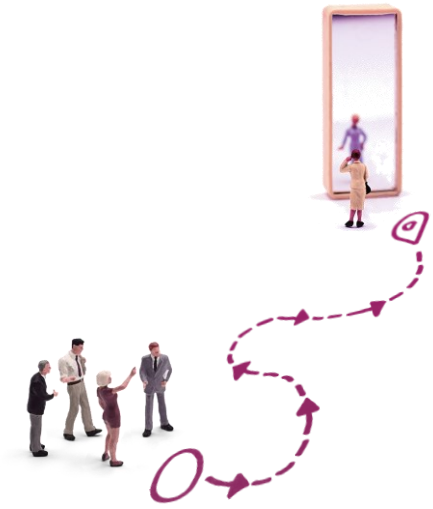


ALTHAMMER & KILL

Künstliche Intelligenz vom Hype zum Nutzen

Einsatzmöglichkeiten mit Datenschutz & IT-Sicherheit verantwortungsvoll gestalten

Thomas Althammer, 30.05.2024
Pflegetisch Landeshauptstadt Hannover

1

ALTHAMMER & KILL

Thomas Althammer

Wirtschaftsinformatiker (Int. MBI)

Externer Datenschutzbeauftragter und
Externer Informationssicherheitsbeauftragter u. a.
im Gesundheits- und Sozialwesen (DSGVO, DSG-EKD, KDG)

Lehrbeauftragter an der Hochschule Hannover
und der Kath. Universität Eichstätt-Ingolstadt

Co-Leiter FINSOZ Fachgruppe IT-Compliance

2

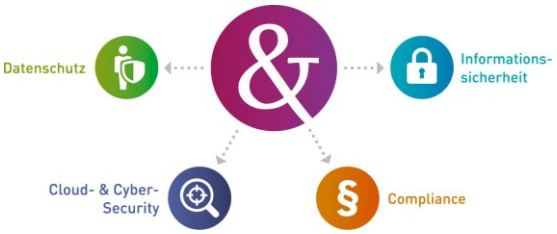
Kurz vorgestellt

ALTHAMMER & KILL

Althammer & Kill

Unternehmensberatung mit 45 Mitarbeitenden
(Datenschutzbeauftragte, Juristen, Security-Spezialisten)

gegründet 2014, bundesweit im Einsatz mit
Büros in Hannover, Düsseldorf, Mannheim



3

3

Kurz vorgestellt

ALTHAMMER & KILL

Aktuelle Projekte im Umfeld KI

- KI-Einsatz in Projekten datenschutzkonform & IT-sicher gestalten
- Beratung zu Produktentwicklung mit KI-Funktionen, z. B. Apps & Robotik
- Risikobewertung und Datenschutz-Folgenabschätzungen für KI-Lösungen

4

4

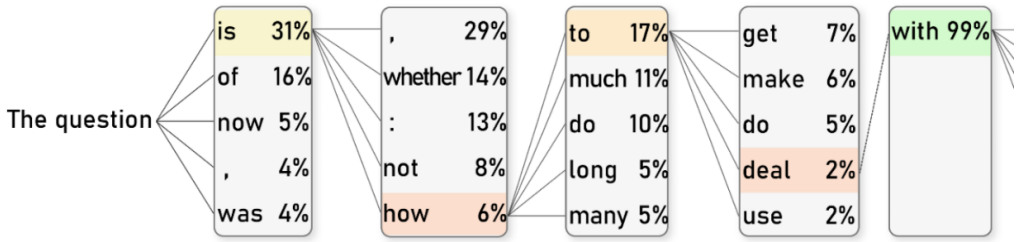
„Künstliche Intelligenz“ zwischen Hype und Realität

5

Wie funktioniert
Machine Learning/KI?

