The Social Engineer

Ein immersives Agentenspiel in Virtual Reality zur Bewusstseinssteigerung gegenüber Social Engineering

Motivation

Millionen von Zuschauern fiebern im Kino oder vor dem heimischen Bildschirm mit, wenn Elliot in *Mr. Robot*[1] Informationen von Social Media Profilen nutzt, um Sicherheitskräfte auszutricksen und Zugang zu Sicherheitssystemen von Firmen zu gelangen, wenn sich Debbie in *Ocean's 8*[2] als Reinigungskraft verkleidet, um so heimlich in einer Businesskonferenz ein Abhörgerät zu platzieren, oder wenn sich Benjamin in *Who Am I*[3] als hilfesuchender Schüler ausgibt, um das WLAN in der Europol-Zentrale anzuzapfen. In all diesen Fällen ist es das bewusste Ausnutzen des Menschen als Schwachstelle, die kalkulierte Manipulation der menschlichen Psyche, und der direkte Kontakt zwischen Angreifer und Opfer, was für Faszination bei den Zuschauern sorgt. Während klassische Hacker meist versuchen, technische Systeme aus einem dunklen Keller heraus zu knacken, wird bei so genannten *Social Engineering* Angriffen versucht, Menschen so zu täuschen und zu manipulieren, dass sie vertrauliche Informationen herausrücken oder Zugänge zu beschränkten Orten gewähren.[4] Klassische Arten von *Social Engineering* Attacken sind unter anderem das Vortäuschen einer falschen Identität im direkten Kontakt (*Impersonation*), am Telefon (*Vishing*) oder per E-Mail (*Phishing*), das Untermischen in eine Gruppe von Menschen (*Tailgaiting*), das Verteilen von Schadsoftware durch liegengelassene USB-Sticks (*USB Baiting*), oder das Ausnutzen von privaten Informationen aus dem Internet (*Social Networking*).[5] Opfer von *Social Engineering* Angriffen sind meist Mitarbeiter/innen von Firmen mit Zugang zu sicherheitskritischen Daten, aber auch Privatpersonen. Während *Social Engineering* Attacken in Hollywood als Grundlage für spektakuläre Filmszenen genutzt werden, verursachen sie in der Wirtschaft jährlich einen hohen finanziellen Schaden. So war laut Bitkom im Jahr 2019 bereits mehr als jedes fünfte Unternehmen in Deutschland von *Social-Engineering* Attacken betroffen.[6] Dabei ist nach Angaben von Sicherheitsexperten das fehlende Bewusstsein von Mitarbeiter/innen in Betrieben eine der häufigsten Ursachen von erfolgreichen *Social Engineering* Attacken.[7]

---

[1] https://www.imdb.com/title/tt4158110/?ref_=ttep_ep_tt
[2] https://www.imdb.com/title/tt5164214/?ref_=nv_sr_srsg_0
[3] https://www.imdb.com/title/tt3042408/?ref_=nv_sr_srsg_0
[4] https://ieeexplore.ieee.org/document/6950510
[5] https://www.sciencedirect.com/science/article/abs/pii/S2214212614001343?via%3Dihub
[6] https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf
[7] Gavin Watson, Andrew Mason, and Richard Ackroyd. 2014. Social engineering penetration testing: executing social engineering pen tests, assessments and defense. Syngress.

