Technische Universität München
Fakultät für Informatik

Seminararbeit
im Rahmen des Seminars
"Der Staat als Hacker"

Social Engineering und Phishing

Jens Fröhlich

12. Juni 2025

Inhaltsverzeichnis

1 Einleitung **2**

1.1 Social Engineering und Phishing 2

1.2 Relevanz des Themas 2

1.2.1 Fallzahlen 2

1.2.2 Wirtschaftliche Schäden und Auswirkungen auf Unternehmen und Privatpersonen 3

2 Definition von Social Engineering **3**

2.1 Grundprinzipien und Psychologie des Social Engineerings 3

2.2 Gängige Methoden 4

3 Definition von Phishing **4**

3.1 Definition und Abgrenzung als Teilbereich des Social Engineerings 4

3.2 Die Verschiedenen Arten von Phishing und ihre Ziele 4

4 Bekannte Phishing-Skandale und ihre Folgen **5**

4.1 Democratic National Committee (DNC)-Hack 5

4.2 Twitter Spear Phishing Attack (2020) 5

4.3 Weitere Skandale 5

5 Bezug zum Ethischen Hacking **5**

5.1 Social Engineering und Phishing als Werkzeuge im Penetration Testing . . . 5

5.2 Aufklärung und Sensibilisierung durch simulierte Angriffe 6

5.3 Rechtliche und ethische Rahmenbedingungen 6

6 Fazit und Ausblick **6**

6.1 Zusammenfassung 6

6.2 Bedeutung von Präventionsmaßnahmen und Sensibilisierung 6

6.3 Zukünftige Entwicklungen und Herausforderungen 6

1 Einleitung

1.1 Social Engineering und Phishing

"Hallo Mama/Papa, ich bin's. Ich habe mein Handy verloren und brauche dringend Geld. Kannst du mir bitte 100 Euro überweisen? Ich kann dir später alles erklären." - Diese Art an Nachricht wird wohl kaum einem neu vorkommen und ist ein gutes Beispiel für eine Thematik, die uns heutezutage immer häufiger begegnet: **Social Engineering**.

Dabei liegt der komplette Fokus auf dem Mensch als Schwachstelle, um durch gezielte psychologische Manipulation an vertrauliche Informationen zu gelangen. Dabei wird oft das Vertrauen des Opfers ausgenutzt, um es dazu zu bringen, sensible Daten preiszugeben oder bestimmte Handlungen vorzunehmen.[1]

Phishing im Speziellen ist eine besonders verbreitete Form des Social Engineerings. Hier handelt es sich konkret um den Versuch, über gefälschte E-Mails, Webseiten oder Nachrichten an persönliche Daten zu gelangen.[2]

1.2 Relevanz des Themas

1.2.1 Fallzahlen

Durch die hohe Erfolgsquote von Social Engineering bzw. Phishing stehen diese diese perfiden Angriffsmethoden nicht zu Unrecht so häufig im Rampenlicht. Knapp zwei von drei von sogenannten Databreaches sind auf das Element Mensch zurückzuführen, wovon mehr als 80% von diesen Breaches auf Phishing zurückzuführen sind. Zudem sind laut SlashNext die Zahl an Phishing-Angriffen ist seit 2021 um 49% gestiegen. Besonders hervorzuheben hierbei ist, dass der Anstieg mit der Veröffentlichung von ChatGPT das 4000-fach erreicht hat.[3]

Zudem hat IBM analysiert, dass in etwa 15% aller Datenschutzverletzungen auf Phishing, und dadurch auch Social Engineering, zurückzuführen sind.[4]

[1] *Social Engineering – der Mensch als Schwachstelle* 2025.
[2] *Spam, Phishing & Co* 2025.
[3] *Phishing Trends Report (Updated for 2025)* 2025.
[4] *Cost of a Data Breach | Report 2024* 2025.

