

Gekommen, um zu bleiben: Cyberangriffe durch KI und die Vorbereitung darauf

Prof. Dr. Maria Leitner

Universität Regensburg, Fakultät für Informatik und Data Science



Universität Regensburg

DFN-CERT Konferenz 2025, Hamburg

11. Februar 2025

100%ige Sicherheit gibt es nicht



Cybersicherheit ist eine Herausforderung



Cybersicherheit ist Teamarbeit



Die Bedrohungslage wächst stetig



Cyberangriffe durch KI



Automatisierung

Skalierbarkeit

Desinformation



Deepfakes

- Bild / Video
- Stimme / Audio



Beispiele



Es kann
alle treffen



World ▾ Business ▾ Markets ▾ Sustainability ▾ Legal ▾ Breakingviews ▾ Technology ▾ Investigations ▾ More ▾

Consultant fined \$6 million for using AI



US Crime + Justice

'Mom, these bad men have me': She believes

scal
kidn

World / Asia



By F
8

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'



By Heather Chen and Kathleen Magramo, CNN

🕒 2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Angriffe werden...

intelligenter
automatisierter
schneller
häufiger

→ schwieriger zu erkennen

Verteidigung mit KI

Anomalieerkennung

Automatisierung

Leichterer Zugang durch Sprachmodelle



Vorbereitung ist das A und O



Aber wie? Es gibt so viele Möglichkeiten



Örtlich

- Virtuell
- Vor Ort

Organisational

- Universitäten
- Hochschulen
- Dienstleister
- Schule
- uvm.

Medial

- Vorträge
- Videos
- Podcasts
- Dokumente
- uvm.

Sozial

- Gruppen
- Individuell

Methodisch

- E-Learning
- Cyberübungen
- uvm.



Cyberübungen

- Diskussionsorientiert, aktionsorientiert
- Interaktiv, dynamisch und realitätsnahe
- Zielgruppe: für alle Interessierte
- Mit oder ohne technischer Infrastruktur (z.B. Cyber Range)
- Folgt einem Drehbuch



Cyberübungen: Varianten



Planspiel

Simulation

Blue Team
Training

Red Teaming

Capture the
Flag (CTF)

Cyber
Defense
Drills (CDX)

Cyberübung

uvm.

Ziele der Teilnehmenden

- Situationen erleben
- Technische Analysen
- Entscheidungen treffen
- Kommunikation intern
- Kommunikation extern
- Test der Notfallpläne
- Dokumentation



