, zumeist mit der Redewendung „Eine Hand wäscht die andere“. Die Regel hat für eine Gesellschaft enorme Vorteile, indem sie den Ausbau des Handels, der Verteidigung und der gegenseitigen Hilfeleistung ermöglicht (vgl. [Schu11b]).

Ein Angreifer kann die Regel auszunutzen, indem er durch kleine Gefälligkeiten, Geschenke oder Zugeständnisse die Zielperson dazu bringen kann, zu tun was den Wünschen des Angreifers entspricht um nicht in dessen Schuld zu stehen (vgl. [Schu11b]).

### 3.5.1.2 Verpflichtung und Konsistenz

Die meisten Menschen wollen konsequent erscheinen. Sie wollen in ihren Worten Überzeugungen und Taten konsistent sein da die Gesellschaft der Konsistenz einen hohen Wert beimisst und sie sich im Alltag gut bewährt. Eine Orientierung am Konsistenzprinzip hilft schnelle Entscheidungen zu treffen, ohne alle relevanten Informationen prüfen zu müssen, indem man im Einklang mit früheren Entscheidungen und festgelegten Standpunkten handelt.

Der Angreifer versucht die Zielperson dazu zu bringen einen bestimmten Standpunkt zu beziehen. Die Zielperson spürt eine Verpflichtung konsequent zu sein und bei diesem Standpunkt zu bleiben. Wenn der Angreifer nun bittet Handlungen auszuführen die mit diesem Standpunkt im Einklang stehen, ist die Zielperson eher geneigt diesen Bitten oder Aufrückerungen nachzugehen. Wenn Menschen sich öffentlich und aktiv auf einen Standpunkt festgelegt haben, dies mit Mühen verbunden war und durch innere Überzeugung geschah, ist die Verpflichtung noch größer (vgl. [Cial 17c]). „Die Konsistenz ist so stark, das Menschen gegen ihre eigenen Interessen verstossen, nur um nach außen hin als Konsistent zu gelten.“ [Schu 11c]

### 3.5.1.3 Soziale Bewährtheit

Das Prinzip der sozialen Bewährtheit besagt das Menschen dazu neigen ihre Entscheidungen wie sie handeln und was sie glauben danach auszurichten was andere Menschen in dieser Situation glauben oder machen. Das Verhalten der anderen Personen wird in diesem Moment als richtig angenommen. Wenn Personen unsicher sind, da eine mehrdeutige Situation vorliegt wird dieses Verhalten noch verstärkt. Auch die Feststellung einer Ähnlichkeit zu anderen Personen verstärkt dieses Verhalten.

Ein Angreifer kan dieses Prinzip benutzen um die Zielperson zu einer Handlung zu ermutigen indem er sie in eine unsichere Situation bringt und darauf hinweist dass schon viele andere Personen genauso gehandelt haben. (vgl. [Cial 17d])

### 3.5.1.4 Sympathie

„Menschen sind eher bereit, sich von jemandem überzeugen zu lassen, den sie kennen und sympathisch finden.“ [Cial 17e] Der Mensch tendiert dazu, diejenigen zu mögen, die ihn mögen. [Stir 21d]

Ebenso wie bei dem Prinzip der sozialen Bewährtheit, ist auch hier Ähnlichkeit ein Faktor der Einfluss darauf hat ob jemand eine andere Person sympathisch findet. Dabei ist es

unabhängig davon ob sich dies in ähnlichen Meinungen Charaktereigenschaften oder Lebensweisen äußert. (vgl. [Jerr 04]) Ein weiterer Faktor bei der Entwicklung von Sympathie ist die körperliche Attraktivität. Einer Forschung zufolge werden Attraktiven Menschen unterbewusst automatisch positive Eigenschaften zugeschrieben (vgl. [Lang 00]). Dies führt dazu, dass sie andere Personen leichter beeinflussen können. Wiederholte Kontakte unter positiven Rahmenbedingungen mit einer Person, bestenfalls eine erfolgreiche Kooperation, sind ebenfalls gute Möglichkeiten um Sympathie zu erzeugen. (vgl. [Cial 17f])