ALTHAMMER & KILL

The question is how to deal with the issue



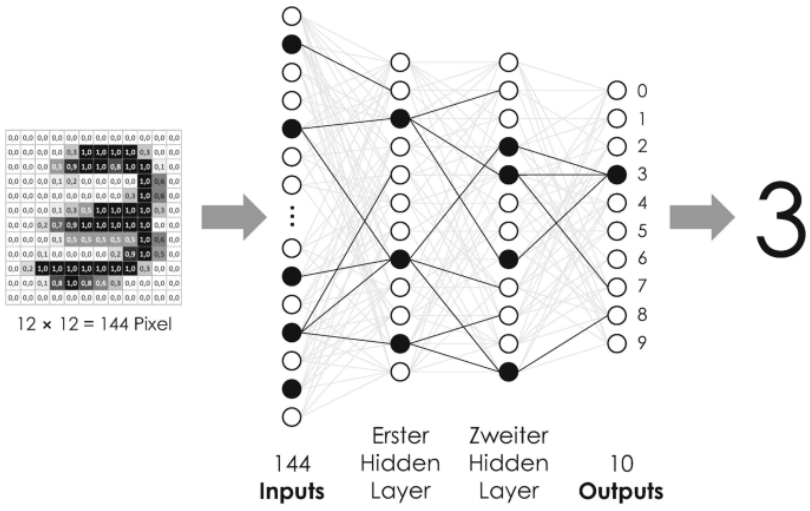
6

(Sobieszek/Price 2022)

6

Wie funktioniert
Machine Learning/KI?

ALTHAMMER & KILL



7

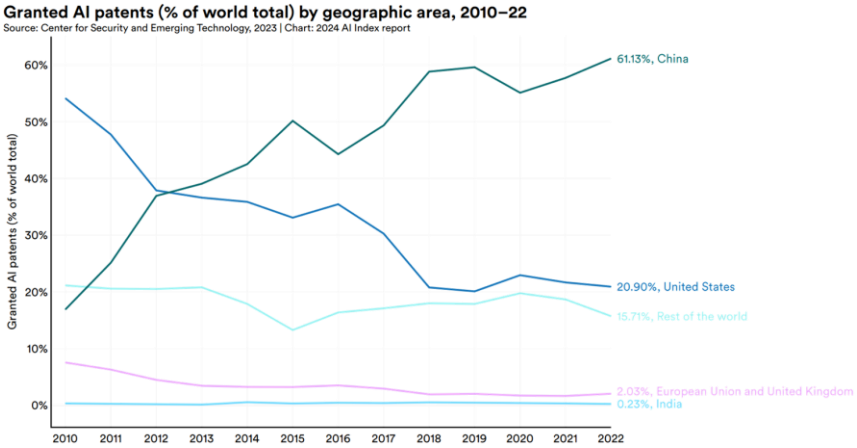
(Lang 2023)

7

Wie funktioniert
Machine Learning/KI?

ALTHAMMER & KILL

Wo findet KI-Entwicklung statt?



8

Quelle: Artificial Intelligence Index Report 2024 (Stanford)

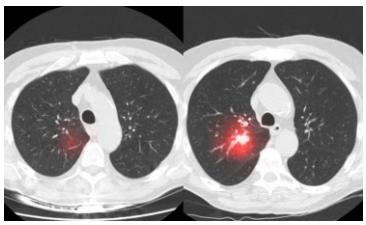
8

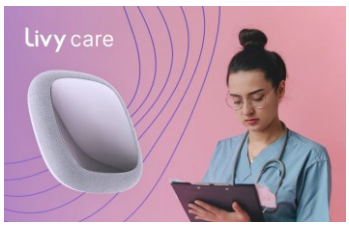
KI im Kontext
Datenschutz & IT-Sicherheit

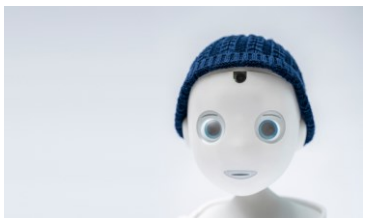
9

ALTHAMMER & KILL

Anwendungsfälle in der Pflege







10

ALTHAMMER & KILL

VASA-1: Lifelike Audio-Driven Talking Faces

Quelle: https://www.microsoft.com/en-us/research/project/vasa-1/

ALTHAMMER & KILL

Anforderungen Datenschutz

- Rechtsgrundlagen
- Verantwortung
- Vertrag mit KI-Anbieter
- Privacy by Design
- **Datenschutz-/Risiko-Folgenabschätzung**
- Datenminimierung
- Transparenz
- Drittstaaten/TIA
- Betroffenenrechte

