



Führungsetagen zu KI in der Cyberabwehr: Heute Unsicherheit, morgen Schlüsselrolle

Neue Zahlen der Sophos Management-Studie in DACH zeigen je nach Branche, Unternehmensgröße und Land große Unterschiede in der Einschätzung von KI in der Cybersicherheit.

Aktuell herrscht noch Unsicherheit und überwiegt die Sorge vor krimineller Nutzung von KI. Für die Zukunft glaubt eine Mehrheit an eine Schlüsselrolle der KI in der Cyberabwehr.

Künstliche Intelligenz (KI) ist längst Teil des digitalen Angriffsarsenals: Mit KI-basierten Taktiken wie täuschend echten Deepfakes, intelligentem Phishing oder Social Scams erweitern Cyberkriminelle kontinuierlich ihr Instrumentarium. Doch auch auf der Gegenseite, in den Sicherheitsinfrastrukturen der Unternehmen, erweist sich KI mit seinen Möglichkeiten für Erkennung, Prävention und automatisierter Abwehr als wichtiges Standbein der Cybersicherheit. Und seine Bedeutung wächst an dieser Stelle. Wie hoch aber ist die tatsächliche Relevanz von KI aus Sicht der Unternehmensführungen in Deutschland, Österreich und der Schweiz? Neue Zahlen aus der diesjährigen Sophos Management-Studie in der DACH-Region liefern hierzu ein differenziertes und teils überraschendes Bild.

Chance oder Risiko – die Mehrheit der Führungskräfte zeigt sich unentschlossen

In der DACH-weiten Gesamtbetrachtung hält nur rund ein Fünftel der befragten Führungskräfte (20 Prozent) den Einsatz von KI für „sehr wichtig“ in der Cybersicherheit. 12,3 Prozent aller Befragten (Deutschland 13 Prozent, Schweiz und Österreich je 12 Prozent) halten die Technologie aktuell noch weitestgehend irrelevant für diesen Bereich. Gleichzeitig stuft etwa ein Viertel (28 Prozent) künstliche Intelligenz vor allem als Risiko ein, weil sie auch von Cyberkriminellen aktiv genutzt wird. Der mit Abstand größte Anteil, nämlich 36 Prozent, ist sich unsicher und gibt an, die Rolle von KI in der Cyberabwehr nicht einschätzen zu können.

„Wir erleben derzeit eine digitale Schlüsselphase: Viele Führungskräfte erkennen aktuell die strategische Relevanz von KI für den Cyberschutz noch nicht oder sind verunsichert durch die gleichzeitigen Risiken. Hier braucht es gezielten Wissenstransfer und konkrete Anwendungsbeispiele, um das Potenzial von KI in der Cyberabwehr zu verdeutlichen“, kommentiert Michael Veit, Security Evangelist bei Sophos. Die Empfehlung von Michael Veit ist ein schrittweiser, pragmatischer Einstieg in die intelligenten Technologien: „Unternehmen sollten mit kleinen, kontrollierbaren KI-Pilotprojekten in der Threat Detection oder E-Mail-Sicherheit starten. Wichtig sind außerdem Investitionen in die Weiterbildung der IT-Teams und klare Governance-Richtlinien für den KI-Einsatz. So können sie schrittweise Erfahrungen sammeln und das enorme Potenzial der Technologie für ihre Sicherheitsstrategie erschließen.“

Branchenunterschiede: Handel sieht KI besonders kritisch

Ein Blick in die einzelnen Branchen zeigt, wie stark die Wahrnehmung von KI im Sicherheitskontext variiert. Besonders verhalten reagiert das verarbeitende Gewerbe, in dem knapp 40 Prozent der Befragten angaben, die Bedeutung von KI nicht beurteilen zu können. Im Dienstleistungssektor fällt der Anteil der Unsicheren ebenfalls hoch aus, allerdings wird KI hier auch häufiger als strategisch wichtig bewertet.

Der Handel zeigt sich besonders sensibel gegenüber den Risiken: Dort äußerten länderübergreifend knapp 39 Prozent der Befragten die Sorge, dass KI primär als Angriffs-Werkzeug genutzt werden könnte.