1.2.2 Wirtschaftliche Schäden und Auswirkungen auf Unternehmen und Privatpersonen

Auch meldet IBM im Jahr 2024 ein ungefährer Schaden von 4.88 Millionen US-Dollar pro Vorfall.[5] Vor allem Unternehmen werden oft betroffen, da man dort oft klare Hierarchien hat und deswegen die Angreifer gezielter bestimmte Personen impersonifizieren können und somit die Mitarbeiter schneller dazu bringen können, sensible Daten preiszugeben oder Schadsoftware herunterzuladen. Außerdem kann, wenn ein Unternehmen stark betroffen ist, ein enormer Vertrauensverlust gegenüber der Öffentlichkeit entstehen, was sich negativ auf die Verkaufszahlen auswirken kann.

Ein sehr bekanntes Bespiel dafür ist der Target (US-amerikanische Einzelhändler) Hack von 2013, welcher (wenn auch nur indirekt) ungefähr 162 Millionen US-Dollar Schaden verursacht hat. Dadurch, dass Kreditkarteninformationen von Milionen Kunden gestohlen wurden, hat Target sowohl einen extremen Vertrauensverlust erlitten, als auch starke finanzielle Einbußen hinnehmen müssen.[6]

2 Definition von Social Engineering

2.1 Grundprinzipien und Psychologie des Social Engineerings

Die Ausnutzung von menschlichen Eigenschaften wie Vertrauen, Angst, Autorität, Hilfsbereitschaft und viele mehr stehen im Vordergrund beim **Social Engineering**. Durch gezielte Manipulation oder Erpressung werden unzählige Opfer (oftmals ohne ihr Wissen) dazu gebracht gewisse Geldsummen für vermeindliche Dienstleistungen zu überweisen, sensible Daten anzugeben oder gezielte Schutzmechanismen (z.B. 2-Faktor-Authentifizierung) zu umgehen.[7]
Hier geht es keineswegs um die Umgehung von technischen Schutzmaßnahmen, sondern um das gezielte Täschen vom Mensch als Schwachstelle. Durch bewährtes Probiere von bestimmten Angriffstechniken verfeinern Angreifer ihre Methoden immer weiter, dass Menschen schneller (und häufiger) beeinflusst werden können, um so auf Systeme zuzugreifen, oder an sensible Daten zu gelangen. Deswegen hilft auch nur eine Sache gegen diese Art von Angriffen: **Aufklärung**.

[5] *Was ist Phishing?* 2025.
[6] *The Target Breach: A Historic Cyberattack with Lasting Consequences* 2025.
[7] *Social Engineering – der Mensch als Schwachstelle* 2025.

2.2 Gängige Methoden

Neben den Subgenres von Phishing und Whaling ist **Baiting** sehr verbreitet. Hier geht es darum, dem Opfer falsche Versprechen zu geben. Sei es entweder ein Gewinnspiel, welches angeblich gewonnen wurde oder sogar in physischer Form, wie z.B. ein USB-Stick, der gezielt an einen gut ersichtlichen Ort gelegt wurde und mit Malware präpariert ist.[8]

Bei **Quid pro Quo** wird darauf geachtet, Opfern attraktive Dienstleistungen anzubieten, um im Gegenzug an sensible Daten (oder Geld) zu gelangen. Diese Strategie wurde im Netz vor allem durch den YouTuber *Jim Browning* bekannt. Durch seine Videos, in denen er sogenannte Call-Center aufdeckt und diese sukzessive inflitriert und am Ende an die lokalen Behörden übergibt, wird deutlich, wie einfach es ist, Menschen zu manipulieren.[9]

Honeytrapping ist eine gängige Methode um sich mit Menschen, die auf diversen Dating-Plattformen nach ihrer Traumfrau suchen, anzufreunden und dadurch einen finanziellen Vorteil zu erlangen. Vor allem der Aufschwung von Künstlicher Intelligenz und Date-Portalen hat es den Angreifern umso leicht gemacht gefälschte Profile zu erstellen und falsche Versprechen zu geben.[10]

3 Definition von Phishing

3.1 Definition und Abgrenzung als Teilbereich des Social Engineerings

- PLATZHALTER

3.2 Die Verschiedenen Arten von Phishing und ihre Ziele

- Spear Phishing, Whaling, Clone Phishing, Voice Phishing, Smishing, Vishing, Pharming, E-Mail Phishing, ..
- Ziele (Datenklau (Finanzen maybe, aber auch Anschrift), Identitätsdiebstahl, Malware-Verbreitung, ..)