Ziel:
Rechtskonformer und sicherer Einsatz von KI-Systemen

Herausforderungen IT-Sicherheit

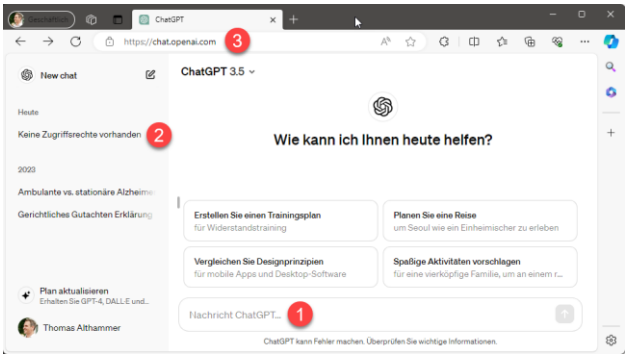
Poisening -
Trojan Horse -
Prompt Injection -
Sponge Attack -
Model/Data Theft -
Deception –
AI-based Attacks –

ALTHAMMER & KILL

ChatBots & Datenschutz

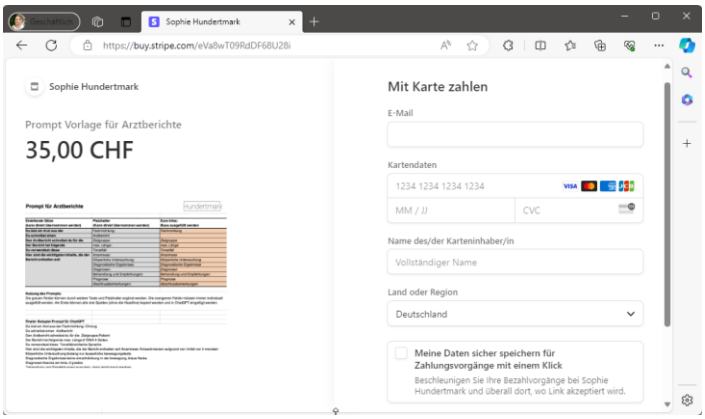
Abgesehen von den „ Datenschutz-Basics“:

1. Vertrauliches oder personenbezogene Daten im Prompt?
2. Nutzung des Outputs? Lernendes Sprachmodell?
3. Wie sind die Datenströme?



ALTHAMMER & KILL

Prompt-Vorlage: Arztbrief mit ChatGPT



Quelle: https://www.sophiehundertmark.com/chatgpt-und-generative-ai-fuer-arztberichte/

ALTHAMMER & KILL

Herausforderung Zugriffsrechte

Unternehmensinterne ChatBots:

- Qualität der Trainingsdaten (Bias, Diskriminierung, Datenschutz, Schutzrechte Dritter)
- Überprüfung von Prompts – wie Zugriffsrechte handhaben?
- Bewertung und Überprüfung der Ausgabe in Hinblick auf Berechtigung, Korrektheit, etc.

