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

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

TECHNISCHE HOCHSCHULE NÜRNBERG
GEORG SIMON OHM

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/**

DokID: SB_0050_FO_Erklärung_zur_Veröffentlichung_der_Abschlussarbeit_prüfungsrechtliche Erklärung_public Vers. 2, 22.09.2017, A. Härtel (4.SB)

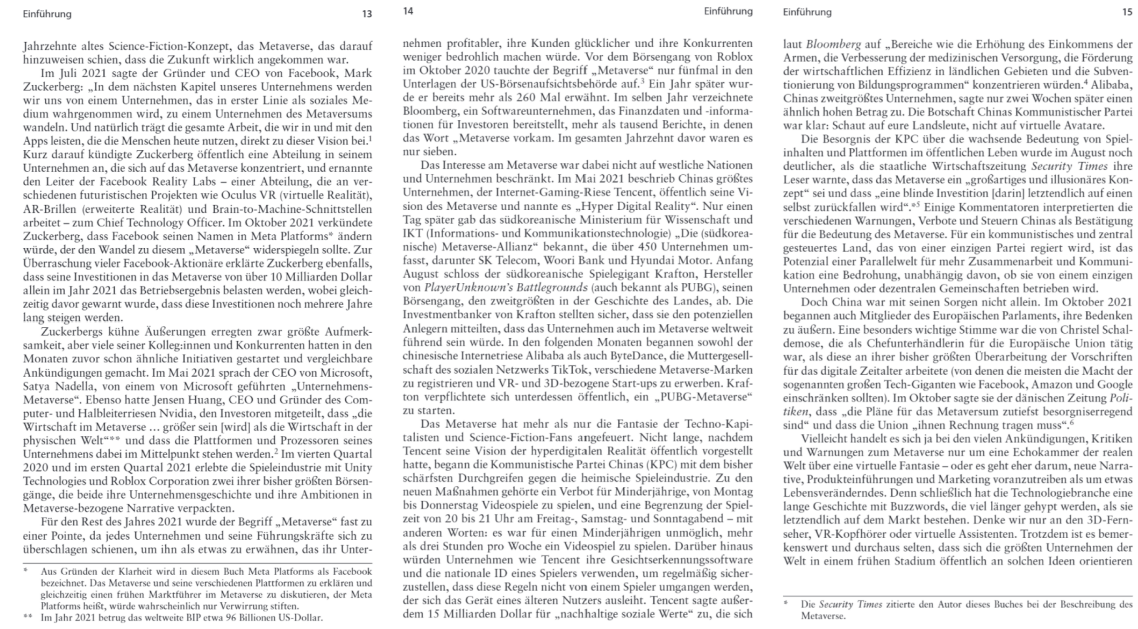
Anleitungen und Tests

1 Anleitungen

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 library as an example.

Bilder einfügen nach paragraph muss was stehen bevor das bild kommt



Einführung 13

Jahrzehnte altes Science-Fiction-Konzept, das Metaverse, das darauf hinzuweisen schien, dass die Zukunft wirklich angekommen war.

Im 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 wahrgenommen wird, zu einem Unternehmen des Metaversums wandeln. Und natürlich trägt die gesamte Arbeit, die wir in und mit den Apps leisten, die die Menschen heute nutzen, direkt zu dieser Vision bei.[1] Kurz darauf kündigte Zuckerberg öffentlich eine Abteilung in seinem Unternehmen an, die sich auf das Metaverse konzentriert, und ernannte den Leiter der Facebook Reality Labs – 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* ändern würde, der den Wandel zu diesem „Metaverse" widerspiegeln sollte. Zur Überraschung vieler Facebook-Aktionäre 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.

Zuckerbergs kühne Äußerungen erregten zwar größte Aufmerksamkeit, aber viele seiner Kolleg:innen 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"** und dass die Plattformen und Prozessoren seines Unternehmens dabei im Mittelpunkt stehen werden.[2] 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.

Für den Rest des Jahres 2021 wurde der Begriff „Metaverse" fast zu einer Pointe, da jedes Unternehmen und seine Führungskräfte sich zu überschlagen schienen, um ihn als etwas zu erwähnen, das ihr Unter-

* Aus Gründen der Klarheit wird in diesem Buch Meta Platforms als Facebook bezeichnet. Das Metaverse und seine verschiedenen Plattformen zu erklären und gleichzeitig einen frühen Marktführer im Metaverse zu diskutieren, der Meta Platforms heißt, würde wahrscheinlich nur Verwirrung stiften.

