

Prompt Hacking: Anstiften, Verführen, Manipulieren

Wenn Sprachmodelle mehr preisgeben, als sie sollen

Prompt Hacking: Anstiften, Verführen, Manipulieren – Wenn Sprachmodelle mehr preisgeben, als sie sollten

In unserem Alltag nutzen wir immer häufiger Sprachmodelle – sei es in Chat-Funktionen beim Support oder in automatischen Anrufsystemen (ACD). Diese Modelle sollen einen bestimmten Zweck erfüllen und greifen dabei auch auf zum Teil sensible Daten zurück, zum Beispiel auf Verläufe, Verhalten, Prozesse und persönliche Daten.

Die Nutzung von Prompt Hacking (sog. Prompt Injection) stellt eine zunehmende Herausforderung im Umgang mit diesen modernen Sprachmodellen (LLMs) dar. Durch gezielte Manipulationen in Text- oder Spracheingaben können Angreifer das Verhalten oder die Antworten des Modells gezielt oder unbewusst beeinflussen.

Diese und weitere Angriffsmöglichkeiten sowie das Potenzial von Prompt Injection stellen wir im Vortrag detailliert dar.

Was Sie im Webinar erwartet:

- **Arten von Prompt Injection (Direct/Indirect)**
- **Prompt-Injection-Techniken wie Cross-modal Attacks, Jailbreak Prompts, Role Play, Code-Switching, moralisches Framing, Obfuscation**
- **Auswirkungen von Prompt Injection (Umgehung von Sicherheitspolicies, Preisgabe sensibler Daten etc.)**

Wann:

Montag, 11. Mai 2026
13:30 bis 14:30 Uhr

Wo:

Onlinewebinar

Die Veranstaltung ist kostenfrei.

13:30 Uhr **Begrüßung**

13:35 Uhr **Prompt Hacking: Anstiften, Verführen, Manipulieren – Wenn Sprachmodelle mehr preisgeben, als sie sollten**

Marco Di Filippo
Ethical Hacker, Cyber Security Evangelist,
Senior Cyber Security Engineer,
Gründer, Autor

ab 14:20 Uhr **Fragen; Networking**

Veranstalter:

IHK für Oberfranken Bayreuth
Bahnhofstraße 25
95444 Bayreuth

Ansprechpartner:

Ralph Buus
☎ 0921 886-470
@ buus@bayreuth.ihk.de

In Zusammenarbeit mit:



whitelishackers
[cyber attack investigation and research]



Anmeldung online unter
ihkofr.de/promthacking1105

Bitte melden Sie sich bis spätestens **Freitag, 8. Mai 2026** verbindlich an.

Dieses Webinar findet statt im Rahmen der BIHK-Webinarreihe zur IT-Sicherheit.

Im Rahmen des bayerischen Pakts für berufliche Weiterbildung 4.0 bieten die bayerischen IHKs gemeinsam mit dem Staatsministerium für Digitales und weiteren Partnern Webinar-Reihen wie diese hier als "Digitalimpulse" für Unternehmen an.