Der Angreifer studiert seine Zielperson um sich ein möglichst genaues Bild von ihr zu machen. Sie passen ihren Kleidungsstil an den der Zielperson an und achten darauf ein gepflegtes äuseres Erscheinungsbild abzugeben. Durch die Vortäuschung gleicher Interessen und gut plazierter Komplimente versuchen sie Sympathie zu erzeugen und so die Zielperson anfällig für ihre Wünsche und Forderungen zu machen. (vgl. [Cial 17f])

### 3.5.1.5 Autorität

Gehorsam gegenüber Autoritäten ist ein Prinzip das die Menschen schon seit Kindheitstagen prägt. Bereits Eltern bringen ihren Kindern bei das Gehorsam gegenüber den richtigen Autoritäten gut und Ungehorsam schlecht ist. Sie sollen ihren Eltern, Lehrern oder anderen Autoritäten gehorchen und sie nicht in Frage stellen da dies als respektlos gilt. Im Erwachsenenalter wird verlangt sich rechtlichen, militärischen und politischen Systemen unterzuordnen. Auch in der Bibel wird beschrieben, „wie Ungehorsam gegenüber der höchsten Autorität dazu führte, dass Adam, Eva und der Rest der Menschheit des Paradieses verlustig gingen.“ [Cial 17g] In vielen Fällen ist es richtig auf die Anweisungen von Autoritäten zu befolgen da diese über Wissen Erfahrung und Macht verfügen. Oft reicht es auch schon den Anschein von Autorität zu erzeugen um automatischen Gehorsam zu erzeugen. Hierfür reichen oft schon die Insignien der Autorität, wie der richtige Titel, die passende Kleidung und Luxusartikel, wie Schmuck oder teure Fahrzeuge. (Vgl. [Cial 17h])

Der Angreifer benutzt die Insignien der Autorität, wie z.B. eine Uniform, Visitenkarte oder ein Luxusauto um der Zielperson zu suggerieren das er über Macht verfügt und Zielperson seinem Willen entsprechend handeln sollte. Hierbei ist auch die richtige Körpersprache, Stimme und Artikulation wichtig damit die Zielperson nicht misstrauisch wird und die Autorität hinterfragt. (Vgl. [Stir 21e])

### 3.5.1.6 Knappheit

Das Knappheitsprinzip besagt, „dass Möglichkeiten uns umso wertvoller erscheinen, je weniger erreichbar sie sind“[Cial 17i]. Das Verlangen einer Person kann durch zeitliche oder mengenmäßige Begrenzungen sowie durch Konkurrenzdruck gesteigert werden. [Cial 17j]

Der Gedanke etwas zu verlieren motiviert die Menschen dabei stärker als der Gedanke etwas Gleichwertiges gewinnen zu können (vgl. [Hobf01]). Insbesondere in Situationen, die von Risiko und Unsicherheit geprägt sind, beeinflusst die Gefahr eines möglichen Verlustes die Entscheidungsprozesse erheblich (vgl. [Amos 81],[Cars 97]).

Wenn Wahlfreiheit beschnitten oder bedroht wird, steigt das Verlangen, diese Freiheiten sowie die damit verbundenen Produkte und Dienstleistungen zu behalten, erheblich an. Dies löst eine Gegenreaktion aus, die das Interesse an der Sache und die Bemühungen, sie zu erlangen, intensiviert. Dieser Effekt wird als „Reaktanz“ bezeichnet. (Vgl. [Breh 66]) Besonders ausgeprägt ist diese Reaktanz in der Trotzphase bei Kleinkindern und in der Pupertät bei Jugendlichen, da diese Lebensabschnitte durch ein aufkommendes Individualitätsgefühl gekennzeichnet sind. (Vgl. [Cial 17j])

Das Knappheitsprinzip bezieht sich auch auf Informationen. Verschiedene Forschungsarbeiten haben gezeigt, dass Informationen die schwerer zu erhalten sind eine größere Überzeugungskraft besitzen (vgl. [Rich 71], [Step 75], [Step 73]). Unterliegt die Information einer Zensur überzeugt sie sogar ohne dass die Information tatsächlich vorlag (vgl. [Step 75]).

