***Pressekontakt:***
*Tobias Leschka*
*Tel.: + 43 664 57 39 730*
*E-Mail: tobias.leschka@reiterpr.com*

# Generative KI verändert die Bedingungen für Cybersicherheit bei Unternehmen

*Gen AI vergrößert einerseits Schwachstellen, andererseits erwartet mehr als jedes zweite Unternehmen, Bedrohungslagen durch die Technologie schneller zu erkennen und Fehler zu vermeiden.*

**Wien, 20. November 2024 – Die Studie „New defenses, new threats: What AI and Gen AI bring to cybersecurity" des Capgemini Research Institute zeigt auf, dass neue Cybersicherheitsrisiken für Unternehmen entstehen. Aufgrund der starken Verbreitung von KI und generativer KI (Gen AI) ist eine Transformation der Cyberabwehrstrategien notwendig, um Bedrohungen zu prognostizieren, sie zu erkennen und darauf zu reagieren. Zwei Drittel der Organisationen priorisieren derzeit den Einsatz von KI in ihren Cybersecurity Operations.**

Der Studie zufolge betrachten Organisationen KI zwar als Technologie mit strategischer Bedeutung für die Stärkung ihrer Cybersicherheitsstrategien, doch die großflächige Einführung[1] von Gen AI in den verschiedensten Branchen führt zu einer erhöhten Vulnerabilität. Generative KI bringt für Organisationen drei große Risikofelder mit sich: ausgefeiltere Angriffe durch eine größere Anzahl von Akteuren, eine wachsende Angriffsfläche und die Zunahme von Schwachstellen im gesamten Lebenszyklus individueller Gen-AI-Lösungen. Der Missbrauch von KI und generativer KI durch Mitarbeitende verschärft die Situation und kann das Risiko für Datenlecks signifikant steigern.

*„Der Einsatz von KI und generativer KI ist ein zweischneidiges Schwert: Einerseits birgt er neuartige Risiken, andererseits ermöglicht er Organisationen, Cybersicherheitsvorfälle schneller und präziser zu erkennen. Intelligente Tools unterstützen IT-Sicherheitsteams dabei, Angriffe abzuwehren, Strategien kontinuierlich zu verbessern und die Sicherheitslandschaft angesichts der fortwährenden Bedrohungslage stets im Blick zu behalten. Entscheidend für den Erfolg sind eine robuste Datenmanagement-Infrastruktur, geeignete Frameworks, klare ethische Richtlinien für den Einsatz von KI – sowie der Mensch. Trainings und Sensibilisierungsprogramme für Mitarbeitende sollten fester Bestandteil des Arbeitsalltags sein"*, so Arun Varghese, Head of Practices bei Capgemini Österreich.

## Zwei Drittel der Organisationen befürchten stärkere Gefährdung

Nahezu alle befragten Organisationen (97 Prozent) berichten von Sicherheitsverstößen oder -problemen im Zusammenhang mit dem Einsatz generativer KI im vergangenen Jahr. Gen AI birgt darüber hinaus neue Risiken wie Halluzinieren und das Generieren voreingenommener, schädlicher oder unangemessener Inhalte sowie Angriffe durch Prompt Injection[2]. Zwei von drei Organisationen (67 Prozent) befürchten Data Poisoning und den Verlust sensibler Daten über Datensätze, die zum Training von Gen-AI-Modellen verwendet werden.

Auch die Fähigkeit von generativer KI, hochrealistische synthetische Inhalte zu erzeugen, birgt neue Risiken: Mehr als zwei von fünf der befragten Organisationen (43 Prozent) geben an, infolge einer Deepfake-Attacke finanzielle Verluste erlitten zu haben.

[1] Fast ein Viertel (24 Prozent) der Organisationen hat Gen-AI-Funktionalität bereits einigen oder den meisten ihrer Geschäftsbereiche und Standorte zur Verfügung gestellt. Vgl.: Capgemini Research Institute: „Harnessing the value of generative AI 2nd edition: Top use cases across sectors", Juli 2024.

[2] Manipulation des Ausgabeverhaltens von KI- und Gen-AI-Modellen.

Fast 6 von 10 Unternehmen halten es für notwendig, ihr Cybersicherheitsbudget zu erhöhen, um ihre Abwehr entsprechend zu stärken.

