Pressekontakt:
Melzer PR Group
Christina Danner
Tel.: +43-1-526 89 08-0
E-Mail: office@melzer-pr.com

Studie zu künstlicher Intelligenz und Cybersecurity:

Unternehmen mit Cyberangriffen überfordert

- Fast drei Viertel der Unternehmen weltweit (73 Prozent) testen Anwendungsfälle für KI in der Cybersicherheit
- Zwei von drei Unternehmen planen den Einsatz von KI zur Stärkung ihrer Cybersicherheit bis zum Jahr 2020

Wien, 15. Juli 2019 – Unternehmen erhöhen ihre Investitionen in KI-Systeme zum Schutz vor der nächsten Generation von Cyberangriffen. Zu diesem Ergebnis kommt eine neue Studie des Capgemini Research Institute. Rund zwei Drittel der Unternehmen glauben, ohne KI nicht in der Lage zu sein, auf kritische Bedrohungen zu reagieren. Durch die Fortschritte in Cloud-, Internet-of-Things- (IoT-), 5G- und Dialogschnittstellen-Technologien erhöht sich die Anzahl der Endgeräte, Netzwerke und Benutzeroberflächen – und somit die Anzahl der potenziellen Einfallstore für Angreifer.

Die Studie *Reinventing Cybersecurity with Artificial Intelligence: The new Frontier in Digital Security* befragte 850 Führungskräfte aus den Bereichen IT-Informationssicherheit, Cybersicherheit und IT-Betrieb in zehn Ländern. Die Befragten sind in Großunternehmen aus sieben Branchen tätig. Zudem wurden vertiefende Interviews mit Branchenexperten, Cybersicherheits-Start-ups und Wissenschaftlern geführt.

KI-gestützte Cybersicherheit unverzichtbar

56 Prozent der Führungskräfte weltweit sagten, dass ihre Cybersicherheitsanalysten überfordert sind von der Vielzahl der Datenpunkte, die sie überwachen müssen, um Verletzungen zu erkennen oder zu verhindern. Darüber hinaus hat sich die Art der Cyberrisiken, die ein sofortiges Eingreifen erfordern oder von Cyberanalysten nicht schnell genug behoben werden können, deutlich erhöht. Dazu zählen:

- Cyberangriffe auf zeitkritische Anwendungen. International gaben 42 Prozent an, dass sie gestiegen sind – und zwar durchschnittlich um 16 Prozent
- automatisierte Angriffe, die in einem derart hohen Tempo mutieren, dass sie durch traditionelle Reaktionssysteme nicht neutralisiert werden können. Laut 43 Prozent der Befragten hat deren Häufigkeit um durchschnittlich 15 Prozent zugenommen

Angesichts dieser neuen Bedrohungen ist eine klare Mehrheit der Unternehmen (69 Prozent international) der Ansicht, ohne den Einsatz von KI nicht auf kritische Cyberangriffe reagieren zu können. Bereits um solche Bedrohungen identifizieren zu können, benötigen 61 Prozent weltweit nach eigener Aussage KI.

Führungskräfte erhöhen KI-Investitionen für mehr Cybersicherheit
International ist eine klare Mehrheit der Führungskräfte der Auffassung, dass KI für die Zukunft der Cybersicherheit von grundlegender Bedeutung ist:

- Weltweit gaben 64 Prozent der Befragten an, durch KI die Kosten für die Erkennung von Verletzungen und die Reaktion senken zu können – und zwar um durchschnittlich 12 Prozent.
- 74 Prozent der Führungskräfte gaben an, dass durch KI eine kürzere Reaktionszeit möglich wird: Die nötige Zeit um Bedrohungen zu erkennen, Verstöße zu beheben und Patches zu implementieren, konnte um durchschnittlich 12 Prozent reduziert werden.
- 69 Prozent beobachten zudem, dass KI die Genauigkeit bei der Erkennung von Verstößen verbessert
- 60 Prozent gaben an, dass KI die Effizienz der Cybersicherheitsanalysten erhöht, indem sie die Zeit, die sie mit der Analyse von Fehlalarmen verbringen, verkürzt und ihre Produktivität verbessert

Im Einklang damit werden für das Geschäftsjahr 2020 international bei so gut wie jedem zweiten Unternehmen (48 Prozent) die Budgets für KI in der Cybersicherheit um fast ein Drittel (29 Prozent) steigen. Was die Bereitstellung betrifft, so testen 73 Prozent Anwendungsfälle für KI in diesem Bereich. Nur jedes fünfte Unternehmen nutzte KI dazu vor 2019, doch die Einführung wird weiterhin rasant ansteigen: Fast zwei von drei (63 Prozent) Unternehmen planen, KI bis 2020 einzusetzen, um ihre Verteidigung zu stärken.

