Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Forschungsorientierte Lehre:
Einsatz von Web-APIs zur Serviceintegration

Risikoorientierter Impuls zum Vortrag „Möglichkeiten des Model Context Protocols als „USB-C“ für KI-Lösungen (prototypische Tests)“
(Kernvortrag: *Hannes Dyballa und Peter Schwips*)

im Rahmen der ceCMG Tagung Mai 2026 | Frankfurt am Main

Prof. Dr.-Ing. habil. Andreas Schmietendorf

HWR Berlin/FB2 sowie Otto-von-Guericke Universität Magdeburg/FIN

Forschungsorientierte Lehre

Allgemeines Verständnis:

- Methodischer Umgang mit einem infinite wachsenden Informationspool
- Verändertes Lehrverständnis in den höheren Fachsemestern (Dozent – Coach)
- Studierende als innovative Ressource
- KI fordert andere Prüfungsformen

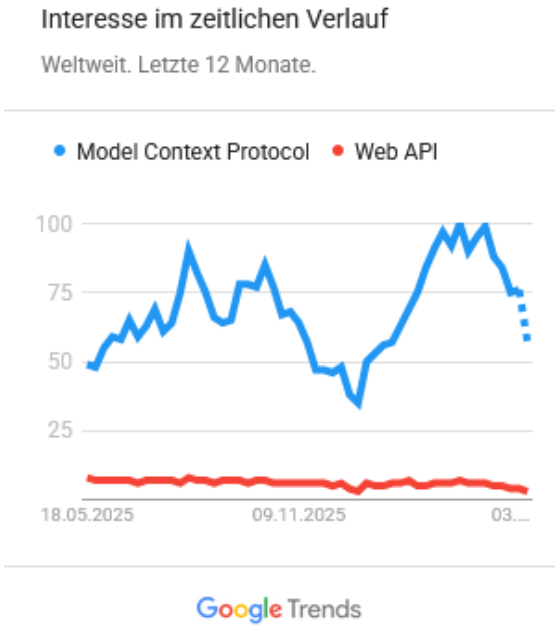
Spezieller Fokus im Themendiskurs:

- Moderne webbasierte Integrationsarchitekturen
- Integration als Schlüssel zur Digitalisierung
- KI im System- und Software-Engineering
- Analytisch- und experimentelle Lehrausrichtung

Abbildung wurde generiert mit Hilfe von Microsoft Copilot – genutzter Promt: forschungsorientierter Lehransatz an Hochschulen

MCP - Model Context Protocol

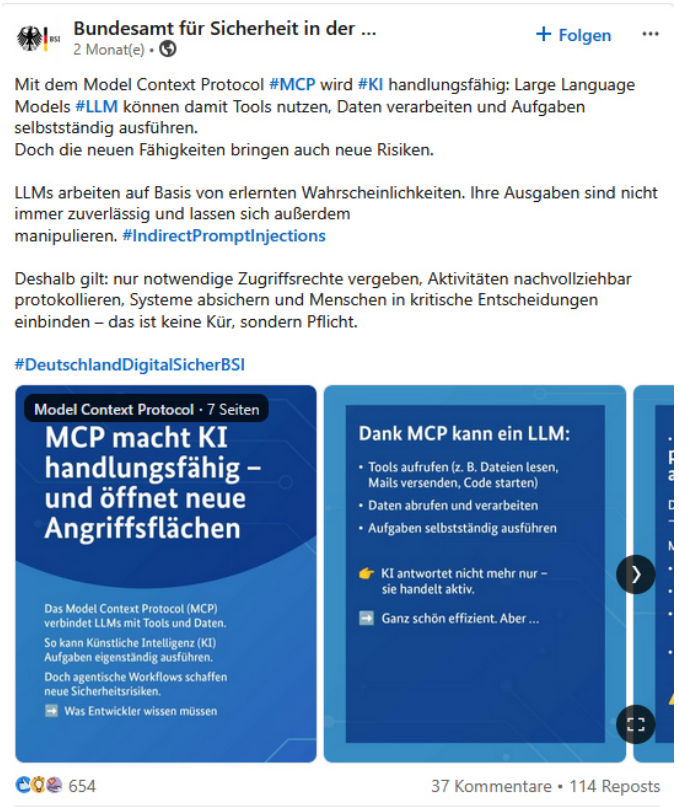
- Large Language Models (LLMs)
  - Vortrainierte KI-Modelle
  - Problem der KI-Halluzination
  - Kein Bezug zu aktuellen Daten
- Retrieval-Augmented Generation (RAG)
  - Reduktion inkonsistenter Ergebnisse
  - Ext. aktuelle Daten im Promt Engineering
  - API Funktionsaufruf durch LLM
- Model Context Protocol (MCP)
  - Natürlichsprachliche Systeminterkation
  - Fokus: Schnittstelle LLM und ext. Tools, Daten, …
  - offener Standard von *Anthropic* – KI-Agenten …



