

GESELLSCHAFT FÜR INFORMATIK E.V.



Workshop der Fachgruppe SECMGT

Künstliche Intelligenz in der Informationssicherheit

17. Mai 2024

Goethe-Universität Frankfurt am Main

Wir verstehen uns als **Praktiker-Forum**, das sich mit dem Management von Informationssicherheit, den entsprechenden Risiken und Lösungen für Unternehmen, Behörden und anderen Organisationen beschäftigt.

- ☀ wir bieten eine neutrale Plattform „von Spezialisten für Spezialisten“ für Vernetzung, Wissens- und Erfahrungsaustausch,
- ☀ wir bringen uns zukunftsorientiert und ergebnisoffen in die aktuelle Fachdiskussion zur Informationssicherheit ein,
- ☀ wir sind Teil des GI-Fachbereichs "Sicherheit - Schutz und Zuverlässigkeit",
- ☀ wir veranstalten regelmäßig Workshops, bei denen auch Nichtmitglieder stets willkommen sind,
- ☀ wir informieren Sie über: www.secmgt.de und secmgt@gi-fb-sicherheit.de

Leitungsgremium

Machen Sie mit!



Sprecher der Fachgruppe
Dr. Frank Damm
FTI Consulting



stellv. Sprecher der Fachgruppe
Benedict Voßbein
UIMC Dr. Voßbein
GmbH & Co. KG



Prof. Dr. Alexander
Lawall
IU Internationale
Hochschule



Prof. Dr.
Ralf Kneuper
IU
Internationale
Hochschule



Isabel Münch
Bundesamt für
Sicherheit in der
Informationstechnik



Georg Reiss
Stadtwerke
Frankfurt
am Main



Peer Reymann
ITQS GmbH



Marion Steiner
IT-Security@Work
GmbH



Bernhard C. Witt
it.sec GmbH & Co. KG

- Bewegen im Gebäude
- Mittagspause und Mittagessen
- Getränke
- Toiletten

Herzlichen Dank an die Sponsoren!



Ohne externe Unterstützung ist die Durchführung einer solchen Veranstaltung nicht denkbar.

Die Fachgruppe bedankt sich darum bei den Sponsoren:

Goethe-Universität Frankfurt am Main für den Raum.

UIMC DR. VOSSBEIN GmbH & Co KG für die Getränke.

Nächste Termine



Sep/Okt/Nov 2024 Workshop der Fachgruppe
Thema: tbd

Aktuelle Informationen zu unseren Aktivitäten finden Sie immer unter
<https://fg-secmgt.gi.de> oder Sie sprechen uns einfach an.

Künstliche Intelligenz in der Informationssicherheit



Die Buzzwords „Künstliche Intelligenz/KI/Artificial Intelligence/AI, haben gerade in den letzten Jahren, vorwiegend durch die Technologie der Large Language Models (LLM) und Lösungen wie z.B. ChatGPT von der Firma OpenAI, einen extremen Schub in der öffentlichen Wahrnehmung erhalten und scheinen in aller Munde zu sein.

Immer mehr Unternehmen, Produkte und Veranstaltungen nehmen dieses Thema auf und werben mit innovativen Produkten, Lösungen und Ideen. Die immer größere Bekanntheit hat auch Auswirkungen auf die Arbeitswelt, da viele Unternehmen versuchen, die (neu) entdeckten Möglichkeiten zu operationalisieren, was auch eine tiefere Durchdringung der Arbeitswelt bedeutet. Dies liegt vor allem daran, dass mittlerweile nicht nur intelligente Sprachsteuerungen existieren, sondern auch solche Produkte eine standardmäßige Integration in Systeme finden (bspw. Windows Copilot).

Hierbei stellt sich die Frage, ob der momentane Schwung, die mediale Aufmerksamkeit und die forcierte Produktentwicklung in diesem Bereich eine Chance oder ein Risiko für die Informationssicherheit sind. Da Auswirkungen auf die Informationssicherheit erkennbar sind, fand der Begriff der Künstlichen Intelligenz auch Einzug in den jährlichen Bericht „Die Lage der IT-Sicherheit in Deutschland“ des Bundesamts für Sicherheit in der Informationstechnik.