„KI bietet enorme Chancen für die Cybersicherheit", sagt Oliver Scherer, CISO von Europas führenden Elektrofachmärkten, der Handelsgruppe Media-Saturn. *„Denn von der Erkennung, manuellen Reaktion und Behebung gelangen Sie zu einer automatisierten Behebung. Das möchten Unternehmen in den nächsten drei bis fünf Jahren erreichen."*

Erhebliche Hindernisse für KI-Einführung im großen Maßstab
Die größte Herausforderung bei der Implementierung von KI für Cybersicherheit ist das mangelnde Verständnis dafür, wie Anwendungsfälle vom Proof of Concept bis zur flächendeckenden Umsetzung skaliert werden können. 69 Prozent der Befragten gaben zu, dass sie in diesem Bereich zu kämpfen hatten.

„Cyberangriffe haben eine neue Komplexität und Geschwindigkeit erreicht – und diese Bedrohung wächst weiter. Immerhin sind sich die meisten Unternehmen bewusst, dass Cybersicherheitsanalysten viele Angriffe nur noch mit Hilfe von KI zuverlässig abwehren können", sagt Dr. Paul Lokuciejewski, Leiter Cybersicherheit bei Capgemini Invent. *„Damit KI ihr volles Potenzial in der Cybersicherheit entfalten kann, brauchen die Unternehmen eine mit der Cyberstrategie klar abgestimmte Roadmap, um eine effiziente Implementierung sicherzustellen. Wichtig ist auch, sich auf die wesentlichen Anwendungsfälle zu fokussieren, die skalierbar sind und den höchsten Return on Investment generieren. Auf diesem Weg können Unternehmen nicht nur Kosten sparen, sondern auch die Wahrscheinlichkeit gravierender Sicherheitsvorfälle reduzieren."*

Die Studie *Reinventing Cybersecurity with Artificial Intelligence: the new frontier in digital security* steht hier zum Download bereit.

Methodik der Studie
Im Rahmen dieser Studie wurden 850 Führungskräfte auf gehobener und höchster Ebene von Unternehmen mit einem Jahresumsatz von mindestens einer Milliarde US-Doller befragt. Sie sind verteilt auf sieben Branchen: Konsumgüter, Einzelhandel, Banken, Versicherungen, Automobil, Versorgungsunternehmen und Telekommunikation. Ein Fünftel der Führungskräfte sind CIOs und jeder Zehnte ist CISO in seinem Unternehmen. Die Führungskräfte gehören zu Unternehmen mit Hauptsitz in Frankreich, Deutschland, Großbritannien und den USA – zu jeweilis 12 Prozent – sowie in Australien, den Niederlanden, Indien, Italien, Spanien und Schweden. Capgemini führte auch Interviews mit führenden

Köpfen der Branche sowie Wissenschaftlern, um den aktuellen Status und die Auswirkungen von KI auf die Cybersicherheit zu untersuchen.

Über Capgemini

Capgemini ist einer der weltweit führenden Anbieter von Management- und IT-Beratung, Technologie-Services und Digitaler Transformation. Als ein Wegbereiter für Innovation unterstützt das Unternehmen seine Kunden bei deren komplexen Herausforderungen rund um Cloud, Digital und Plattformen. Auf dem Fundament von 50 Jahren Erfahrung und umfangreichem branchenspezifischen Know-how hilft Capgemini seinen Kunden, ihre Geschäftsziele zu erreichen. Hierfür steht ein komplettes Leistungsspektrum von der Strategieentwicklung bis zum Geschäftsbetrieb zur Verfügung. Capgemini ist überzeugt davon, dass der geschäftliche Wert von Technologie durch Menschen entsteht. Die Gruppe ist ein multikulturelles Unternehmen mit über 200.000 Mitarbeitern in mehr als 40 Ländern, das 2018 einen Umsatz von 13,2 Milliarden Euro erwirtschaftet hat.

Mehr unter https://www.capgemini.com/at-de/. People matter, results count.

Über das Capgemini Research Institute

Das Capgemini Research Institute[1] 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 Großbritannien, Indien und den USA.
Mehr unter www.capgemini.com/researchinstitute

[1] Das „Digital Transformation Institute" wurde kürzlich in „Capgemini Research Institute" umbenannt.