

Fake-Bewertungen im Internet

Themenbereiche:	Security, Privacy
Studierende:	Luzi Kobald
Betreuungsperson:	Ursula Uttinger
Experte:	Jan Alsenz
Auftraggebende:	Hochschule Luzern – Informatik
Keywords:	Reviews, Security, Online-Shopping, Trust

1. Aufgabenstellung

Seit der Entstehung des Internets zeichnet sich der Online-Handel von Dienstleistungen und Waren durch ein stetes Wachstum aus. Dieses Wachstum wird durch die ebenfalls steigende alltägliche Internet-Nutzung vieler Menschen rund um die Welt beschleunigt. Im Rahmen dieses Wachstums finden allerdings auch gefälschte Bewertungen, sogenannte «Fake-Reviews», zu solchen Dienstleistungen und Produkten vermehrt ihren Platz auf den gängigen Webshops und Bewertungs-Plattformen wie Amazon, Google Reviews, Tripadvisor uvm. «Fake-Reviews» haben meist den Zweck Verkaufszahlen direkt oder indirekt durch gefälschte positive Bewertungen zu steigern, oder die Verkaufszahlen der Konkurrenz durch gefälschte negative Bewertungen zu vermindern. Dabei handelt es sich grundsätzlich um einen Vertrauensmissbrauch durch den Verfasser einer solchen Bewertung gegenüber dem Käufer bzw. Leser dieser Bewertung.

Im Rahmen dieser Arbeit galt es herauszufinden wie gefälschte Bewertungen entstehen, wie sie verbreitet werden und welche Auswirkungen sie haben. Zudem sollte herausgefunden werden welchen Online-Plattformen am ehesten vertraut werden kann, und welchen nicht. Als weiterführende Fragestellung sollte zudem die Frage beantwortet werden, welche Auswirkungen sogenannte «Fake-Reviews» auf die IT-Sicherheit und den Datenschutz haben. Schlussendlich stellte sich die Frage, ob es wirksame Gegenmassnahmen gibt, oder ob es überhaupt einer konkreten Lösung für das Problem der «Fake-Reviews» bedarf.

2. Lösungskonzept

In einer ersten Phase sollte eine Umfassende Literaturrecherche durchgeführt werden, um eine möglichst ganzheitliche Perspektive des Themas «Fake-Reviews» zu erlangen. Dies beinhaltete eine Übersicht über die wichtigsten Aspekte des Themas zu erlangen, mitunter Soziologische, Wirtschaftliche und Technische. Dabei wurde versucht quantifizierbare Daten zu finden, was jedoch nach einer ersten Recherche-Phase zugunsten qualitativer Studien aufgegeben wurde. Dies wurde entschieden, da die Vergleichbarkeit der vorhandenen Untersuchungen und deren technische Natur dies im Rahmen der Arbeit erschwert hätten.

Infolgedessen wurde der Entscheid gefasst eine qualitative Analyse der Verhältnisse auf den gängigen Online-Plattformen aus internationaler und nationaler Sicht durchzuführen- ein Vergleich der Plattformen Digitec (CH) und Amazon (D/A). Im Rahmen Dessen sollte der Aspekt des «Nutzer-Vertrauens» im Zentrum der Untersuchung stehen um aufzuzeigen wie sich die Plattformen unterscheiden. Auch wurde eruiert, welche Aspekte möglicherweise zu einer verminderten Anfälligkeit gegenüber gefälschten Bewertungen führen könnten und einer weiteren Untersuchung bedürfen.

Da die Auswirkungen von «Fake-Reviews» auf die IT-Security ebenfalls beleuchtet wurde, stellte sich heraus dass die Themen im Bereich «Nutzer-Vertrauen» grosse Gemeinsamkeiten aufweisen. Folglich wurde entschieden, aufzuzeigen inwiefern «Fake-Reviews» Bestandteil der IT-Security sein können, und welche Handlungsempfehlungen für Nutzer von Online-Verkaufsplattformen von gängigen IT-Security-Handlungsempfehlungen ableitbar wären.