Sowohl die vielseitige Möglichkeit an *Social Engineering* Szenarien als auch die oft unterschätzte Gefahr dieser Angriffe waren für uns die Motivation, das Konzept für das Spiel *The Social Engineer* zu entwickeln. Darin schlüpfen Spielerinnen und Spieler in die Rolle einer Mitarbeiterin bzw. eines Mitarbeiters einer Sicherheitsfirma, um in unterhaltsamen sowie gewaltfreien Szenarien, und durch Anwenden verschiedener *Social-Engineering* Techniken, Schwachstellen in fiktiven Unternehmen aufzudecken. Die Verwendung von Virtual Reality als Spieleplattform sorgt dabei für ein realistisches und immersives Spielerlebnis. Das Ziel des Spiels ist es, über die Möglichkeiten und Gefahren von *Social Engineering* aufzuklären, und das Bewusstsein gegenüber dem Thema zu steigern. Das Spielkonzept und die im Spiel verwendeten Attacken wurden in Zusammenarbeit mit einer IT-Sicherheitsfirma erarbeitet, mit dem Ziel, dass das Spielen von *The Social Engineer* zu einer erhöhten Sensibilisierung im privaten und beruflichen Alltag führt. Während die Hauptzielgruppe des Spiels private Spieler/innen sind, kann das Spiel ferner auch als Selbsttrainingstool in Firmen oder im Rahmen von Sicherheitsschulungen verwendet werden.

Abbildung 1: Eindrücke aus The Social Engineer*: (a) Spieler benutzt USB-Stick in einem Büro, (b) Startsequenz im Home-Office, (c) Außenansicht der fiktiven Firma, (d) Beobachten von Mitarbeiter/innen in der Firmenlobby, (e) Betrachten von Social-Media-Seiten einer Mitarbeiterin während eines Impersonation Angriffs.*

Spielkonzept

Im Virtual Reality Spiel *The Social Engineer* (siehe Abbildung 1) übernehmen Spieler/innen in der Egoperspektive eine Rolle als *Social Engineering Penetrationtester/in*. In einem fiktiven simulierten Unternehmen inklusive Sicherheitsmechanismen und Mitarbeiter/innen müssen sie im Rahmen eines Sicherheitstest unterschiedliche *Social Engineering* Angriffe durchführen und dabei verschiedene Schwachstellen aufdecken, ohne selbst entlarvt zu werden. In der Spielwelt können die Spieler/innen sich frei bewegen, sich mit Mitarbeiter/innen unterhalten sowie mit wichtigen Gegenständen interagieren. Einige Spielmechaniken sind inspiriert von bekannten Sandbox Stealth-Spielen wie *Hitman*[8], *Thief*[9] oder *Invisible*[10]. Im Gegensatz zu den genannten Spielen, verzichtet *The Social Engineer* jedoch vollständig auf Waffen und Gewalt, und kreiert durch die Einbindung von echten *Social Engineering* Techniken ein komplett neues Spielerlebnis.

Zu Beginn des Spiels erhalten Spieler/innen eine Missionsbeschreibung in Form eines Videoanrufs ihrer IT-Sicherheitsfirma, welche Informationen über die involvierte Zielfirma, eine Liste von benötigten *Social Engineering* Techniken sowie verschiedene Missionsziele enthält. Durch den Open-World-Ansatz des Spiels können Missionsziele auf unterschiedliche Art und Weise erreicht werden, immer ist jedoch eine korrekte Ausführung von verschiedenen *Social Engineering* Techniken in der richtigen Reihenfolge

[8] https://store.steampowered.com/app/236870/HITMAN/
[9] https://store.steampowered.com/app/239160/Thief/
[10] https://store.steampowered.com/app/243970/Invisible_Inc/

und ohne dabei entdeckt zu werden notwendig, um ein Missionsziel zu erreichen. Dabei demonstriert das Spiel die direkten Auswirkungen und Gefahren von *Social Engineering* Attacken. Wenn Spieler/innen auffliegen, können sie eine Mission von einem Checkpoint aus erneut starten. Nach jedem erreichten Missionsziel erhalten Spieler/innen eine Missionszusammenfassung mit nützlichen Do's and Don'ts zum Abwehren und Vermeiden von *Social Engineering* Attacken im echten Leben als Take-Away-Nachricht.