Beim Phishing wird häufig das Knappheitsprinzip eingesetzt. In den E-Mails wird von zeitlich begrenzten Angeboten oder Fristen gesprochen, nach deren Ablauf etwas Schlimmes passieren oder verloren gehen könnte. Ebenso werden exklusive Angebote, die auf geheimen Informationen basieren, verwendet, um die Opfer dazu zu verleiten, den Anweisungen zu folgen.

Angreifer können das Knappheitsprinzip auch nutzen um das Reziprozitätprinzip zu verstärken. Indem sie Information teilen von den sie behaupten dass sie schwer zu bekommen waren, steigt der Wert dieser Gabe für die Zielperson die sich nun revanchieren möchte.

# Kapitel 4

## Social Engineering im Metaverse

### 4.1 Das Metaverse als Ziel für Social Engineering

#### 4.1.1 Was macht das Metaverse interessant für Social Engineering

##### 4.1.1.1 Charakterisierung der möglichen Zielpersonen

##### 4.1.2 Gefahren für Minderjährige im Metaverse

### 4.2 Anwendungsmöglichkeiten von Social Engineering im Metaverse

#### 4.2.0.1 Identitätsdiebstahl

TODO

Beispiel Warframe

#### 4.2.1 Deep Fakes

TODO

Avatar ist ein Gegenstand und kann lauschen

#### 4.2.2 Manipulation durch Gamification-Elemente

#### 4.2.3 Biometrische Hacks

TODO

Brillen können gehackt werden Biometrische Daten ausgelesen werden wie mimiken etc

## 4.3 Auswirkungen des Social Engineering im Metaverse

### 4.3.1 persönliche Auswirkungen

### 4.3.2 soziale Auswirkungen

### 4.3.3 wirtschaftliche Auswirkungen

## 4.4 Fallbeispiel

Fallstudie: Der Angriff auf VirtuCon Hintergrund VirtuCon war eine großangelegte virtuelle Konferenz im Metaverse, die auf einer populären Plattform für digitale Zusammenkünfte und Veranstaltungen stattfand. Die Konferenz zog Tausende von Teilnehmern an, darunter führende Experten in den Bereichen Technologie, Wirtschaft und Bildung. VirtuCon bot eine Vielzahl von Sitzungen, Workshops und Networking-Möglichkeiten in einer vollständig immersiven 3D-Umgebung. Der Angriff Einige Tage vor der Veranstaltung begannen die Organisatoren, Berichte über gefälschte Veranstaltungseinladungen zu erhalten, die an Teilnehmer gesendet wurden. Diese Einladungen enthielten Links, die angeblich zu exklusiven Vorregistrierungsboni oder speziellen Zugängen für die Konferenz führten. Tatsächlich leiteten diese Links die Nutzer jedoch auf gefälschte Login-Seiten, die darauf abzielten, persönliche Daten und Zugangsinformationen zu stehlen. Parallel dazu schafften es die Angreifer, während der Veranstaltung mehrere Avatare zu kapern. Diese gekaperten Avatare wurden genutzt, um in verschiedenen Sitzungen und Chaträumen anwesend zu sein, wo sie weiterhin gefälschte Links verbreiteten und sogar versuchten, in private Gespräche einzudringen, um vertrauliche Informationen zu erlangen. Analyse Die Angreifer nutzten eine Kombination aus Phishing-Techniken und der Übernahme von Avataren, um das Vertrauen der Teilnehmer zu gewinnen und sie zur Preisgabe sensibler Informationen zu verleiten. Die Immersion und das Engagement im Metaverse trugen dazu bei, dass die Teilnehmer weniger misstrauisch gegenüber den ungewöhnlichen Aktivitäten waren, da sie die Interaktionen als Teil der Konferenzerfahrung ansahen. Die psychologischen Tricks, die dabei zum Einsatz kamen, umfassten das Vorspiegeln von Dringlichkeit (durch das Angebot von "exklusiven Boni"), die Nutzung von Autorität und Vertrautheit (durch das Kapern bekannter Avatare) und das Ausnutzen der Neugier und des Wunsches nach Vernetzung der Teilnehmer. Lessons Learned und Ableitungen für die Zukunft Diese Fallstudie unterstreicht die Notwendigkeit umfassender Sicherheitsmaßnahmen und Awareness-Programme für Teilnehmer und Organisatoren von Veranstaltungen im Metaverse. Dazu gehören:

