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)

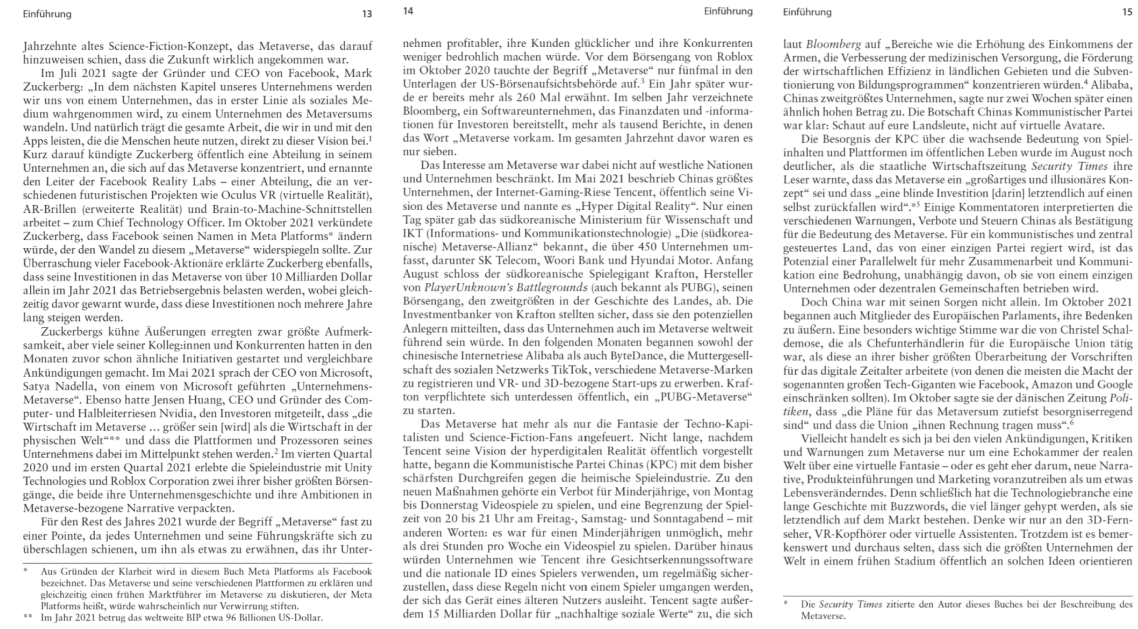
Anleitungen und Tests

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 Definition des Social Engineering

»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 kan der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen.«[Kevi 11]

Was ist Social Engineering? 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]

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

Arzte Psychologen und Therapeuthen 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 11]

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, gleichfalls gibt es alternative Definitionen für Social Engineering (Politikwissenschaft).[1 8]

3.2 Geschichte des Social Engineering

copy

1 Die Geschichte des Social Engineerings ist eng mit der Entwicklung menschlicher Kommunikation und Interaktion verbunden. Social Engineering bezeichnet in diesem Kontext die Kunst der Manipulation von Menschen, um sie dazu zu bringen, vertrauliche Informationen preiszugeben oder bestimmte Handlungen auszuführen. Diese Praktik kann für verschiedene Zwecke eingesetzt werden, von Spionage und Betrug bis hin zur Sicherheitsanalyse. Im Folgenden skizziere ich einige Schlüsselmomente und Entwicklungen in der Geschichte des Social Engineerings, die für deine Bachelorarbeit relevant sein könnten:

Frühe Geschichte und Kriegsführung: Bereits in antiken Geschichten und Kriegen spielte Social Engineering eine Rolle, etwa wenn Spione Informationen sammelten oder wenn durch List und Täuschung Kriege gewonnen wurden. Ein berühmtes Beispiel aus der griechischen Mythologie ist das Trojanische Pferd, das als Strategie betrachtet werden kann, den Feind durch Täuschung zu besiegen.

19. und frühes 20. Jahrhundert: Mit der Industrialisierung und der zunehmenden Komplexität der Gesellschaft nahmen auch Betrug und Täuschung zu. Berühmte Betrüger wie Victor Lustig, der angeblich den Eiffelturm "verkaufte", nutzten Social Engineering-Techniken, um ihre Betrügereien durchzuführen.

Zweiter Weltkrieg: Im Zweiten Weltkrieg wurde Social Engineering von verschiedenen Geheimdiensten eingesetzt, um Spionage zu betreiben und feindliche Operationen zu stören. Die Operation Fortitude, bei der die Alliierten die Deutschen über den tatsächlichen Ort der D-Day-Invasion täuschten, ist ein Beispiel für erfolgreiches Social Engineering.