3. Spezielle Herausforderungen

«Fake-Reviews» haben viele Facetten, mitunter Rechtliche, Technische, Wirtschaftliche und Soziologische. Dabei ist es wichtig, für eine gesamtheitliche Betrachtung sich nicht zu stark auf einen Aspekt des Themas zu fokussieren, zumal es gerade zum technischen Aspekt der Erkennung von «Fake-Reviews» eine Vielzahl von Arbeiten gibt. Die rechtliche und praktische Betrachtung des Phänomens wurde zudem in einer Vorarbeit zur Genüge beleuchtet.

Zusätzlich ist das Thema von Fälschungen im digitalen Raum allgemein im Begriff starken Wandels. Neuartige Neuronale Netze, umgangssprachlich als «AI/KI» (Artificial Intelligence / Künstliche Intelligenz) bezeichnet, wie z.B. ChatGPT (basierend auf «GPT-4») sind in der Lage überzeugende, weit verbreitbare gefälschte Text-Inhalte auf Anfrage zu generieren. Das rasante Wachstum der Qualität und Verbreitung dieses Phänomens hat kaum voraussagbare Auswirkungen auf das untersuchte Thema dieser Arbeit.

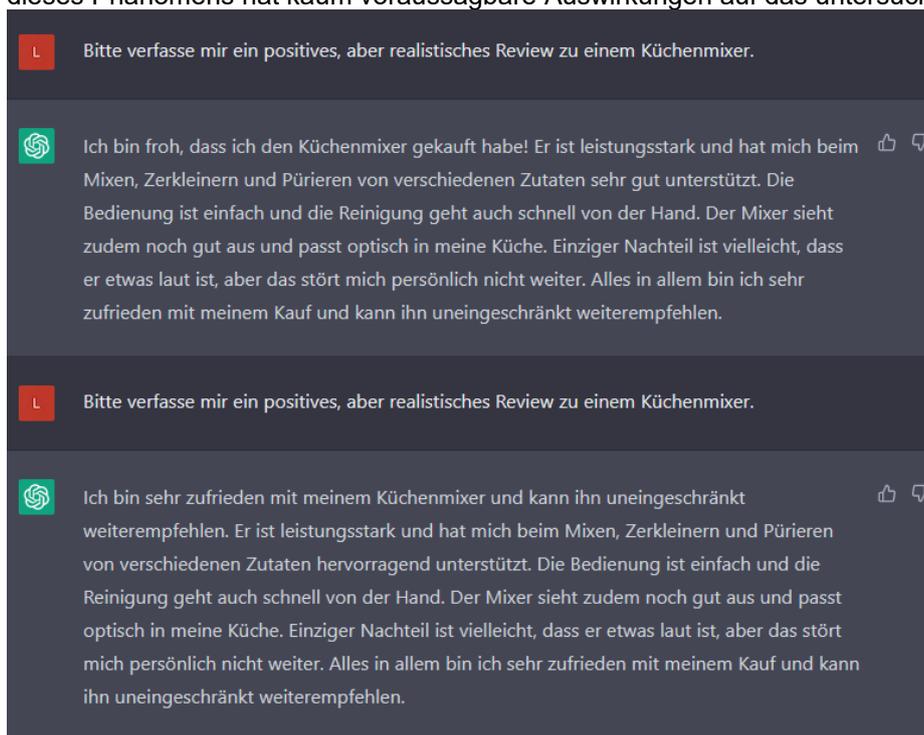


Abbildung 1: ChatGPT-Fake-Reviews

4. Ergebnisse

Ein direkter Vergleich zwischen Amazon und Digitec liess keine quantitative Vergleiche bezüglich «Fake-Reviews» zu, jedoch konnten definitive qualitative Unterschiede festgestellt werden, welche das Nutzer-Vertrauen beeinflussen können und dadurch die Anfälligkeit der Plattform selbst für «Fake-Reviews». Im Rahmen der Arbeit wurde festgestellt, dass sich die Plattformen stark in ihrem Fokus auf «Community»,

spricht auf die Pflege der Plattform als Nutzer-Gemeinschaft und positiven Nutzer-Interaktionen im Rahmen eines Online-Shops unterscheiden.