ALTHAMMER & KILL

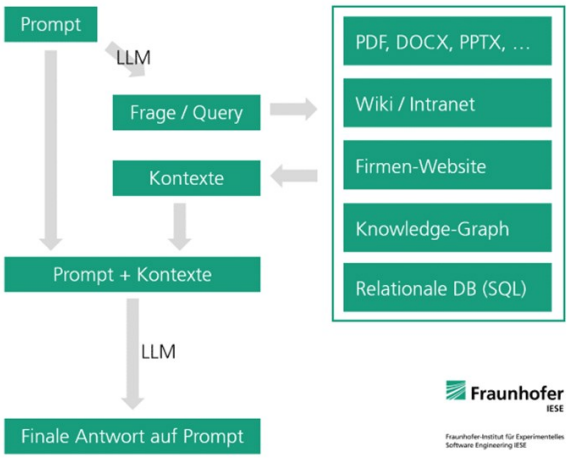
Lücken füllen

Grounding

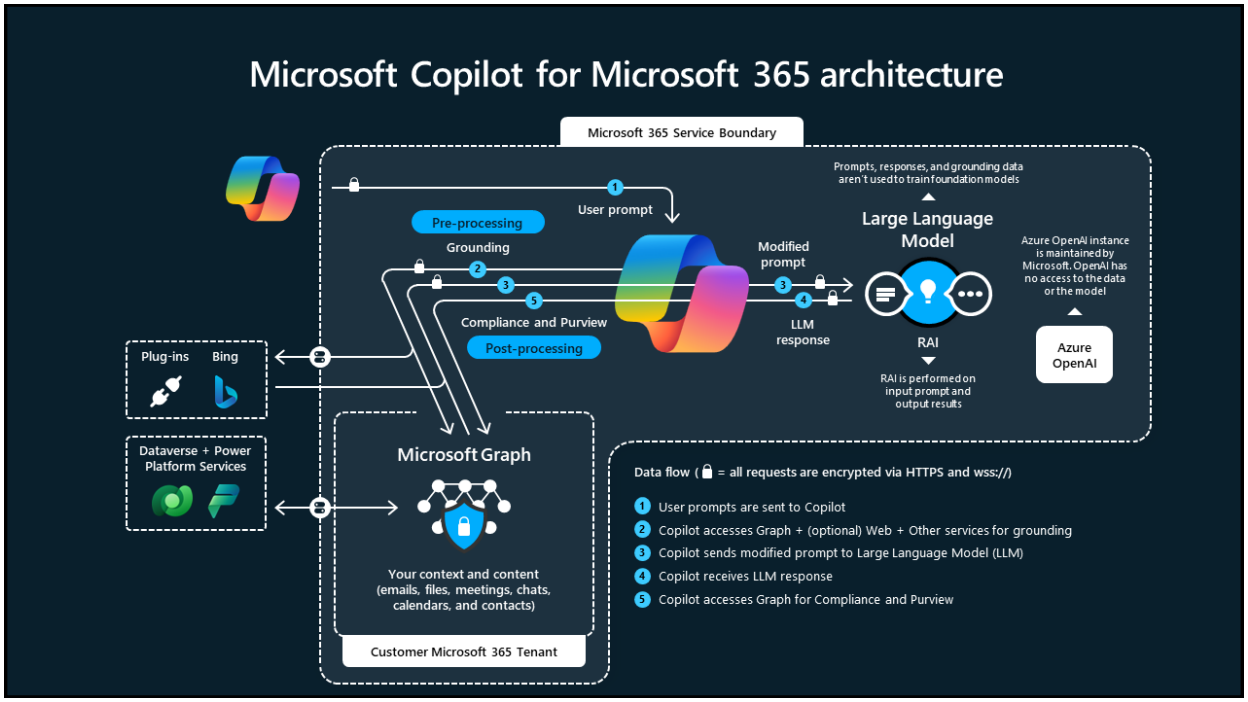
Prompt wird Kontext gegeben, Zugriff auf Daten und Quellen, Callbacks für Rückfragen

Retrieval-Augmented Generation

Einfügen relevanter Fakten aus externen Datenquellen/Dokumenten



Quelle: https://www.iese.fraunhofer.de/blog/retrieval-augmented-generation-rag



17

Hürde Datenschutz?
KI im Einsatz

18

ALTHAMMER & KILL

Datenschutz bei Copilot und Azure

	ChatGPT Free/Plus EU-TermsOfUse	ChatGPT Team/ Enterprise/API Business-Terms	Copilot Copilot Pro TermsOfUse	Copilot für Microsoft 365 MS-DPA
Auftragsverarbeitung (Abschluss DPA möglich?)	⛔ nicht verfügbar	✅ DPA vorhanden	⛔ nicht verfügbar	✅ vorhanden
Nutzung mit personenbezogenen Daten	⛔ nein	✅ möglich	⛔ nein	✅ möglich
Nutzung mit vertraulichen Daten	⛔ nein	⚠ teilweise	⛔ nein	✅ über Vereinbarung
Ausschluss Eigeninteressen Anbieter (Training, Optimierung)	⚠ nein/teilweise	✅	⛔ nein/unklar	✅
Einsatz im Gesundheitswesen	⛔ **nicht empfohlen**	✅ **möglich**	⛔ **nicht empfohlen**	✅ **möglich**

Stand 04/2024; Quellen u. a. VISCHER, Hunger/Rosenthal

ALTHAMMER & KILL

Aufgaben Datenschutz bei Einsatz von KI

Voraussetzungen

- Zweck?
- Nutzung Lokal, Hosting, Cloud
- Rechtsgrundlage
- Richtlinien
- Sensibilisierung und Schulung

Anbieter & Lösung

- Eignung
- Sitz/Rechtsrahmen, Datenströme
- Nutzungsbedingungen
- Auftragsverarbeitung bzw. Joint Controllership
- Erlaubter Nutzungsumfang (privat/beruflich/vertraulich)
- Qualität des KI-Modells (Herkunft der Trainingsdaten)
- Eigene Zwecke des Anbieters (Training, Verbesserung?)