**KI und Gen AI unverzichtbar zur Angriffserkennung und Reaktion**

Die Befragung von 1.000 Organisationen, die KI für ihre Cybersicherheit in Betracht ziehen oder bereits einsetzen, zeigt, dass die meisten dies tun, um ihre Daten-, Anwendungs- und Cloud-Sicherheit zu stärken. Denn dank dieser Technologie können sie riesige Datenmengen in kürzester Zeit analysieren, Muster erkennen und potenzielle Sicherheitsverletzungen vorhersagen.

Seit der Integration von KI in ihre Sicherheitskontrollzentren (Security Operations Centers / SOCs) haben mehr als 60 Prozent der Befragten die Dauer bis zur Erkennung von Angriffen um mindestens 5 Prozent verkürzt; fast 40 Prozent stellten eine um mindestens 5 Prozent reduzierte Behebungsdauer von Sicherheitsvorfällen fest.

Drei von fünf der befragten Organisationen (61 Prozent) betrachten KI als unverzichtbar für eine effektive Reaktion auf Bedrohungen, da sie es ermöglicht, proaktive Sicherheitsstrategien gegen immer versiertere Angreifer umzusetzen. Darüber hinaus geht derselbe Anteil der Befragten davon aus, dass sie durch Gen AI auch langfristig proaktive Verteidigungsstrategien realisieren und Bedrohungen schneller erkennen werden. Mehr als die Hälfte von ihnen ist zudem der Ansicht, dass diese Technologie es Cybersicherheitsanalysten erleichtern wird, sich stärker auf Strategien zur Bekämpfung komplexer Gefährdungen zu konzentrieren.

**Methodik**

Das Capgemini Research Institute hat 1.000 Organisationen aus 12 Branchen und 13 Ländern im asiatisch-pazifischen Raum, in Europa und Nordamerika befragt. Diese Organisationen ziehen KI für die Cybersicherheit in Betracht oder setzen sie bereits ein. Sie erwirtschaften einen Jahresumsatz von mindestens einer Milliarde US-Dollar. Die Befragung fand im Mai 2024 statt. Die befragten Organisationen stammen aus den Branchen Automobil, Konsumgüter, Einzelhandel, Banken, Versicherungen, Telekommunikation, Energie- und Versorgungsunternehmen, Luft-, Raumfahrt und Verteidigung, Hightech, Maschinen- und Anlagenbau, Pharma- und Gesundheitswesen sowie aus dem öffentlichen Sektor.

**Über Capgemini**

Capgemini ist ein globaler Business- und Technologie-Transformationspartner für Organisationen. Das Unternehmen unterstützt diese bei ihrer dualen Transformation für eine stärker digitale und nachhaltige Welt – stets auf greifbare Fortschritte für die Gesellschaft bedacht. Capgemini ist eine verantwortungsbewusste, diverse Unternehmensgruppe mit einer über 55-jährigen Geschichte und 340.000 Mitarbeitenden in mehr als 50 Ländern. Kunden vertrauen auf Capgemini, um das Potenzial von Technologie für die ganze Breite ihrer Geschäftsanforderungen zu erschließen. Capgemini entwickelt mit seiner starken Strategie, Design- und Engineering-Expertise umfassende Services und End-to-End-Lösungen. Dabei nutzt das Unternehmen seine führende Kompetenz in den Bereichen KI, Cloud und Daten sowie profunde Branchenexpertise und sein Partner-Ökosystem. Die Gruppe erzielte 2023 einen Umsatz von 22,5 Milliarden Euro.
Get the future you want | www.capgemini.com/at-de

**Über das Capgemini Research Institute**

Das Capgemini Research Institute ist Capgeminis hauseigener Think-Tank in digitalen Angelegenheiten. Das Institut veröffentlicht Forschungsarbeiten über den Einfluss digitaler Technologien auf große Unternehmen. Das Team greift dabei auf das weltweite Netzwerk von Capgemini-Experten zurück und arbeitet eng mit akademischen und technologischen Partnern zusammen. Das Institut hat Forschungszentren in Indien, Singapur, Großbritannien, und den USA.
Besuchen Sie uns auf https://www.capgemini.com/de-de/insights/capgemini-research-institute/.