

CYBER-BOOTCAMP AM 16. OKTOBER | 10:30 BIS 11:15 UHR

Wenn KI zur Waffe wird: Deepfakes, CEO-Fraud & KI- gestützte Angriffe



MICHAEL GÄFGEN

Senior Consultant,
HiSolutions

Agenda

1. Einstieg: Zahlen, Daten, Fakten

2. Wofür und wie nutzen Angreifer KI?

3. Maßnahmen

4. Fazit



1.1 KI ist längst relevant

1 von 4 Breaches in IT-Systeme durch KI ermöglicht worden

6.000.000 \$ durchschnittlicher Schaden bei KI-Breach



"This growing imbalance—where attacks can be launched for thousands while breaches cost millions—is fundamentally changing the economics of cyber risk."

IBM

1.2 „Gut angekommen“ – auch in Deutschland laut BSI

Jedes 6. Unternehmen mit KI angegriffen

KI nachzuweisen, fällt enorm schwer – 6% bestätigt

KI –Sicherheitsstudie des BSI

Nur jedes 10. Unternehmen ist vorbereitet!



2.2 Fallbeispiel Spearfishing - Arup

Konferenz mit Finanzabteilung

Deepfake-Videos überzeugen Mitarbeiter



Überweisung von 25.000.000\$ an die Täter

2.3 Sind Angriffe durch KI besser und rentabler?

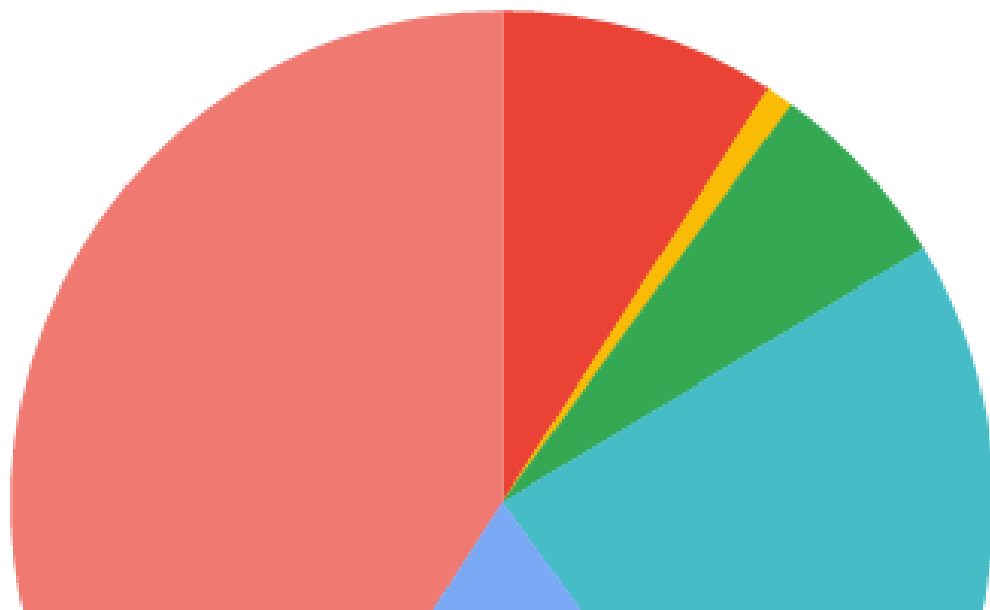


	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on Objectives
Phishing	High	Medium	Low	Low	High	Medium	Medium
Malware	Low	Low	Low	Medium	High	Low	Medium
Denial-of-Service (DoS)	High	Low	Low	Low	Low	Low	Medium
Man-in-the-Middle (MitM)	Low	Low	Low	Low	Low	Low	Medium
SQL Injection	Low	Low	Low	High	Low	Low	Medium
Zero-Day Attack	Low	Low	Low	Low	Medium	Low	Medium

Simulation durch Google Deepmind

Reconnaissance

- Gather Victim Identity Information
- Social Media Harvesting
- Search Open Technical Databases
- Gather Victim Organization Information
- Search Open Websites/Domains
- Phishing for Information



Fallbeispiel in Cloudumgebung, rasante Verbreitung durch automatische „Analyse“

Für Betroffene ist Reaktionszeit damit geringer

2.4 BSI-Bericht: Generative KI-Modelle

Nutzungen durch Angreifer dargestellt

Kostenlos verfügbar

Generative KI-Modelle

Chancen und Risiken für Industrie und Behörden



2.4.1 Täuschung & Fälschung

Erstellung gefälschter Inhalte

Glaubwürdiges Phishing

Identitätsdiebstahl

2.4 .2 Wissen, Daten & Schadcode

„Alltagshilfe“ bei der Erklärung von Schwachstellen

Automatisierte Ausführung

Platzierung durch LLMs

Derzeit noch keine Erstellung von Malware durch KI allein





2.4.3 Poisoning Attacks

Auch KI-Modelle selbst können „Ziel“ sein

„Vergiften“ der Datengrundlage

Gefälschte Inhalte, Manipulation von Trainingsdaten

2.4.4 Privacy Attacks

„Nachvollziehen“ von KI-erstellten Daten

Diebstahl von Vektordaten

Modelldiebstahl / Erstellung eines Modell-Klons



3. Maßnahmen - Gibt es denn etwas neues?

„Basics“ der IT-Sicherheit sind wichtiger denn je!

Dazu vermehrt Due-Dilligence-Maßnahmen gegen Social Engineering

Zu KI: Monitoring der Nutzung, sperren auffälliger Nutzer

Die relevantesten Angriffsarten sind bereits bekannt!

BSI, Microsoft, Obliegenheiten – An vielen Orten gibt es Hinweise!

4. Fazit - Wie steht es nun um das Thema?

Laut einigen Experten steigt Quantität wahrscheinlich nicht

Jedoch kommen durch die Nutzung von KI neue Risiken hinzu

Zudem vor allem Open-Source Software, Cloud Identity und OT verstärkt betroffen

Unternehmen unter 1000 Beschäftigte jedoch besonders betroffen

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com

Quellen:

- [KI-Sicherheitsstudie 2026](#) BSI
- [Generative KI-Modelle](#) BSI
- [2503.11917](#) Google-Deepmind
- [Arup revealed as victim of \\$25 million deepfake scam involving Hong Kong employee | CNN Business](#)
- [IBM Study: One in Four Malicious Breaches are AI-Enabled, Costing Companies \\$6 Million on Average](#)