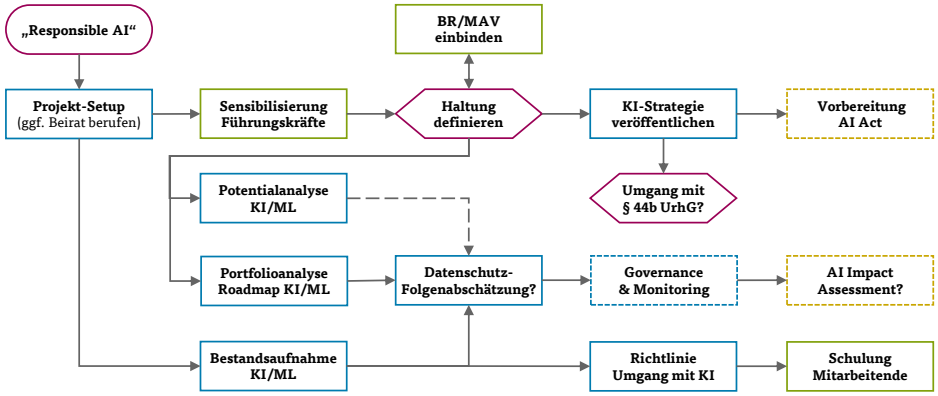
Betrieb & Einsatz

- Dokumentation (Verarbeitung und KI-Verfahren)
- Betroffenenrechte (z. B. Auskunft, Widerspruch)
- Datenschutz-Folgenabschätzung
- Risiko-Bewertung AI-Act
- Prozesse, Umgang mit Vorfällen
- Richtigkeit Output

Hürde Datenschutz?
KI-Einsatz gestalten

ALTHAMMER & KILL

Projektskizze KI in der Pflege



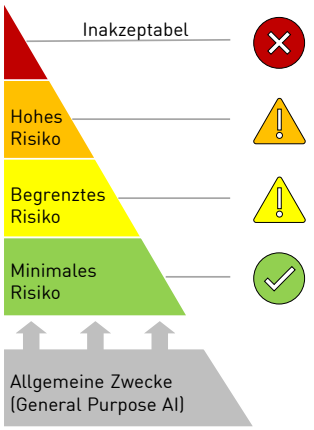
21

21

Ausblick

ALTHAMMER & KILL

Risikostufen AI Act



Einsatz von KI verboten
Beeinflussung, Ausnutzung von Schwäche oder Schutzbedürftigkeit, verschiedene Formen von Überwachung

Erlaubt unter Vorgaben
in den Bereichen kritische Infrastruktur, Bildung, Strafverfolgung, Medizinprodukte, etc. mit Konformitätsnachweisen

Erlaubt mit Transparenzpflichten
wie klassische Chatbots oder Technologien, die für die Erstellung von Deepfakes geeignet sind; generell KI am Arbeitsplatz

Grundsätzlich erlaubt – nicht weiter reguliert
wie Spamfilter, Empfehlungsmarketing, etc. müssen nur allgemein übliche Auflagen (z. B. die DSGVO) erfüllen

Beurteilung anhand von Leistung und Reichweite
als Level 1 mit Transparenzpflichten für GPAI-Systeme oder Level 2 mit zusätzlichen Pflichten ab 10^25 FLOP

23

Stand Gesetzgebungsverfahren 04/2024

23

Ausblick

ALTHAMMER & KILL

Studie KI in der Sozialwirtschaft

24

24

25

ALTHAMMER & KILL

Vielen Dank!

Bleiben Sie mit uns in Verbindung...

Thomas Althammer

+49 511 330603-10
ta@althammer-kill.de

26

Bildnachweis und Disclaimer

ALTHAMMER & KILL

Hinweis und Nutzungsrechte

Diese Präsentation wurde nach bestem Wissen anhand des zum Zeitpunkt der Erstellung geltenden Rechtsstandes erstellt. Es wird kein Anspruch auf Vollständigkeit und Richtigkeit erhoben. Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers. Weitergabe oder Veröffentlichung sind nur mit ausdrücklicher vorheriger Zustimmung von Althammer & Kill erlaubt.

Wir verwenden Bilder und Grafiken von:
www.miniansichten.de, www.pixabay.de und www.unsplash.com

27

27