Um das Spiel erfolgreich zu spielen, sind weder ein spezielles Vorwissen über *Social Engineering* oder Computerwissen im Allgemeinen noch spezielle Kompetenzen notwendig. Es ist somit für eine breite Zielgruppe geeignet. Während des Spiels können Spieler/innen jederzeit auf eine integrierte Informationen über alle benötigten *Social Engineering* Attacken zurückgreifen. Zusätzlich können Spieler/innen Hilfe in Form von kurzen Ein-Satz-Anweisungen anfordern, welche ein weiteres Vorgehen vorschlagen, sowie im Spiel platzierte Hinweisindikatoren aufsuchen, falls sie einmal feststecken und nicht weiter kommen.

Abbildung 2: Interaktionen im Spiel The Social Engineer*: (a) Teleportationssystem zur Erkundung der Firma, (b) Dialog mit einer Mitarbeiterin, (c) Platzieren eines USB-Sticks, (d) Auswählen einer App im virtuellen Tablet.*

Virtual Reality Prototyp

Das Spielkonzept haben wir in Form eines Virtual Reality Prototypen umgesetzt, welcher aus einer detaillierten Spielwelt und einer aus drei Zielen bestehenden Mission in einer fiktiven Werbeagentur besteht und ein möglichst großes Spektrum an verschiedenen Arten von *Social Engineering* Attacken abdeckt. Dafür haben wir ein typisches Bürogebäude mit komplett eingerichteten Räumen erstellt, und Nicht-Spieler-Charaktere entwickelt, welche typische Rollen und Arbeitsabläufe einer Werbeagentur übernehmen sowie auf unterschiedliche Weise auf die Aktionen der Spieler/innen reagieren. In der Spielwelt und im Verhalten der Mitarbeiter/innen sind verschiedene typische Schwachstellen verteilt. Der Prototyp enthält drei voneinander unabhängige Missionsziele, welche alle in einem Durchlauf erreicht werden können. Diese sind auf verschiedene Abteilungen der Werbeagentur verteilt:

- In der Kreativabteilung müssen Informationen über bisher unveröffentlichte Designentwürfe gesammelt werden.
- Aus der zugangsbeschränkten IT-Abteilung sollen IT-Daten entwendet werden.
- In der Verwaltungsabteilung müssen Bilder von vertraulichen Finanzdaten gemacht werden.

Der Prototyp wurde als Virtual Reality Spiel umgesetzt, um ein möglichst realistisches und immersives Spielerlebnis zu schaffen. Neben der 360-Grad-Ansicht der Spielwelt wird dies insbesondere durch realistische Interaktionen erreicht. Dafür sind eine vordefinierte Spielfläche, ein VR Headset und zwei Controller nötig. Das Spiel besteht aus vier grundlegenden Interaktionen:

- Erkundung der Spielwelt: Alle echten Bewegungen der Spieler/innen werden in die virtuelle Welt übertragen. Dadurch kann die Spielwelt erkundet werden. Zusätzlich kann ein Teleportationssystem benutzt werden, um größere Strecken zurückzulegen, sich zu drehen, wenn der Rand des Spielfelds erreicht wird, oder falls kein Spielfeld zur Verfügung steht (siehe Abbildung 2a).

- Dialog mit Mitarbeiter/innen: Spieler/innen können mit den meisten Personen in der Werbeagentur ein Gespräch in Form eines textbasierten Dialogs führen. Verschiedene Antwortoptionen können mit dem Controller ausgewählt werden (siehe Abbildung 2b).
- Interaktion mit Objekten: Die Bewegungen der Controller werden im Spiel als virtuelle Hände dargestellt. Dadurch können wichtige Elemente wie USB-Sticks aufgehoben und bedient werden (siehe Abbildung 2c).
- Virtuelles Tablet: Das wichtigste Tool im Spiel ist ein virtuelles Tablet, welches in einer Hand getragen wird und wie ein richtiges Tablet durch Touch-Interaktionen mit der anderen Hand bedient wird. Es fungiert als Spielmenü und enthält eine Sammlung an Apps, welche genutzt werden können, um Informationen zu erhalten und verschiedene *Social Engineering* Angriffe zu starten (siehe Abbildung 3). Die enthaltenen Apps sind unter anderem ein Browser mit Informationen über die Zielfirma, eine Social Media App mit Profilen der Mitarbeiter/innen, eine Telefon App zum Anrufen von Mitarbeiter/innen, eine Dokumenten App zum Ansehen gefundener Dokumente, eine Foto App zum Fotografieren der Spielwelt, eine Map App welche einen Gebäudeplan enthält, eine Wiki App mit Informationen über verschiedene *Social Engineering* Attacken, sowie eine Help App um Hinweise für das weitere Vorgehen zu erhalten.

