

29. InfoTechDay

19.11.2024

HERZLICH WILLKOMMEN!



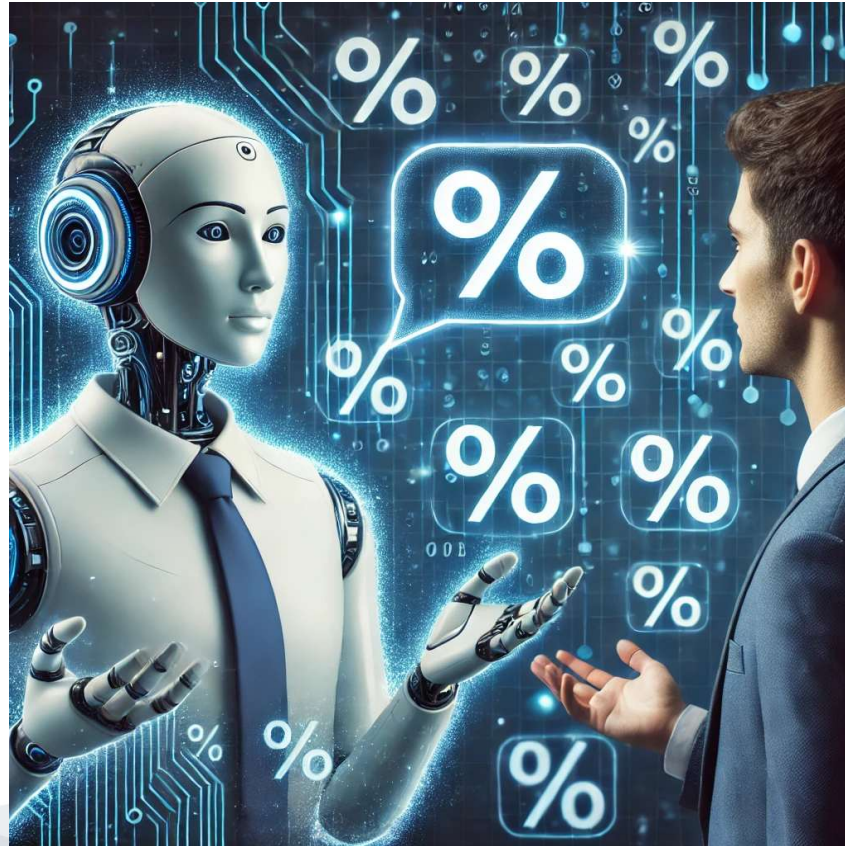
AI und Security

Patrick Wahlmüller (Microsoft MVP)



Motivation

INFOTECH
[IT & Communication]



Ihr Systemhaus.



Agenda

- Einleitung
- Bedrohungen
- Fazit



Künstliche Intelligenz

INFOTECH
[IT & Communication]



Ihr Systemhaus.



Aktuelle Bedrohungen

- Angriffe durch KI-gestützte Tools
- Manipulation und Desinformation
- Sicherheitslücken in KI Systemen
- Adaptive und schwer erkennbare Malware
- Analyse und Auswertung von gestohlenen Daten
- Social Engineering

Angriffe durch KI gestützte Tools

- Automatisierte Phishing Angriffe
- Generative KI für Schadcode-Erstellung



Manipulation und Desinformation

- Deepfake-Technologien
- Manipulation von sozialen Medien



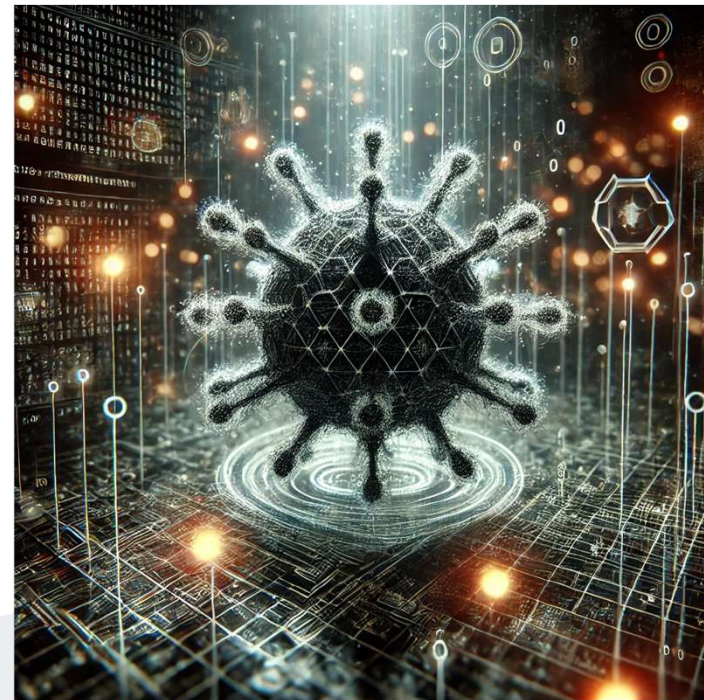
Sicherheitslücken in KI-Systemen

- Angriffe auf KI-Systeme
- Datenexposition durch LLMs
- Eingabe von sensiblen Daten in Chatbots



Adaptive und schwer erkennbare Maleware

- KI-gestützte Maleware
- Echtzeit-Überwachung und Hacking



Analyse und Auswertung gestohlener Daten

- KI-gestützte Datenanalyse



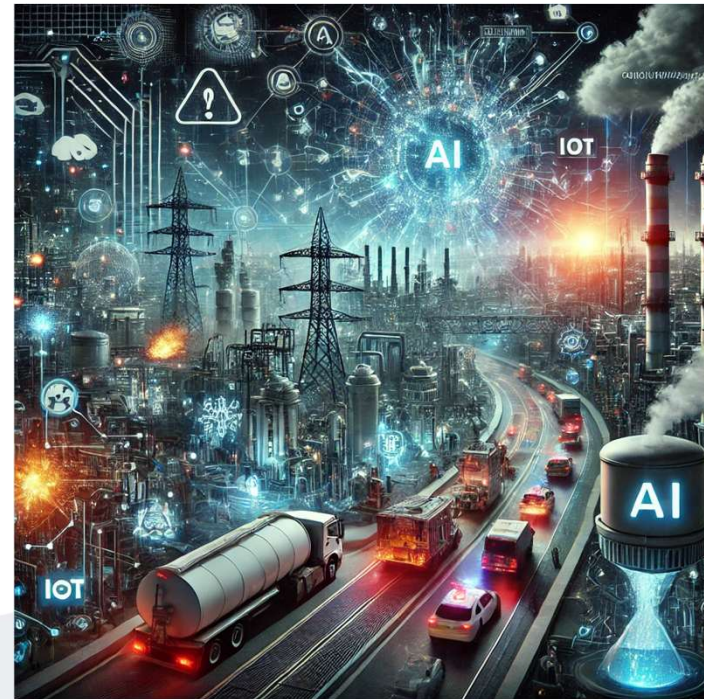
Social Engineering

- Psychologische Manipulation



Automatisierte Durchführung von Angriffen auf kritische Infrastruktur

- Energieversorgung
- Wasserversorgung
- Verkehrssteuersysteme
- Industrie- und Fertigungsanlagen
- IoT-Geräte



Fazit

- Vielzahl von Bedrohungen
- KI für red & blue

DANKE!



INFOTECH

[IT & Communication]

Ihr Systemhaus.