Generell befinden sich Anbieter von gefälschten Bewertungen in rechtlichen Graubereichen und sind technisch oftmals den automatischen Erkennungs-Mechanismen einen Schritt voraus, was eine Gemeinsamkeit mit der IT-Security aufzeigt.

Es wurde festgestellt, dass «Fake-Reviews» heutzutage einen wesentlichen Aspekt der IT-Security darstellen. Google-Such-Ergebnisse wie auch App-Store-Downloads sind anfällig für Fake-Reviews und Ranking-Missbrauch, was oftmals Malware-Infektionen zur Folge hat. Ausserdem wurde festgestellt, dass viele Herangehensweisen welche im Rahmen von Nutzer-Awareness-Kampagnen in der IT-Security erarbeitet worden sind für die Sensibilisierung von Nutzern für die Erkennung von «Fake-Reviews» von Nutzen sein könnten. Auch liessen sich diverse IT-Security-Angriffsarten auf das Thema der «Fake-Reviews» zurückführen. Es wurde eine grobe Liste an Verhaltensempfehlungen im Rahmen dieser Arbeit verfasst welche abgesehen von Empfehlungen für:

- Das Erwerben von Waren und Dienstleistungen auf Online-Plattformen
- Software-Käufen und -Downloads in mobilen App-Stores für Smartphones
- Software-Downloads über Suchmaschinen am Desktop-PC

5. Ausblick

Da viele Tangenten des Themas von «Fake-Reviews» zur IT-Security bestehen, ist es naheliegend Konsumentenschutz-Organisationen zu empfehlen Awareness-Programme zu erarbeiten welche Online-Käufer über mögliche Vertrauensmissbräuche informieren und orientieren. Insbesondere sollte dabei das Ausmass der nötigen zu vermittelnden Skepsis gegenüber Online-Reviews den gängigen technischen Fähigkeiten von Anbietern solcher Dienste entsprechen. Es lassen sich diesbezüglich insbesondere viele Parallelen zum Phänomen von «Phishing-Mails» ziehen. Die technischen Fähigkeiten für die automatisierte Erzeugung von «Fake Reviews» sind Stand Ende 2022 im Begriff ein Ausmass anzunehmen das bisher kaum denkbar gewesen wäre. Die zukünftigen Aussichten für die Vertrauensverhältnisse auf Online-Plattformen sind dadurch schwer vorhersagbar.

Generell lässt sich die Aussage treffen, dass die Grösse und Bekanntheit einer gegebenen Online-Plattform aktuell wesentlich zu deren Anfälligkeit für «Fake-Reviews» beiträgt. Zudem ist die Neuheit und somit Bekanntheit ein wesentlicher Faktor für die Wahrscheinlichkeit, dass ein Produkt oder eine Dienstleistung gefälschte Bewertungen erhält. Es wäre in zukünftigen Arbeiten möglich, einen national orientierten Markt mit einem grösseren, internationalen Markt quantitativ zu vergleichen, um herauszufinden ob sich ein geographisch granular orientierter Markt wie Digitec gegenüber Plattformen wie Amazon im Volumen der identifizierten «Fake Reviews» wesentlich unterscheidet.

Die technisch automatisierte Bekämpfung des Phänomens wird aufgrund der Ähnlichkeit zum Phänomen der «Phishing Mails» im Bereich der IT-Security als stets ungenügend beurteilt. Dies sollte anerkannt werden und als Anlass verstanden werden, Nutzer solcher Plattformen eine entsprechende Skepsis zu vermitteln, welche der jeweiligen Plattform angemessen ist. Dies könnte Inhalt einer zukünftigen Arbeit sein.