Das Zeitalter der Informationstechnologie: Mit dem Aufkommen von Computern und dem Internet hat sich Social Engineering weiterentwickelt. Phishing-Angriffe, bei denen Betrüger versuchen, über gefälschte E-Mails sensible Informationen zu erlangen, sind ein gängiges Beispiel. Kevin Mitnick, ein berühmter Hacker, nutzte in den 1980er und 1990er Jahren Social Engineering, um in Netzwerke einzudringen, indem er sich als Mitarbeiter ausgab und Passwörter oder andere kritische Informationen erbeutete.

21. Jahrhundert: Heute ist Social Engineering ein kritisches Element der Cybersecurity. Unternehmen und Organisationen müssen sich gegen eine Vielzahl von Social Engineering-

Angriffen wappnen, darunter Spear-Phishing, Pretexting und Baiting. Die zunehmende Vernetzung und Digitalisierung bieten Angreifern immer neue Angriffsflächen.

Ausbildung und Gegenmaßnahmen: Die Erkenntnis, dass der menschliche Faktor oft das schwächste Glied in der Sicherheitskette ist, hat zur Entwicklung von Schulungsprogrammen und Gegenmaßnahmen geführt. Unternehmen investieren in die Ausbildung ihrer Mitarbeiter, um sie über die Risiken des Social Engineerings aufzuklären und ihnen beizubringen, wie sie Angriffe erkennen und vermeiden können.

In deiner Bachelorarbeit könntest du darauf eingehen, wie Social Engineering-Techniken sich im Laufe der Zeit verändert haben und welche Methoden heute am effektivsten sind. Außerdem könnte die Untersuchung der psychologischen Aspekte, die Social Engineering so wirkungsvoll machen, sowie der Gegenstrategien, die Organisationen entwickeln, um sich zu schützen, interessante Themenbereiche sein.

Für eine fundierte Bachelorarbeit zum Thema Social Engineering sind akademische und zuverlässige Quellen essenziell. Hier sind einige empfohlene Ressourcen, die als Ausgangspunkt für deine Recherche dienen können. Bitte beachte, dass du für die aktuellsten Informationen und spezifische Fallstudien auch auf Artikel in Fachzeitschriften und Konferenzberichte zugreifen solltest.

Bücher und Monografien: Workman, Michael. A Test of Interventions for Security Threats from Social Engineering. Information u. Management, 45(8), 2008, Seiten 507-512. Dieser Artikel untersucht, wie Bildung und Bewusstsein die Anfälligkeit für Social Engineering-Angriffe reduzieren können. Gragg, Derrick. Ä Multi-Level Defense Against Social Engineering.SSANS Institute InfoSec Reading Room, 2003. Ein technischer Bericht, der Strategien zur Abwehr von Social Engineering bietet. Offizielle Dokumentationen und Richtlinien:

National Institute of Standards and Technology (NIST). "Guide to Malware Incident Prevention and Handling for Desktops and Laptops."NIST Special Publication 800-83, Revision 2. NIST Publikationen bieten Richtlinien und Best Practices für die IT-Sicherheit, einschließlich des Schutzes gegen Social Engineering. Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz-Kompendium. Das BSI bietet umfassende Richtlinien zur IT-Sicherheit, einschließlich Empfehlungen zum Umgang mit Social Engineering.

Für eine vertiefende Auseinandersetzung mit der Geschichte des Social Engineerings und dessen vielschichtigen Aspekten gibt es einige Schlüsselwerke, die du in deiner Forschung heranziehen kannst. Diese Bücher bieten sowohl historische Einblicke als auch praktische Beispiele und theoretische Rahmenbedingungen, um das Phänomen des Social Engineerings umfassend zu verstehen:

Social Engineering: The Art of Human Hacking von Christopher Hadnagy Veröffentlicht: 2010 Verlag: Wiley ISBN: 978-0470639535 Inhalt: Dieses Buch bietet eine umfassende Einführung in die Techniken des Social Engineerings, illustriert durch echte Beispiele und Fallstudien. Hadnagy diskutiert sowohl die psychologischen Grundlagen als auch die Anwendung von Social Engineering in verschiedenen Kontexten.

