STUDIE ZUR KI IN DER CYBERSICHERHEIT

München, Februar 2024 – KI-gestützte Angriffe werden von deutschen Unternehmen als größte Cyberbedrohung für dieses Jahr angesehen. Die Software Bewertungsplattform Capterra untersuchte, in welchen Bereichen Unternehmen KI-gestützte Systeme nutzen, um sich vor Angriffen zu schützen und welche Vorteile und Herausforderungen ihnen begegnen.

Im Rahmen der Umfrage wurden 670 Teilnehmer befragt, die an den Cybersicherheits-maßnahmen ihres Unternehmens beteiligt sind und einen Teil des IT-Budgets im Unternehmen für die KI-gestützte Cybersicherheit einplanen.

Interne Bedrohungen durch Mitarbeiter ist eine nicht zu unterschätzende Gefahr

Phishing und Social-Engineering-Angriffe (41 %), interne Bedrohungen durch unbeabsichtigte oder böswillige Handlungen von Mitarbeitern (32 %) sowie Ransomware-Angriffe (29 %) werden als Hauptgründe genannt, warum sich Unternehmen für eine Investition in KI-gestützte Cybersicherheit entschieden haben.

Um Risiken, die durch Phishing oder unbeabsichtigtes Handeln von Mitarbeitern entstehen, entgegenzuwirken, haben KI-Investitionen in diesen Bereichen Priorität:

- Cloud-Sicherheit (56 %)
- E-Mail-Sicherheit (55 %)
- Netzwerksicherheit (47 %)

Vorteile der KI-gestützten Cybersicherheit gegenüber der herkömmlichen Cybersicherheit

Während ein herkömmliches Tool auf einem "statischen" Schutz basiert, bei dem es nur auf eine bekannte Bedrohung des Systems reagiert, basieren die KI-Tools auf einem "dynamischen" Erkennungsansatz. So kann beispielsweise eine höhere Schutzfunktion gewährleistet werden, indem sie Muster oder anomale Aktivitäten erkennen, die mit Bedrohungen im Zusammenhang stehen.

Diese sind die wichtigsten 3 Vorteile für die Studienteilnehmer:

- Verhaltensanalyse: Identifizierung von Anomalien und Mustern, die auf Bedrohungen hinweisen (49 %)
- Echtzeit-Monitoring: Erkennung von Bedrohungen, sobald sie auftreten (48 %)
- Automatisierung: von routinemäßigen Sicherheitsaufgaben wie Warnungspriorisierung, Vorfallsreaktion und Patch-Management (40 %)

Die größten Herausforderungen beim Einsatz künstlicher Intelligenz für die Cybersicherheit

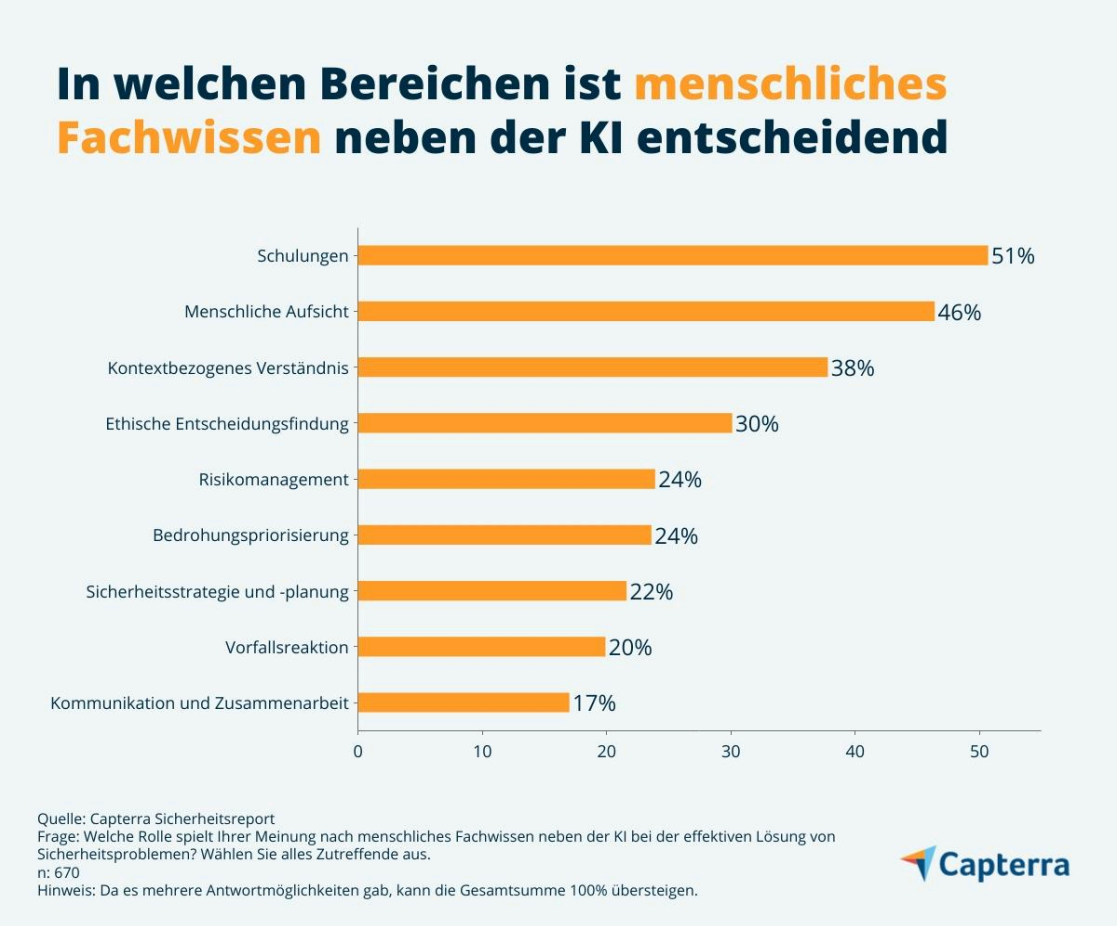
Eine der größten Herausforderungen der Künstlichen Intelligenz in der Cybersicherheit ist die mangelnde Analysegenauigkeit und die Menge an generierten Informationen (43 %). Während KI-Algorithmen große Datenmengen verarbeiten und Muster erkennen können, hängen ihre Analysefähigkeiten von den Informationen ab, auf die sie zuvor trainiert wurden.