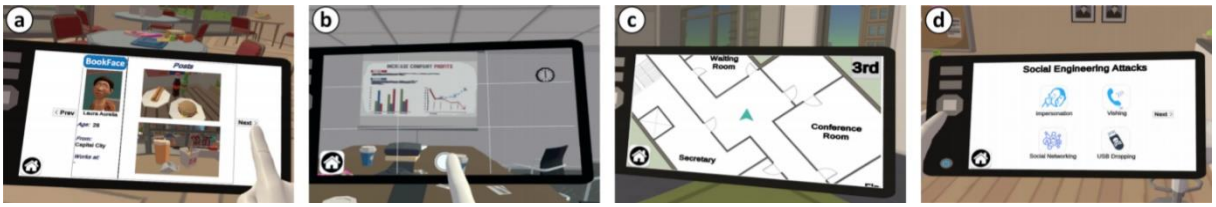

Abbildung 3: Apps des virtuellen Tablets: (a) Social Media App mit Informationen über Angestellte, (b) Foto App, (c) Map App welche einen Gebäudeplan enthält, (d) Wiki App mit Informationen über verschiedene Social Engineering *Angriffsarten.*

Entwicklungsphase des Prototyps

Das Konzept und der Prototyp des Spiels wurden im Zeitraum von zwei Jahren als Universitätsprojekt entwickelt. Um inhaltliche Korrektheit und Integrität zu gewährleisten, haben wir ein informelles Interview mit zwei *Social Engineering* Experten von einer IT-Sicherheitsfirma[11] sowie einem Experten im Bereich *Serious Games* geführt. Gemeinsam haben wir überlegt, wie ein geeignetes Spielkonzept rund um das Thema *Social Engineering* aussehen kann, welche Attacken sich am besten in so einem Spiel umsetzen lassen, und welche Aspekte ein Spiel enthalten muss, um nachhaltig das Bewusstsein steigern zu können.

Aus den Ergebnissen des Interviews haben wir uns fiktive Szenarien bestehend aus einer Firma, deren dazugehörigen Mitarbeiter/innen und typischen Schwachstellen erstellt. Diese wurden in Stories verwandelt, welche das Verwenden von *Social Engineering* Attacken enthalten. Daraus haben wir einen Paper Prototypen in Form eines Brettspiels erstellt, welcher aus einem Gebäudeplan als Spielfeld, Spielfiguren als Mitarbeiter/innen und Karten für Dialoge und Menüs bestand. Diesen haben wir verwendet, um in Testdurchläufen herauszufinden, ob Spieler/innen das generelle Spielkonzept verstehen und ob die Schwierigkeit der Missionen angemessen ist.

Daraufhin haben wir die VR Version des Spielkonzepts implementiert. Während der Implementierung lag der Fokus besonders auf dem Gesamtkonzept des Spiels. Wir wollten schlüssige Stories welche zu Spielspaß und einem Lerneffekt führen sowie eine einfache und realistische Interaktion mit dem Spiel erreichen. Auch eine detaillierte Spielwelt war uns wichtig. Der finale Prototyp ist ausgelegt für eine Benutzung mit der *HTC VIVE* VR-Brille, kann aber auch auf einer *Oculus Rift* VR-Brille gespielt werden.