Größere Unternehmen setzen stärker auf KI-Potenzial

Einen deutlichen Einfluss auf die Einschätzung von künstlicher Intelligenz hat auch die Unternehmensgröße. In Betrieben mit mehr als 200 Mitarbeitenden bewerten die Befragten den Einsatz von KI signifikant häufiger als relevant. So stuften rund 28 Prozent der größeren Unternehmen in Deutschland den KI-Einsatz als „sehr wichtig“ ein – ähnlich hoch wie in Österreich (28,6 %) und der Schweiz (35,3 %). In kleineren Unternehmen mit 50 bis 199 Mitarbeitenden hingegen liegt dieser Anteil durchweg niedriger. Die Ergebnisse legen nahe, dass mit steigender Unternehmensgröße auch die digitale Reife und die Bereitschaft zur Auseinandersetzung mit KI wachsen.

Pro oder contra ist eine Frage von jünger oder älter

Auch das Alter der Führungskräfte beeinflusst die Bewertung deutlich. Befragte unter 45 Jahren zeigen in allen drei Ländern eine höhere Zustimmung zur Aussage, dass KI ein bedeutender Faktor für die Cyberabwehr ist. In der Schweiz liegt dieser Anteil beispielsweise bei 26 Prozent unter den Jüngeren, während nur sieben Prozent der älteren Befragten zustimmen. Gleichzeitig erweist sich die Unsicherheit bei den über 45-Jährigen durchweg am höchsten.

Die Schweiz zeigt sich am zurückhaltendsten

In der länderspezifischen Auswertung zeigt sich die Schweiz insgesamt am vorsichtigsten: Nur 16 Prozent der dortigen Befragten halten KI für strategisch wichtig, aber 48 Prozent fühlen sich nicht in der Lage, deren Rolle überhaupt einzuschätzen. In Deutschland (21 Prozent) und Österreich (22 Prozent) sind die Zustimmungswerte deutlich höher – wenngleich auch hier jeweils ein Drittel der Führungskräfte angibt, keine klare Einschätzung treffen zu können.

Managements glauben an eine künftige Schlüsselrolle der KI in der Cyberabwehr

Trotz aktueller Unsicherheiten rund um KI in der Cyberabwehr glauben die meisten an eine Schlüsselrolle der Technologie in der Zukunft: In allen drei Ländern halten es viele Befragte für realistisch, dass KI in den nächsten fünf bis zehn Jahren eine zentrale Rolle in der Cybersicherheit übernehmen könnte. In Deutschland halten das insgesamt 65 Prozent der Befragten für „auf jeden Fall“ oder „vielleicht“ vorstellbar. In Österreich liegt dieser Anteil mit 72 Prozent sogar noch höher. In der Schweiz zeigen sich mit 74 Prozent die größten Zukunftserwartungen an KI-Technologien.

Auffällig ist dabei die Haltung der jüngeren Befragten unter 45 Jahren: In der Schweiz zum Beispiel halten hier 78,3 Prozent den KI-Einsatz künftig für realistisch – deutlich häufiger als ihre älteren Kollegen.

Am Wendepunkt? Von Zögern zu strategischem Handeln

Die Ergebnisse zeigen: Auch wenn derzeit noch viele Fragen offen sind, scheint die strategische Bedeutung von KI in der Cybersicherheit – vor allem mit Blick auf die kommenden Jahre – erkannt zu werden. Vieles deutet darauf hin, dass die Technologie an einem Wendepunkt stehen könnte. So dominieren zwar heute noch Unsicherheit und Risikobewusstsein. Allerdings zeichnet sich für die kommenden Jahre auch ein deutlicher Wandel in der Akzeptanz und vermuteten Rolle ab. Besonders bemerkenswert ist dabei das Gefälle zwischen den Generationen. Jüngere Führungskräfte haben bereits heute einen deutlich positiveren Blick auf die intelligenten Systeme und trauen ihr häufiger künftig eine zentrale Rolle zu.

Für Unternehmen ergeben sich daraus klare Handlungsfelder: Wissensaufbau im Management, praktische Pilotprojekte und eine schrittweise Integration von KI-Tools in die bestehende Sicherheitsarchitektur. „Der Schlüssel liegt darin, KI nicht als abstraktes Konzept zu betrachten, sondern konkrete Anwendungsfälle zu identifizieren und in kleinen Schritten zu testen,“ sagt Michael Veit. „So entsteht Vertrauen durch praktische Erfahrung.“

Über die Umfrage

Ipsos hat im Auftrag von Sophos im Frühjahr 2025 200 C-Level-Managerinnen und -Manager (keine IT-Verantwortlichen) aus verschiedenen Branchen in Deutschland sowie jeweils 50 in Österreich und der Schweiz zum Thema IT-Sicherheit in ihren Unternehmen befragt.

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

X/Twitter: [@sophos_info](#)

Pressekontakt:

Sophos

Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications

Arno Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

Ariane Wendt +49-172-4536839

sophos@tc-communications.de