[8] Villavicencio 2022.
[9] *Jim Browning - YouTube* 2025.
[10] Villavicencio 2022.

4 Bekannte Phishing-Skandale und ihre Folgen

4.1 Democratic National Committee (DNC)-Hack

Ein sehr bekanntes Beispiel für einen Phishing-Angriff ist der DNC-Hack von 2015 und 2016, bei dem die demokratische Partei der USA Opfer eines Spear-Phishing-Angriffs wurde. Dabei wurden E-Mails an 300 Angehörige der demokratischen Partei oder der Clinton-Kampagne verschickt, die von russischen Hackern stammten. Die zwei Gruppen, "Fancy Bearünd "Cozy Bear", haben insgesamt 70GB von den Servern der Clinton-Kampagne und 300GB von den DNC-Servern gestohlen. Diese Daten, zusammen mit 20.000 E-Mails wurden auf WikiLeaks veröffentlicht.[11]

Im Januar 2017 haben sowohl das FBI, als auch die CIA, NSA und mehrere andere US-Geheimdienste untersucht, ob die russische Regierung mit diesem Angriff die Präsidentschaftswahl 2016 beeinflussen im Wohle von Donald Trump beeinflussen wollte.[12]

Obwohl es also keine klaren Beweise gibt, kann man schon davon ausgehen, dass der Angriff eine große Rolle bei der Beeinflussung der Wahl gespielt hat. Man kann also sagen, dass dieser Angriff nicht nur ein Beispiel für Social Engineering und Phishing ist, sondern auch für die weitreichenden politischen und gesellschaftlichen Auswirkungen, die politisch motivierte Angriffe haben können.

4.2 Twitter Spear Phishing Attack (2020)

- PLATZHALTER

4.3 Weitere Skandale

- PLATZHALTER

5 Bezug zum Ethischen Hacking

5.1 Social Engineering und Phishing als Werkzeuge im Penetration Testing

- PLATZHALTER

[11] *How The DNC Hack Changed the 2016 Presidential Election Results* 2025.
[12] *Intercepted Russian Communications Part of Inquiry Into Trump Associates* 2025.

5.2 Aufklärung und Sensibilisierung durch simulierte Angriffe

- PLATZHALTER

5.3 Rechtliche und ethische Rahmenbedingungen

- PLATZHALTER

6 Fazit und Ausblick

6.1 Zusammenfassung

- PLATZHALTER

6.2 Bedeutung von Präventionsmaßnahmen und Sensibilisierung

- PLATZHALTER

6.3 Zukünftige Entwicklungen und Herausforderungen

- PLATZHALTER

Literaturverzeichnis

Cost of a Data Breach | Report 2024. URL: https://www.ibm.com/reports/data-breach (besucht am 23. 05. 2025).

How The DNC Hack Changed the 2016 Presidential Election Results. URL: https://www.idstrong.com/sentinel/the-dnc-hack (besucht am 25. 05. 2025).

Intercepted Russian Communications Part of Inquiry Into Trump Associates. URL: https://www.nytimes.com/2017/01/19/us/politics/trump-russia-associates-investigation.html (besucht am 25. 05. 2025).

Jim Browning - YouTube. URL: https://www.youtube.com/@JimBrowning (besucht am 21. 05. 2025).

Phishing Trends Report (Updated for 2025). URL: https://hoxhunt.com/guide/phishing-trends-report#part-i-phishing-trends-amp-statistics (besucht am 22. 05. 2025).

Social Engineering – der Mensch als Schwachstelle. URL: https://www.bsi.bund.de/dok/11287460 (besucht am 21. 05. 2025).

Spam, Phishing & Co. URL: https://www.bsi.bund.de/dok/507910 (besucht am 21. 05. 2025).

The Target Breach: A Historic Cyberattack with Lasting Consequences. URL: https://www.frameworksec.com/post/the-target-breach-a-historic-cyberattack-with-lasting-consequences (besucht am 23. 05. 2025).

Villavicencio, A. *10 Arten von Social-Engineering-Angriffen*. 2022. URL: https://www.crowdstrike.com/de-de/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/ (besucht am 21. 05. 2025).

Was ist Phishing? URL: https://www.ibm.com/de-de/think/topics/phishing (besucht am 23. 05. 2025).