Im Workshop der GI-Fachgruppe SECMGT möchten wir den Spagat zwischen „Aufklärung“ und „Anwendung“ aus verschiedenen Blickwinkeln wagen und das Thema allen Teilnehmerinnen und Teilnehmern näher bringen und mit Ihnen diskutieren. Was ist künstliche Intelligenz? Was kann sie leisten? Welche Einsatzszenarien sind relevant für Unternehmen und welche Risiken der Informationssicherheit haben diese? Bestehen auch Einsatzszenarien zur Verbesserung der Informationssicherheit? Was bedeutet dies für das Management der Informationssicherheit?

Dazu wollen wir uns mit den folgenden Themen beschäftigen:

- wesentliche Eigenschaften der künstlichen Intelligenz und der LLMs,
- konkrete Anwendungsfälle und deren Bedeutung für die Informationssicherheit,
- konkrete Sicherheitsmaßnahmen zur Minderung der Risiken von KI.

Agenda Workshop (1/2)



- 10:00** **Dr. Frank Damm, Sprecher der Fachgruppe SECMGT**
Begrüßung & Vorstellung der Fachgruppe
- 10:30** **Prof. Dr. Thomas Zöller - Professur für Data Science und Artificial Intelligence, Fachbereich Data Science, IU Internationale Hochschule**
KI im Fokus: Einblicke in die Modelle hinter den aktuellen KI-Anwendungen in der Cybersicherheit (inkl. 10 Minuten Diskussion/ FAQ)
- 11:10** Kommunikationspause
- 11:25** **Roland Bernhardt - Data & AI Experte - Microsoft**
KI und Angriffsvektoren (inkl. 10 Minuten Diskussion/ FAQ)
- 12:10** Kommunikations- und Mittagspause

Agenda Workshop (2/2)



- 14:00** **Dr. Christoph Droste, Bundesamt für Sicherheit in der Informationstechnik**
LLMs und andere KI-Tools - Hilfe, Hype und Hybris –
Welche Bedeutung hat KI für die Cybersicherheit? (inkl. 10 Minuten Diskussion/ FAQ)
- 14:40** Kommunikationspause
- 15:00** **Holger Wöhle - E.ON SE - VP Head of Information Security Management**
Use Cases AI in Cyber Security (inkl. 10 Minuten Diskussion/ FAQ)
- 15:45** Kommunikationspause
- 16:00** **Moderierte Diskussion/Erfahrungsaustausch**
Erfahrungen der Teilnehmer
- 16:30** Ende der Veranstaltung

Nach dem Workshop



Teilnahmenachweis/continuing professional education

Diese Veranstaltung dient auch der continuing professional education. Um CPE-Punkte zu sammeln, nutzen Sie eines der vorbereiteten CPE Formulare. Tragen Sie dort Ihren Namen und Ihre Zertifizierung ein. Eine/r der anwesenden Leitungsgremiumsmitglieder bestätigt gegen Ende der Veranstaltung Ihre Teilnahme durch Unterschrift auf dem Formular.

Präsentationen vom Workshop

finden Sie kurz nach der Veranstaltung unter:
<https://fg-secmgt.gi.de/veranstaltung>,
sofern sie uns zur Verfügung gestellt werden.

Welche Auswirkungen können Use Cases für KI auf unsere Bruttowertschöpfung haben?

Wirtschaftsgliederung	2. Gliederungsebene, Volumen > 350 Mrd. €	Bruttowertschöpfung (2023, Mrd. €)	Top 3
Produzierendes Gewerbe	Produzierend und Bau	1.157	1
Dienstleistungsbereiche	Öffentliche Dienstleister, Erziehung, Gesundheit	695	2
	Handel, Verkehr, Gastgewerbe	616	3
	Unternehmensdienstleister	429	
	Grundstücks- und Wohnungswesen	376	
Teilsomme		3.273	
Land- und Forstwirtschaft, Fischerei		30	
Dienstleistungsbereiche	Information und Kommunikation	189	
	Finanz- und Versicherungsdienstleister	143	
	Sonstige Dienstleister	130	
Teilsomme		492	
Gütersteuern		391	
Gütersubventionen		- 36	
Gesamtsumme		4.192	

Quelle: Statistisches Bundesamt, Wichtige Zusammenhänge im Überblick, 2023

**Wir freuen uns auf den fachlichen
Austausch mit Ihnen!**