- Verifizierung und Authentifizierung: Die Implementierung robuster Verifizierungs- und Authentifizierungsverfahren für alle Teilnehmer, Inhalte und Interaktionen.
- Aufklärung und Training: Die Sensibilisierung der Nutzer für die Risiken und Anzeichen von Social Engineering-Angriffen.
- Technische

Sicherheitslösungen: Die Nutzung von Sicherheitstechnologien, um den Zugriff auf Veranstaltungen zu sichern und die Kommunikation zwischen Teilnehmern zu schützen.



# Kapitel 5

## Schutzmechanismen und Abwehrstrategien

### 5.1 Technische Sicherheitsmaßnahmen

#### copy

- Verschlüsselung: Einsatz von Ende-zu-Ende-Verschlüsselung für Datenübertragungen innerhalb des Metaverse, um die Datensicherheit und Privatsphäre zu gewährleisten.
- Authentifizierung und Zugriffskontrolle: Verstärkung der Sicherheitsprotokolle durch Mehrfaktor-Authentifizierung und regelmäßige Überprüfung der Zugriffsrechte, um sicherzustellen, dass nur autorisierte Nutzer Zugang zu sensiblen Bereichen oder Informationen haben.
- Anomalieerkennung und Überwachung: Implementierung von Systemen zur Erkennung ungewöhnlicher Aktivitäten oder Verhaltensweisen, die auf einen Social Engineering-Angriff hindeuten könnten.
- Zwei-Faktor-Authentifizierung (2FA): Eine zusätzliche Sicherheitsebene für den Zugang zu virtuellen Umgebungen, die über das einfache Passwort hinausgeht.
- Ende-zu-Ende-Verschlüsselung: Sicherstellung, dass Kommunikation zwischen den Nutzern nicht von Dritten eingesehen werden kann.

#### eigene

### 5.2 Aufklärung und Bewusstseinsbildung

TODO

Regelmäßige Sicherheitsaudits: Überprüfung und Aktualisierung der Sicherheitseinstellungen und -protokolle, um Schwachstellen zu identifizieren und zu beheben.



# **Kapitel 6**

## **Fazit und Ausblick**

TODO

Sicherheit vorgegaukelt die so noch nicht vorhanden ist. Schwachstelle Mensch Ausblick auf zukünftige Entwicklungen und Forschungsbedarf



## Literaturverzeichnis

- [Alex 16] M. Alexander. *Methods for Understanding and Reducing Social Engineering Attacks*, S. 6 – 13. SANS Institute 2021, 2016.
- [Amos 81] D. K. Amos Tversky. *The Framing of Decisions and the Psychology of Choice*. Science, 211, 1981.
- [Andr 22] D. S. Andreas Dripke, Marc Ruberg. *Metaverse: Was es ist. Wie es funktioniert. Wann es kommt*. Diplomatic Council Publishing, 2022.
- [Ball 22a] M. Ball. *Das Metaverse: Und wie es alles revolutionieren wird*, s. . Liverright Publishing Corporation, 2022.
- [Ball 22b] M. Ball. *Das Metaverse: Und wie es alles revolutionieren wird*, S. 13–15. Liverright Publishing Corporation, 2022.
- [Breh 66] J. W. Brehm. *A theory of psychological reactance*. New York: Academic Press, 1966.
- [BSI 24a] BSI. *Phishing - how much is the phish!?* [online], 15.07.2024.
- [BSI 24b] BSI. *Social Engineering – der Mensch als Schwachstelle*. [online] <https://www.bsi.bund.de/dok/11287460>, 19.06.2024.
- [Cars 97] C. M. Carsten K W De Dreu. *Gain–loss frames and cooperation in two-person social dilemmas: A transformational analysis*. Journal of Personality and Social Psychology, Vol. 72 No. 5, 1997.
- [Chri 14a] P. E. Christopher Hadnagy. *Social engineering enttarnt: Sicherheitsrisiko Mensch*, Chap. 2. mitp-Verlags GmbH u. Co. KG, 2014.
- [Chri 14b] P. E. Christopher Hadnagy. *Social engineering enttarnt: Sicherheitsrisiko Mensch*, Chap. 2, S. 63 – 67. mitp-Verlags GmbH u. Co. KG, 2014.
- [Chri 14c] P. E. Christopher Hadnagy. *Social engineering enttarnt: Sicherheitsrisiko Mensch*, Chap. 2, S. 67 – 71. mitp-Verlags GmbH u. Co. KG, 2014.
- [Chri 14d] P. E. Christopher Hadnagy. *Social engineering enttarnt: Sicherheitsrisiko Mensch*, Chap. 2, s. 68. mitp-Verlags GmbH u. Co. KG, 2014.

