Machbarkeitsstudie eines Chatbots (LLM) zur Verbesserung der Informationssicherheit an der FAU: Lokale Modelle, Plattformvergleich und Integrationsmöglichkeiten

Master - Projekt - Exposé 6. Februar 2024

Autor: Fabian Berger, B. Sc.
Betreuer: Prof. Dr.-Ing. Michael Tielemann
Prüfer: Prof. Dr.-Ing. Michael Tielemann

1 Motivation

Die äußerst hohe Relevanz von Informationssicherheit erfordert innovative Ansätze, um den Wissensaustausch zu fördern. Die Motivation dieses Masterprojekts liegt in der Schaffung eines zugänglichen und anonymen Dialogs zwischen der FAU-Gemeinschaft und einem Chatbot. Dieser soll Informationen zur Informationssicherheit bereitstellen, ohne die Identität der Fragenden preiszugeben. Bei über 500 Lehrstühlen der FAU mit eigenen Arbeitsweisen und unterschiedlichen Kompetenzprofilen ist es von umso größerer Bedeutung, dass Interessierte einen einfachen Zugang zu Informationen erhalten. Dies kann dabei helfen, Interessierte zu motivieren, sich mit dem Thema Informationssicherheit auseinanderzusetzen und so die Sicherheit der FAU als Ganzes zu erhöhen.

2 Problemstellung

Aktuelle Informationsquellen zur Informationssicherheit an der FAU sind möglicherweise nicht ausreichend zugänglich. Vor Allem für Personen, die zwar interessiert, aber noch nicht mit dem Thema vertraut sind, kann es schwierig sein, die richtigen Informationen zu finden.

Dieses Problem soll durch die Bereitstellung eines Chatbots gelöst werden, der anonyme Anfragen beantwortet und so eine niedrigschwellige Informationsquelle darstellt.

3 Konkrete Ziele

Ein Chatbot wird konzipiert, um Fragen zur Informationssicherheit zu beantworten.

Beispielhaft soll dieser Chatbot Fragen zu den folgenden Themen beantworten können:

- Sicherheitsbewusstsein
- Passwortsicherheit
- Phishing
- Schutz vor Malware und Viren
- Identifizierung und Authentifizierung
- Datenschutz und -sicherheit
- Netzwerksicherheit
- Sicherheit bei Cloud-Services

Die Auswahl eines geeigneten und performanten Modells und einer Plattform, basierend auf einer umfassenden Evaluierung, steht im Fokus.

Genauigkeit der Antworten, Benutzerfreundlichkeit, Reaktionszeit, Anpassungsfähigkeit, Sicherheit des Chatbot-Systems selbst, Protokollierung und Skalierbarkeit sind dabei wichtige Kriterien, um die Plattformen zu bewerten.

Anonymität gewährleisten: Der Chatbot wird so gestaltet, dass er Anfragen anonym bearbeitet, um eine Hemmschwelle für die Nutzer zu minimieren.

4 Projektplan

Woche 1 – 2 Start (15.01.2024): Recherche: Evaluierung von Plattformen wie BotLibre[1], LibreChat[2], LlamaIndex[3], Untersuchung von Large Language Modellen sowie manuellen Ansätzen

Woche 3 – 4 Lokale vs. Cloud-Modelle: Detaillierte Analyse von Vor- und Nachteilen, Betrachtung von Sicherheitsaspekten und Datenschutz

Woche 5 Plattformauswahl: Entscheidung von einer oder mehrerer Testplattformen als vorläufige Plattform, Ausschluss von nicht geeigneten Plattformen.

Woche 6 – 8 Integration von Large Language Models: Umsetzung mehrerer LLM-Modelle mit Modifikationen für optimale Ergebnisse

Woche 9 – 10 (Praktikum: Astronomisches Praktikum, 13.03.2024-26.03.2024)

Woche 11 – 12 Testphase: Umfassende Tests zur Sicherstellung der Funktionalität und Leistung, Optimierung der Benutzerfreundlichkeit.

Woche 13 – 14 Testphase: Identifikation und Behebung von Problemen

Woche 15 – 17 Abschluss: Erstellung eines umfassenden Berichts, Dokumentation der Technologien und Modelle

Bei einer geplanten Bearbeitungszeit von 20 Stunden pro Woche ist eine Dauer von 15+2 Wochen geplant.

[1] https://www.botlibre.com/
[2] https://github.com/danny-avila/LibreChat
[3] https://www.llamaindex.ai/