[11] https://www.schutzwerk.com/de/15/Wir-ueber-uns.html

Awards und Förderungen

Dieser Prototyp war Basis für die Einreichung des Spiels beim *Deutschen Computerspielepreis 2021*. Dort wurde er in der Kategorie *Nachwuchspreis – Bester Prototyp* nominiert und mit einer Summe von 25.000 Euro gefördert. Zudem gewann das Spiel den *Audience Choice Award* bei der *CHI PLAY 2020 Student Game Design Competition*. Das Spiel soll nun in unserem neu gegründeten Unternehmen *Zefwih* bis zur Marktreife weiterentwickelt werden. Dazu müssen insbesondere das Konzept und das Gameplay so angepasst werden, dass das Spiel für eine breite Masse spielbar wird.

Vision

Unser Ziel ist es, das Spielkonzept und den Prototyp weiterzuentwickeln, und als vollständiges, unterhaltsames Spiel zu veröffentlichen, welches ohne Vorwissen gespielt werden kann und neben Spielspaß bestenfalls zu einer Steigerung des Bewusstseins gegenüber *Social Engineering* führt. Die Weiterentwicklung basiert dabei auf vier Säulen:

- Coop-Multiplayer: Das Spiel soll nicht nur von einer Person allein, sondern von mehreren Personen gleichzeitig in einem kooperativen Multiplayer-Modus spielbar werden.
- Gameplay: Das Gameplay, die vorhandenen Missionen und die Spielinteraktionen sollen weiter optimiert und ergänzt werden. Das Spiel soll für weitere Plattformen wie z.B. VR Spielehallen verfügbar gemacht werden und in weitere Sprachen wie Deutsch übersetzt werden, sodass eine größer Zielgruppe damit erreicht werden kann.
- Szenarien: Als Grundlage für weitere Levels sollen verschiedene Szenarien an unterschiedlichen Schauplätzen und mit abwechslungsreichen Stories entwickelt werden. Ideen für weitere Schauplätze, an welchen *Social Engineering* Angriffe stattfinden können, gibt es viele, wie z.B. Missionen in Banken, Krankenhäusern, Kraftwerken, Museen oder Kreuzfahrtschiffen. Zusätzlich wären weitere Ergänzungen wie eine Multiplayer-Koop-Modus denkbar, in welchem zwei oder mehr Spieler gemeinsam in einer Spielwelt eine Mission erfolgreich beenden müssen.
- Design: Die Ästhetik der Spielwelt soll verbessert werden, indem ein eigener Art Style verwendet wird. Insbesondere sollen dafür deutlich mehr eigene 3D-Modelle entwickelt sowie eine eigene akustische Untermalung kreiert werden.

Für das Erreichen dieser Visionen sind unter anderem weitere Mittel, weitere Personen, die bestimmte Fachgebiete, wie z.B. das Designen von 3D-Modellen beherrschen, sowie mehr Zeit notwendig. Unser Ziel ist es, die Weiterentwicklung und Veröffentlichung des Spiels durch passende Förderungen sowie mit dem durch Kooperationen weiter voranzutreiben.

Über uns

Wir sind ein Team von vier ehemaligen Studenten und Doktoranden der Universität Ulm, bestehend aus zwei Medieninformatik Masterstudenten (Fabian Fischbach und Pascal Jansen), einem Doktorand der Medieninformatik (Mark Colley) und einem Bachelorstudenten der Wirtschaftsmathematik (Daniel Hirschle). Zusammen haben wir zu Beginn des Jahres 2022 das Startup *Zefwih* gegründet, in welchem wir verschiedene digitale Medienprojekte umsetzen. Dazu gehören Konzepte, Anwendungen und Toolkits für die Bereiche Wirtschaft, Kultur und Forschung.

Links

Unternehmenswebseite: www.zefwih.com

Webseite – The Social Engineer: www.zefwih.com/the-social-engineer/

Trailer – The Social Engineer: https://www.youtube.com/watch?v=DrH3UVByfUc