Als weiterer Nachteil wurde genannt, dass das System nicht unabhängig sei und daher überwacht werden müsse (40 %). KI-basierte Systeme erfordern qualifizierte Fachkräfte, die effektiv mit ihnen arbeiten können. Darüber hinaus ist eine manuelle Überprüfung erforderlich, um genaue Schlussfolgerungen zu ziehen.

Die dritt- und viertgrößte Herausforderung sind „falsch negative“ (32 %) und „falsch positive“ (28 %) Ergebnisse. Künstliche Intelligenz kann dann harmlose Aktivitäten in einem Unternehmen als verdächtig melden (False Positives) oder umgekehrt echte Bedrohungen ignorieren (False Positives).

KI-Erfolg beruht auf einem Zusammenspiel mit menschlichem Fachwissen

Laut den Studienteilnehmern wird menschliches Fachwissen besonders bei Schulungen benötigt. Auch ist eine menschliche Aufsicht über Entscheidungen der KI und das kontextbezogene Verständnis von Outputs ebenfalls sehr wichtig.



"*Während KI-gestützte Cybersicherheit Automatisierung, Geschwindigkeit und Skalierbarkeit mit sich bringt, sorgen Mitarbeiter für kritisches Denken, ein kontextbezogenes Verständnis und ethische Überlegungen für eine effektive Cybersicherheitsabwehr*," kommentiert **Ines Bahr, Senior Content Analystin bei Capterra**.

Methodik
Um die Daten für diesen Bericht zu erheben, führte Capterra im Zeitraum vom 10. bis 26. November 2023 eine Umfrage unter 902 Mitarbeitenden aus Unternehmen jeder Größe in Deutschland durch. Die Teilnehmenden wurden anhand der folgenden Kriterien ausgewählt:

- Zwischen 18 und 65 Jahren
- Sind in Vollzeit angestellt
- Sind in Deutschland ansässig
- Die Unternehmen der Befragten setzen Sicherheitstools ein

Die Befragten sind in die Cybersicherheitsmaßnahmen ihres Unternehmens involviert, sei es verantwortlich (233), mitwirkend (326) oder darüber informiert (343).

Von diesen für die Umfrage qualifizierten Befragten gaben 670 an, dass ein Teil des IT-Budgets in ihrem Unternehmen für die KI-gestützte Cybersicherheit vorgesehen ist. Dieser zweite Teil der Studie bezieht sich hauptsächlich auf die Antworten dieser 670 Befragten.

Über Capterra
Capterra ist die erste Adresse, um die richtige Unternehmenssoftware zu finden. Unsere Plattform umfasst mehr als 95.000 Lösungen aus 900 Softwarerubriken, bietet über 1,8 Millionen verifizierte Nutzerbewertungen – und hilft Unternehmen Zeit zu sparen, produktiver zu arbeiten und ihr Geschäft erfolgreich auszubauen.

Pressekontakt
Ina Schumann, GDMDeutschlandMarketing@Gartner.com