- [Chri14e] P. E. Christopher Hadnagy. *Social engineering enttarnt: Sicherheitsrisiko Mensch*, Chap. 2, S. 72 – 74. mitp-Verlags GmbH u. Co. KG, 2014.
- [Cial17a] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17b] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17c] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17d] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17e] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17f] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17g] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17h] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17i] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Cial17j] R. B. Cialdini. *Die Psychologie des Überzeugens: Wie Sie sich selbst und ihren Mitmenschen auf die Schliche kommen*. Hogrefe Verlag, Bern, 2017.
- [Hadn11a] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe*. mitp-Verlags GmbH u. Co. KG, 2011.
- [Hadn11b] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe*. mitp-Verlags GmbH u. Co. KG, 2011.
- [Hadn11c] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe*. mitp-Verlags GmbH u. Co. KG, 2011.
- [Hadn11d] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe*. mitp-Verlags GmbH u. Co. KG, 2011.
- [Hadn11e] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe*. mitp-Verlags GmbH u. Co. KG, 2011.

- [Hobf01] S. E. Hobfoll. *The Influence of Culture, Community, and the Nested-Self in the Stress Process: Advancing Conservation of Resources Theory*. Applied Psychology, 50, 2001.
- [Hyp22] M. Hyppönen. *Was vernetzt ist, ist angreifbar: Wie Geheimdienste und Kriminelle uns im Netz infiltrieren*. John Wiley and Sons, Inc., 2022.
- [Inve24] F. B. of Investigations. *Internet Crime Report 2023*. [online], TODO Link einfügen, 16.07.2024.
- [Jerr04] S. P. Jerry M. Burger, Nicole Messian. *What a Coincidence! The Effects of Incidental Similarity on Compliance*. Society for Personality and Social Psychology, Inc., Alicia del Prado, Carmen Anderson, 2004.
- [Kevi11a] W. S. Kevin Mitnick. *Die Kunst der Täuschung: Risikofaktor Mensch*, s. 4. mitp-Verlags GmbH u. Co. KG, 2011.
- [Kevi11b] W. S. Kevin Mitnick. *Die Kunst der Täuschung: Risikofaktor Mensch*. mitp-Verlags GmbH u. Co. KG, 2011.
- [Lang00] R. A. Langlois JH, Kalakanis L. *Maxims or myths of beauty? A meta-analytic and theoretical review*. Psychological Bulletin 126, Larson A, Hallam M, Smoot M., 2000.
- [Mali09] A. Malinar. *Hinduismus*, S. 184 – 192. Vandenhoeck u. Ruprecht, 2009.
- [MITN24] MITNICKSECURITY. *The Early History of Social Engineering*. [online], <https://www.mitnicksecurity.com/the-history-of-social-engineering>, 16.06.2024.
- [Mout18] F. Mouton. *SOCIAL ENGINEERING ATTACK DETECTION MODEL Thesis*, S. 12–13. Department of Computer Science in der University of Pretoria, 2018.
- [Ozka18] E. Ozkaya. *Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert*, S. 11 – 13. Packt Publishing, Limited, 2018.
- [Poli24] Polizei-Nordrhein-Westfalen. *Vorsicht: Falsche Polizeibeamte am Telefon!* [online], <https://polizei.nrw/artikel/betrueger-geben-sich-am-telefon-als-polizeibeamte-aus>, 15.07.2024.
- [Rich71] R. A. J. Richard D. Ashmore, Vasantha Ramchandra. *Censorship as an Attitude Change Induction*. Paper presented at the Eastern Psychological Association Annual Meeting, 1971.
- [Schu11a] S. Schumacher. *Magdeburger Journal zur Sicherheitsforschung, Bd. 1*. Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg, 2011.