** Im Jahr 2021 betrug das weltweite BIP etwa 96 Billionen US-Dollar.

14 Einführung

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.[3] Ein Jahr später wurde er bereits mehr als 260 Mal erwähnt. Im selben Jahr verzeichnete Bloomberg, ein Softwareunternehmen, das Finanzdaten und -informationen für Investoren bereitstellt, mehr als tausend Berichte, in denen das Wort „Metaverse vorkam. Im gesamten Jahrzehnt davor waren es nur sieben.

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" bekannt, die über 450 Unternehmen umfasst, darunter SK Telecom, Woori Bank und Hyundai Motor. Anfang August schloss der südkoreanische Spielegigant Krafton, Hersteller von *PlayerUnknown's Battlegrounds* (auch bekannt als PUBG), seinen Börsengang, den zweitgrößten in der Geschichte des Landes, ab. Die Investmentbanker 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.

Das Metaverse hat mehr als nur die Fantasie der Techno-Kapitalisten und Science-Fiction-Fans angefeuert. Nicht lange, nachdem Tencent seine Vision der hyperdigitalen Realität öffentlich vorgestellt hatte, begann die Kommunistische Partei Chinas (KPC) mit dem bisher schärfsten Durchgreifen gegen die heimische Spieleindustrie. Zu den neuen Maßnahmen gehörte ein Verbot für Minderjährige, 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 einen Minderjährigen unmöglich, mehr als drei Stunden pro Woche ein Videospiel zu spielen. Darüber hinaus würden 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 ausleiht. Tencent sagte außerdem 15 Milliarden Dollar für „nachhaltige soziale Werte" zu, die sich

Einführung 15

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 Bildungsprogrammen" konzentrieren würden.[4] 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.

Die Besorgnis der KPC über die wachsende Bedeutung von Spielinhalten und Plattformen im öffentlichen Leben wurde im August noch deutlicher, als die staatliche Wirtschaftszeitung *Security Times* ihre Leser warnte, dass das Metaverse ein „großartiges und illusionäres Konzept" sei und dass „eine blinde Investition [darin] letztendlich auf einen selbst zurückfallen wird".*[5] 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.

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 Chefunterhändlerin 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 *Politiken*, dass „die Pläne für das Metaversum zutiefst besorgniserregend sind" und dass die Union „ihnen Rechnung tragen muss".[6]

Vielleicht 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 dem Markt bestehen. Denke wir nur an den 3D-Fernseher, VR-Kopfhörer oder virtuelle Assistenten. Trotzdem ist es bemerkenswert und durchaus selten, dass sich die größten Unternehmen der Welt in einem frühen Stadium öffentlich an solchen Ideen orientieren

* Die *Security Times* 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 [Hypp 22]
Psychologie hinter SocialEngeneering [Schu 11]

URL einfügen https://ar5iv.labs.arxiv.org/html/2401.05569

You can also write footnotes.[1]

äüö

[1]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

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 24]

»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 24]

»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])

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 21])

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 Weihegenschenk 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 stünde. 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 Karnevallsprogramm bis ins kleinste Detail ausführten.(vgl. [Time 87]) Im Jahr 1899 prägte William Tolman den Begriff SSocial Engineeringünd 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])

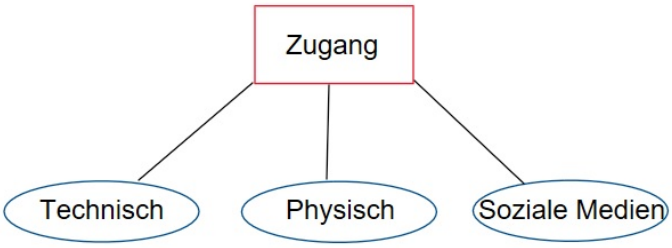


Abbildung 3.1: verschiedene Zugangsarten
(eigene Darstellung)