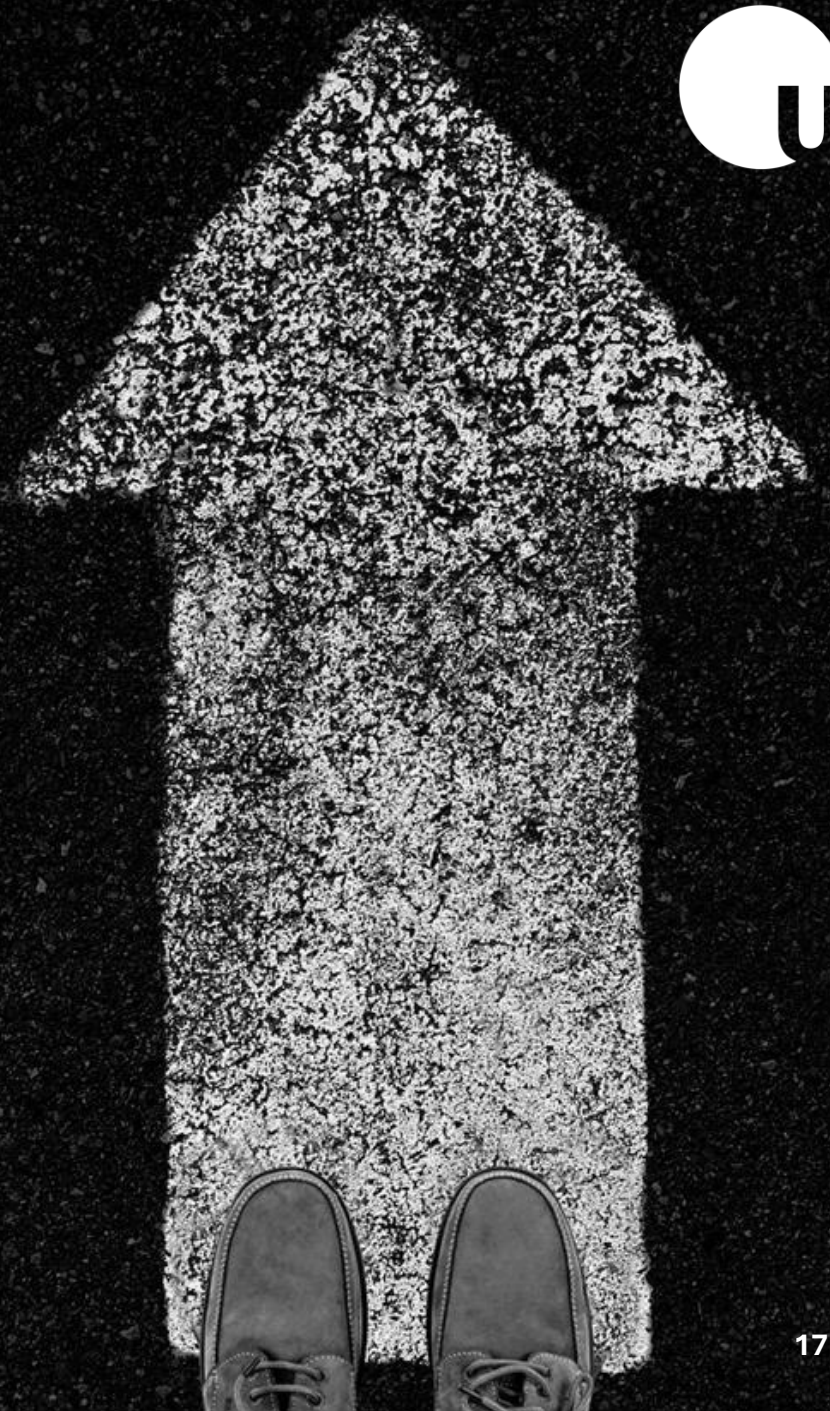
Dynamisch und live

Fehlermachen erlaubt und erwünscht!

Erfahrungsbasiertes Lernen

Für den Ernstfall vorbereitet zu sein!

- Diverse technische Wettbewerbe, z.B.
 - Cyber Security Challenge Germany (Kategorie Earth: für alle)
 - European Cyber Security Challenge (offene Kategorie)
 - DFN Security Challenge
 - CTF Wettbewerbe
- Private Organisationen
- Universitäten, Hochschulen und Forschungseinrichtungen



Zusammenfassung

- Immer relevanter:
 - Wissen und Awareness in Cybersicherheit insbesondere im Umgang mit KI
 - Spielerisches und erfahrungsbasiertes Lernen
- Vorbereitung ist essenziell für Organisationen
- Cyberübungen werden künftig eine größere Rolle einnehmen

Referenzen

Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine learning*, 81, 121-148.

Cyber Security Challenge Germany, URL: <https://cscg.de/>

European Cyber Security Challenge, URL: <https://ecsc.eu/>

Ekelhart, A., Goldenits, G., Mayer, R., & Schuster, V. (2025) Künstliche Intelligenz in der Cybersicherheit Chancen und Risiken. 44 p.

Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., & Park, P. S. (2024). Devising and Detecting Phishing Emails Using Large Language Models. *IEEE Access*, 12, 42131–42146. IEEE Access.

Leitner, M. (2024). *A Scenario-Driven Cyber Security Awareness Exercise Utilizing Dynamic Polling: Methodology and Lessons Learned*. 634–642.

Leitner, M., Frank, M., Langner, G., Landauer, M., Skopik, F., Smith, P., Akhras, B., Hotwagner, W., Kucek, S., Pahi, T., Reuter, L., & Warum, M. (2021). Enabling exercises, education and research with a comprehensive cyber range. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 4.

Steinebach, M., & Waidner, M. (2018). Artificial intelligence in IT security. *Whither Artificial Intelligence*, 31.