Künstliche Intelligenz in der Cybersicherheit

„Unterstützung im Kampf gegen Hacker oder eine neue Bedrohung.”

Saskia Jürgens

Matrikelnr.: 6143565

Betreuer: Tim Laue & Dr. ...

Problem- und Zielstellung der Arbeit:

Die zentrale Fragestellung dieser Arbeit lautet:

„Wie hilfreich ist KI im Kampf gegen Hacker, und inwieweit stellt sie selbst die größte Herausforderung für die Cybersicherheit dar?“

Ziel der Arbeit ist es, die Ambivalenz der KI in der Cybersicherheit zu analysieren, indem sowohl ihre positiven als auch ihre negativen Auswirkungen untersucht werden. Es sollen praxisnahe Empfehlungen erarbeitet werden, wie die Vorteile von KI genutzt und ihre Gefahren minimiert werden können.

Dokumentation des derzeitigen Wissensstandes / Literaturrecherche

Einerseits wird KI als vielversprechendes Werkzeug zur Bedrohungserkennung und -abwehr betrachtet, wie etwa eine Daisy-KI zum Erkennen von Scam-Anrufen. Andererseits wird auf die Risiken hingewiesen, dass KI auch von Angreifern genutzt werden kann, um ausgeklügelte Angriffe zu starten, beispielsweise durch Deepfake-Technologien oder automatisierte Hackerangriffe. Zudem sind KI-Systeme selbst anfällig für Angriffe.

Erkenntnisdefizite

Ethische und rechtliche Rahmenbedingungen sind unzureichend definiert, insbesondere zur Regulierung des KI-Missbrauchs.
Begrenzte Studien zur Interaktion von KI-Angreifern und Verteidigern („KI gegen KI“).

Unterschiedliche Perspektiven

1. **Verteidigungsperspektive:** Fokus auf KI-gestützte Bedrohungserkennung und automatisierte Abwehr.
2. **Regulierungsperspektive:** Notwendigkeit schärferer internationaler Standards für den Einsatz von KI in der IT-Sicherheit.

Vorgehen und Aufbau der Arbeit in Form einer Arbeitsgliederung:

Die Arbeit ist rein theoretisch ausgerichtet und basiert auf einer umfassenden Analyse vorhandener Literatur und Fachartikel zum Thema „Künstliche Intelligenz (KI) und Cybersicherheit“. Die herangezogene Literatur bezieht sich dabei auf Fachliteratur,

Forschungsarbeiten aus dem Wissenschaftsindex Google-Scholar und praxisbezügliche Zeitungsartikel des online-journalistischen Feldes. Die Arbeit wird die wesentlichen Chancen und Herausforderungen durch KI in der Cybersicherheit aus verschiedenen Perspektiven beleuchten.

Arbeitsgliederung/ Inhaltverzeichnis

Einleitung

Hauptteil

- Grundlagen und Definitionen (Ki, Cybersicherheit, Hacking und Scam definieren)
- KI und ihre rasante Entwicklung
- Cybersicherheit im Kontext von KI
    - Warum ist Cybersicherheit für KI so wichtig?
    - Herausforderungen der Cybersicherheit im Zeitalter der KI
- KI als Schutz vor Cyberbedrohungen
- Die dunkle Seite der KI: KI als Angriffsvektor
    - KI als Mittel zum Hacken
    - Deepfake-Technologie und ihre Bedrohung für Cybersicherheit
    - ChatGPT und andere KI-Tools im Cyberbereich
- Zukünftige Herausforderungen und ethische Fragestellungen

Fazit