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

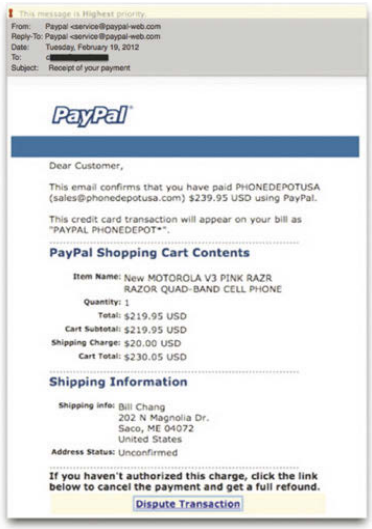
3.3.1 Phishing

Phishing scams might be the most common types of social engineering attacks used today. Most phishing scams tend to have the following characteristics (Bisson, 2015): • They seek to obtain personally identifiable information (PII), such as names, addresses and social security numbers. • They tend to use shortened URLs or embed links that redirect users to sites that appear legitimate. • They usually attempt to instill a sense of urgency in the user by using some sort of fear tactic or a threat in an attempt to get the user to act immediately. Some phishing emails are more poorly crafted than others to the extent that their messages oftentimes exhibit spelling and grammar errors but these emails are no less focused on

directing victims to a fake website or form where they can steal user login credentials and other personal information (Workman, 2008). A recent scam sent phishing emails to users after they installed cracked APK files from Google Play Books that were pre-loaded with malware. This specific phishing campaign demonstrates how attackers commonly pair malware with phishing attacks in an effort to steal users' information (Whitwam, 2015).

Die Form des „Phishing“ oder eben des Angelns nach Informationen ist die wohl am weitesten verbreitete, vor allem durch den Versand von Massen-E-Mails oder durch zielgerichtete E-Mails. In diesen E-Mails sind schädliche Dateien, Links oder Instruktionen für den Adressaten enthalten. Die Konsequenzen durch eine Öffnung dieser Mails sind vielschichtig und oft äußerst bedrohlich. Ebenfalls unter die Kategorie des „Phishing“ fallen die zielgerichteten Angriffe auf (hochrangige) Exponenten von Unternehmen. Wenn es sich um persönlich formulierte E-Mails, die bereits Detailinformationen über den Adressaten beinhalten handelt, sprechen wir von „Spear-Phishing“ – abgeleitet vom Speer, welcher sich fokussiert auf ein Subjekt richtet.

In der Umgangssprache bekannt und in letzter Zeit eine immer häufiger angewendete Form des Phishing ist der CEO-Fraud oder eben das „Whaling“ – abgeleitet vom Wal. Dies umschreibt das Spear-Phishing auf ein hochrangiges Individuum. Die Schäden aus diesen Whaling-Methoden sind enorm, und die Anzahl dieser Angriffe, auch „Business E-mail Compromise (BEC)“ genannt, steigt rasant (Federal Bureau of Investigations 2016). Das Internet Complaint Center des FBI hat im Jahr 2016 bereits über 22.000 Unternehmen und Organisationen als Opfer dieser Betrugsform identifiziert. Die Dunkelziffer ist auch bei diesen Taten hoch, und man kann davon ausgehen, dass nur ein geringer Prozentsatz an Betroffenen an die Öffentlichkeit gelangt. Die fünf häufigsten Betrugsmuster gemäß dieser Studie des FBI aus dem Jahr 2016 seien die folgenden (Federal Bureau of Investigations 2016): 1. Drittparteien: Unternehmen werden mit gefälschten angeblichen Lieferantenangaben angeschrieben, Rechnungen an das vermeintliche Konto des Lieferanten – das auf die Täter lautet – zu bezahlen. In der Praxis lässt sich dieses Muster häufig beobachten. 2. CEO-Fraud: Anhand kompromittierter E-Mail-Accounts auf Stufe C-Level wie CEO, CFO, CTO, CSO, CIO (Geschäftsleitung/Vorstand) werden Mitarbeiter aufgefordert, Geld an ein bestimmtes Konto zu überweisen oder überweisen zu lassen. Die E-Mail-Konten können dabei gefälscht oder tatsächlich gehackt und übernommen worden sein. Die hier angewandte Methode ist auch unter den Namen „Business Executive Scam“ oder „Financial Industry Wire Frauds“ bekannt. 3. Datendiebstahl auf Basis CEO-Fraud: Gefälschte E-Mails auf Stufe C-Level werden genutzt, um sensible Daten abzugreifen. Es kann sich dabei um Daten aus der Personalabteilung, der Buchhaltung, des Controlling oder des Geschäftsleitungssekretariats handeln. 4. Weitere betrügerische Kommunikation: Die persönlichen E-Mail-Accounts von Mitarbeitern werden gehackt und zur Kommunikation mit Dritten (Geschäftspartnern, Kunden, Lieferanten etc.) genutzt. Auch hier wird wieder um Zahlung von Beträgen an die Konten der Täter gebeten.