- [Schu 11b] S. Schumacher. *Magdeburger Journal zur Sicherheitsforschung, Bd. 1.* Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg, 2011.
- [Schu 11c] S. Schumacher. *Magdeburger Journal zur Sicherheitsforschung, Bd. 1.* Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg, 2011.
- [Step 73] S. A. Stephen Worchel. *The effects of censorship and attractiveness of the censor on attitude change.* Journal of Experimental Social Psychology, 9, 1973.
- [Step 75] M. B. Stephen Worchel, Susan Arnold. *The Effects of Censorship on Attitude Change: The Influence of Censor and Communication Characteristics.* Journal of Applied Social Psychology, 5, 1975.
- [Stir 21a] S. Stirnimann. *Der Mensch als Risikofaktor bei Wirtschaftskriminalität,* Chap. 4, s. 127. Springer Fachmedien Wiesbaden GmbH, 2021.
- [Stir 21b] S. Stirnimann. *Der Mensch als Risikofaktor bei Wirtschaftskriminalität,* Chap. 4, s. 129. Springer Fachmedien Wiesbaden GmbH, 2021.
- [Stir 21c] S. Stirnimann. *Der Mensch als Risikofaktor bei Wirtschaftskriminalität,* Chap. 4, s. 132. Springer Fachmedien Wiesbaden GmbH, 2021.
- [Stir 21d] S. Stirnimann. *Der Mensch als Risikofaktor bei Wirtschaftskriminalität,* Chap. 4. Springer Fachmedien Wiesbaden GmbH, 2021.
- [Stir 21e] S. Stirnimann. *Der Mensch als Risikofaktor bei Wirtschaftskriminalität,* Chap. 4, s. 153. Springer Fachmedien Wiesbaden GmbH, 2021.
- [Tayl03] P. M. Taylor. *Munitions of the Mind : A History of Propaganda (3rd ed.),* S. 208 – 248. Manchester University Press, 2003.
- [Time 87] N. Y. Times. *Society topics of the week.* [online], <https://www.nytimes.com/1887/01/02/archives/society-topics-of-the-week.html>, Januar 1887.
- [Time 99] N. Y. Times. *New profession appears; promoters of social engineering "find a fruitful field.* [online], <https://www.nytimes.com/1899/10/15/archives/new-profession-appears-promoters-of-social-engineering-find-a.html>, Oktober 1899.
- [Wiki 24a] Wikipedia. *Immersion (virtuelle Realität).* [online], TODO Link einfügen, 15.07.2024.
- [Wiki 24b] Wikipedia. *Social Engineering.* [online], TODO Link einfügen, 11.07.2024.

## **Abbildungsverzeichnis**

1	Das Metaverse und wie es alles revolutionieren wird . . . . .	v
3.1	verschiedene Zugangsarten . . . . .	8
3.2	Die fünf häufigsten Kriminalitätsarten im Vergleich zu den letzten fünf Jahren . . . . .	9
3.3	gefälschte E-Mail von PayPal . . . . .	10
3.4	Poster der Polizei Nordrhein-Westfalen . . . . .	12



## Glossar

**Immersion** Immersion beschreibt den durch eine Umgebung der Virtuellen Realität hervorgerufenen Effekt, der das Bewusstsein des Nutzers, illusorischen Stimuli ausgesetzt zu sein, so weit in den Hintergrund treten lässt, dass die virtuelle Umgebung als real empfunden wird.[\[Wiki 24a\]](#). i, v

**Spoofing** Beim Spoofing wird eine andere Nummer beim Angerufenen angezeigt als die, von der aus wirklich telefoniert wird. So kann der Social Engineer jede gewünschte Nummer faken. [\[Chri 14d\]](#). i