The Art of Deception: Controlling the Human Element of Security von Kevin Mitnick und William L. Simon Veröffentlicht: 2002 Verlag: Wiley ISBN: 978-0764542800 Inhalt: Kevin Mitnick, einer der bekanntesten Hacker und ehemaligen Social Engineers, teilt seine Erfahrungen und beschreibt detailliert, wie Social Engineering-Angriffe durchgeführt werden. Das Buch hebt die Bedeutung der menschlichen Psychologie hervor und bietet Einblicke, wie man sich gegen solche Angriffe schützen kann.

"Ghost in the Wires: My Adventures as the Worlds Most Wanted Hacker"von Kevin Mitnick Veröffentlicht: 2011 Verlag: Little, Brown and Company ISBN: 978-0316037709 Inhalt: Dieses Buch ist eine Autobiografie von Kevin Mitnick, die seine Karriere als Hacker nachzeichnet und dabei viele Aspekte des Social Engineerings beleuchtet, einschließlich detaillierter Beschreibungen von seinen berühmtesten Hacks und den dabei angewandten Social Engineering Techniken.

"Phishing for Phools: The Economics of Manipulation and Deception"von George A. Akerlof und Robert J. Shiller Veröffentlicht: 2015 Verlag: Princeton University Press ISBN: 978-0691168319 Inhalt: Obwohl dieses Buch sich primär auf wirtschaftliche Manipulation konzentriert, bietet es wertvolle Einblicke in die Mechanismen und Strategien, die auch im Social Engineering eine Rolle spielen. Es erklärt, wie Menschen zu Entscheidungen verleitet werden, die nicht in ihrem besten Interesse sind.

Online-Ressourcen SANS Institute Reading Room. https://www.sans.org/reading-room/ Der Reading Room des SANS Institute enthält eine Fülle von Forschungsartikeln und Berichten zu verschiedenen Aspekten der Cybersicherheit, einschließlich Social Engineering. Cybersecurity und Infrastructure Security Agency (CISA). https://www.cisa.gov/ CISA bietet Ressourcen und Alerts zu aktuellen Bedrohungen und Anfälligkeiten, auch bezüglich Social Engineering. Bitte beachte, dass der Zugang zu einigen akademischen Artikeln und Büchern eingeschränkt sein kann und möglicherweise über Bibliotheken oder akademische Datenbanken wie JSTOR, Google Scholar oder die Datenbank deiner Universität zugänglich ist. Es ist auch empfehlenswert, die Zitationen in diesen Quellen zu prüfen, um weitere relevante Literatur zu finden.

SANS Institute InfoSec Reading Room URL: https://www.sans.org/reading-room/ Inhalt: Der Reading Room bietet eine Vielzahl von Artikeln und Whitepapers zu Themen der Informationssicherheit, einschließlich ausführlicher Analysen zum Social Engineering.

eigene Version

Im Zeitalter der digitalen Kommunikation ergeben sich jedoch äußerst effektive, neue Möglichkeiten für Kriminelle, mit denen sie Millionen von potenziellen Opfern erreichen können[BSI 24]

3.3 Angriffsmuster

3.4 Zugangsarten

3.4.1 Elektronisch

3.4.2 Physischer

3.4.3 Soziale Medien

3.5 Angriffsvektoren

3.5.1 Phishing

3.5.2 Elizitieren

3.5.3 Pretexten

3.5.4 Dumpster diving

3.5.5 Watering Hole

3.5.6 Ködern

3.5.7 Honigtopf

3.5.8 Tailgating/Piggybacking

3.5.9 Business Email Compromise

3.6 Psychologische Prinzipien hinter Social Engineering

3.6.1 stereotypes Verhalten

3.6.2 Reziprozität

3.6.3 Verpflichtung und Konsistenz

3.6.4 Soziale Bewährtheit

3.6.5 Sympathie

3.6.6 Authorität

3.6.7 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

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

eigene

5.2 Aufklärung und Bewusstseinsbildung

TODO

Brillen können gehackt werden Biometrische Daten ausgelesen werden wie mimiken etc

5.3 Deep Fakes

TODO

Avatar ist ein Gegenstand und kann lauschen Technische Sicherheitsmaßnahmen

Kapitel 6

Fazit und Ausblick

TODO

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

Literaturverzeichnis

[1 8] 1. 7, Chap. 2, s. 4. 5, 6, 8.

[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.

[Hadn 11] C. Hadnagy. *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe.* mitp, 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 11] W. S. Kevin Mitnick. *Die Kunst der Täuschung: Risikofaktor Mensch*, s. 4. mitp, 2011.

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

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