This message is Highest priority.
From: Paypal <service@paypal-web.com>
Reply-To: Paypal <service@paypal-web.com>
Date: Tuesday, February 19, 2012
To: [redacted]
Subject: Receipt of your payment

PayPal

Dear Customer,

This email confirms that you have paid PHONEDEPOTUSA (sales@phonedepotusa.com) $239.95 USD using PayPal.

This credit card transaction will appear on your bill as "PAYPAL PHONEDEPOT*".

PayPal Shopping Cart Contents

Item Name: New MOTOROLA V3 PINK RAZR RAZOR QUAD-BAND CELL PHONE
Quantity: 1
Total: $219.95 USD
Cart Subtotal: $219.95 USD
Shipping Charge: $20.00 USD
Cart Total: $230.05 USD

Shipping Information

Shipping info: Bill Chang
202 N Magnolia Dr.
Saco, ME 04072
United States
Address Status: Unconfirmed

If you haven't authorized this charge, click the link below to cancel the payment and get a full refound.

Dispute Transaction

Abbildung 3.2: gefälschte E-Mail von PayPal
[Chri 14]

3.3.2 Elizitieren per Telefon

3.3.3 Identitätsbetrug

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 Tailgating/Piggybacking

3.5 Psychologische Prinzipien hinter Social Engineering

3.5.1 Mittel der Manipulation

3.5.2 Mittel der Beeinflussung

3.5.2.1 stereotypes Verhalten

3.5.2.2 Reziprozität

3.5.2.3 Verpflichtung und Konsistenz

3.5.2.4 Soziale Bewährtheit

3.5.2.5 Sympathie

3.5.2.6 Authorität

3.5.2.7 Knappheit

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 ëxklusiven 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.

[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.

[BSI 24] BSI. *Social Engineering – der Mensch als Schwachstelle.* [online] https://www.bsi.bund.de/dok/11287460, 19.06.2024.

[Chri 14] P. E. Christopher Hadnagy. *Social engineering enttarnt: Sicherheitsrisiko Mensch*, Chap. 2, s. 63. mitp-Verlags GmbH u. Co. KG, 2014.

[Hadn 11a] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe.* mitp-Verlags GmbH u. Co. KG, 2011.

[Hadn 11b] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe.* mitp-Verlags GmbH u. Co. KG, 2011.

[Hypp 22] M. Hyppönen. *Was vernetzt ist, ist angreifbar: Wie Geheimdienste und Kriminelle uns im Netz infiltrieren.* John Wiley and Sons, Inc., 2022.

[Kevi 11a] W. S. Kevin Mitnick. *Die Kunst der Täuschung: Risikofaktor Mensch*, s. 4. mitp-Verlags GmbH u. Co. KG, 2011.

[Kevi 11b] W. S. Kevin Mitnick. *Die Kunst der Täuschung: Risikofaktor Mensch.* mitp-Verlags GmbH u. Co. KG, 2011.

[Mali 09] A. Malinar. *Hinduismus*, S. 184 – 192. Vandenhoeck u. Ruprecht, 2009.

[MITN 24] MITNICKSECURITY. *The Early History of Social Engineering.* [online], https://www.mitnicksecurity.com/the-history-of-social-engineering, 16.06.2024.

[Mout 18] F. Mouton. *SOCIAL ENGINEERING ATTACK DETECTION MODEL Thesis*, S. 12–13. Department of Computer Science in der University of Pretoria, 2018.

[Ozka 18] E. Ozkaya. *Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert*, S. 11 – 13. Packt Publishing, Limited, 2018.

[Schu 11] S. Schumacher. *Magdeburger Journal zur Sicherheitsforschung.* Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg, 2011.

[Stir 21] S. Stirnimann. *Der Mensch als Risikofaktor bei Wirtschaftskriminalität*, Chap. 4, s. 127. Springer Fachmedien Wiesbaden GmbH, 2021.

[Tayl 03] 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 ßocial 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 24] Wikipedia. *Social Engineering.* [online], TODO Link einfügen, 11.07.2024.

Abbildungsverzeichnis

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. Wikipedia. i

library A suite of reusable code inside of a programming language for software development. i, v

shell Terminal of a Linux/Unix system for entering commands. i