Quelle: Google Trends, Abruf 18. Mai 2026, https://trends.google.de/trends/explore?cat=5&q=%2Fg%2F11x5hnm0vb,%2Fm%2F07sb4tb&hl=de

Bedrohungspotential MCP

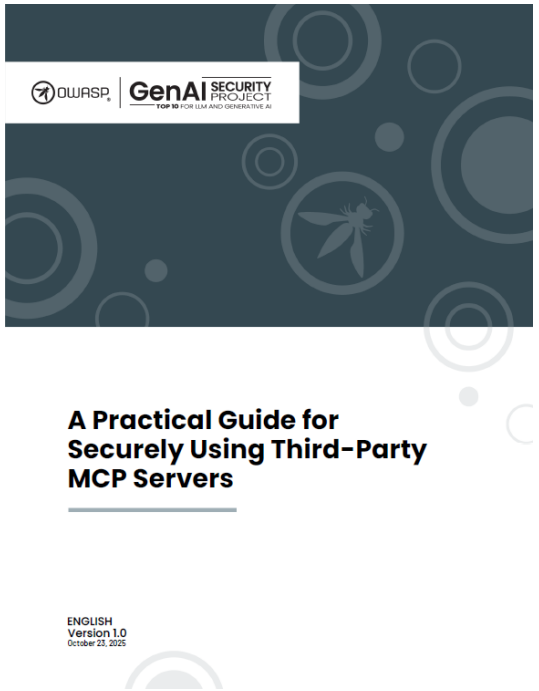
- Risiken beim MCP-Ansatz:
  - Unkontrollierte „bösartige“ Systemaktionen
  - Prompt-Injection-Angriffe bzw. Tool Poisoning
  - frei verfügbare und ggf. manipulierte MCP-Server (remote code execution)
  - Entwendung von Anmeldedaten (Autorisierung und Authentifizierung)
  - Ggf. Unkontrollierte Kosten (u.a. Toolaufrufe)
- Lösungsansätze:
  - Monitoring von MCP-Funktionsaufrufen
  - MCP-Dienste in isolierten Umgebungen (sandbox)
  - Zero-Trust-Sicherheitsprinzip
  - Human-in-the-Loop & Limits



Quelle: https://www.linkedin.com/posts/model-context-protocol-ugcPost-7432684627011706881-7Yi_/?utm_source=share&utm_medium=member_desktop&rcm=ACoAACaTk40B7IF5qgYAomBprKEZ5V-524OEmME

Interessante Quellen

- Sicherheitslücke im MCP-Protokoll von Anthropic bedroht KI-Infrastruktur weltweit, 20. April 2026, https://www.all-about-security.de/sicherheitsluecke-im-mcp-protokoll-von-anthropic-bedroht-ki-infrastruktur-weltweit
- Biswanger, G.: MCP – Die unsichtbare Gefahr in der KI-Integration, BASTA! Spring, 2. – 6. März 2026 in Frankfurt/M.
- Klose, M.: RAG und MCP als Gamechanger für Unternehmensprozesse, 30. Dezember 2025, https://www.computerweekly.com/de/meinung/RAG-und-MCP-als-Gamechanger-fuer-Unternehmensprozesse
- Roden, G.: Mächtigere KI-Systeme mit dem Model Context Protocol (MCP), 30. April 2025 https://www.heise.de/blog/Maechtigere-KI-Systeme-mit-dem-Model-Context-Protocol-MCP-10363599.html
- Gabarda, F. C.: Model Context Protocol (MCP): Sicherheitsrisiken und –kontrollen, 1. Juli 2025, https://www.redhat.com/de/blog/model-context-protocol-mcp-understanding-security-risks-and-controls



Quelle: OWASP https://genai.owasp.org/resource/cheatsheet-a-practical-guide-for-securely-using-third-party-mcp-servers-1-0

Aktuelle Publikationen der Arbeitsgruppe