

## **HXZ.ONE #1 IT-Sicherheitskonferenz beleuchtet die Bedrohung durch Angriffe auf KI-Systeme**

Themen: Ethical Hacking, AI Security, Compliance, Biohacking, LLM-Hacking, WiFi-Hacking, zukünftige Angriffsvektoren und vieles mehr.

**URSTEIN, 11. März 2025** – Die **HXZ.ONE #1 IT-Security Konferenz**, die am **18. März 2025** in Urstein bei Salzburg stattfindet, widmet sich in diesem Jahr unter anderem einem besonders brisanten Thema: **Angriffe auf Large Language Models (LLMs)**. Diese Modelle, die in der modernen KI-Forschung und -Anwendung eine zentrale Rolle spielen, sind zunehmend Ziel von Cyber-Angriffen.

Die Konferenz bietet eine Plattform für Experten und Interessierte, um sich über die neuesten Entwicklungen und Bedrohungen im Bereich der IT-Sicherheit auszutauschen. Durch spannende Vorträge wird das Thema aus verschiedenen Perspektiven beleuchtet und **praxisnahe Lösungsansätze** werden vorgestellt.

In seinem hochspannenden Vortrag „**Hacking Your Enterprise Copilot: A Direct Guide to Indirect Prompt Injections**“ zeigt der renommierte Sicherheitsexperte **Tamir Ishay Sharbat**, wie vertrauenswürdige AI-Assistenten in bösartige Insider verwandelt werden können. Die Teilnehmer erfahren Schritt für Schritt, wie Angreifer **Indirect-Prompt-Injection-Angriffe (IPIs)** entwickeln, um KI-basierte Assistenzsysteme zu hacken, die in immer mehr Unternehmen zum Einsatz kommen. Der Vortrag behandelt den gesamten Prozess zur Schaffung zuverlässiger und robuster IPIs. Dabei wird anhand von **Microsoft Copilot Enterprise** demonstriert, wie die neuesten Angriffstechniken entwickelt und implementiert werden können.

Im Kurzvortrag „**LLMs im Fadenkreuz**“ von **Maximilian Pelka** werden die **Sicherheitsrisiken von Large Language Models (LLMs)** wie **ChatGPT** und **GPT-4** beim Einsatz in produktiven Umgebungen untersucht. Maximilian beleuchtet reale **Angriffsvektoren** und **Schwachstellen**, die bereits in der Praxis ausgenutzt wurden. Themen wie **direkte Prompt-Injection**, **unsichere API-Implementierungen**, **indirekte Manipulationen** und **Schwächen in der Ausgabe-Verarbeitung** werden detailliert behandelt. Der Vortrag wird durch aktuelle Forschung und praktische Demos ergänzt, die auf den Prinzipien des **Web Vulnerability Scannings** basieren.

Zusätzlich zu diesen Vorträgen gibt es bei dieser Veranstaltung viele weitere Vorträge zu **Biohacking**, **Compliance**, **Best-Practice-Tipps** und **Ethical Hacking**. Außerdem bietet sich die Gelegenheit, sich bei Snacks und Getränken mit Salzburgs IT-Security-Community zu vernetzen.

Die **HXZ.ONE #1** findet am **18. März 2025** von **18:30 bis 22:30 Uhr** im **Wissenspark Urstein auf der Freitreppe des Techno-Z CoWorking-Bereiches** als Abendveranstaltung statt. Die Teilnehmerzahl ist auf **100 Personen** begrenzt. Um die Schwelle zur Teilnahme an einem so hochkarätigen Event zu senken und mehr Leute mit diesem wichtigen Thema zu erreichen, beträgt der Preis für ein reguläres Ticket nur **19,99€**.

Die Veranstaltung wird von den **Silber-Sponsoren COPA-DATA, conova communications GmbH, Fachhochschule Salzburg (Department Information Technologies & Digitalisation) und Vivid Planet Software GmbH** unterstützt. Zu den Bronze-Sponsoren zählen die **flocke GmbH und mondess GmbH (IT-Architects & Consultancy)**.

**Die nicht gewinnorientierte IT-Security-Konferenz HXZ.ONE** wird von **IT-Wachdienst.com** bzw. der **toothR new media GmbH** mit Unterstützung der **Agentur AndersHier**, des **Beratungsunternehmens Pulse Revenue** und **bitdynamo** veranstaltet.

Weitere Informationen zur Veranstaltung finden Interessenten unter **<https://hxz.one>**.

**Ansprechpartner:**

DI(FH) Martin Herfurt  
Berater für IT-Sicherheit

IT-Wachdienst.com / toothR new media GmbH  
Urstein Süd 15  
5412 Puch bei Salzburg

eMail: [martin.herfurt@it-wachdienst.com](mailto:martin.herfurt@it-wachdienst.com)  
Threema: <https://threema.id/KMUM3KZH>  
Website: <https://www.it-wachdienst.com>