Presseinformation

Cybersecurity: Kriminelle rüsten mit KI auf, Unternehmen und Behörden ringen um den Anschluss

Zwei Umfragen – unter 1.003 Erwerbstätigen sowie unter 564 Fach- und Führungskräften von Unternehmen und der öffentlichen Verwaltung

Hamburg, 18. Juni 2024 – **Künstliche Intelligenz (KI) ist im Arbeitsalltag angekommen: Rund zwei Drittel der Erwerbstätigen in Deutschland verwenden ChatGPT und Co. zumindest testweise, 37 Prozent arbeiten regelmäßig mit KI-Anwendungen. Doch auch Cyberkriminelle machen sich vermehrt die Stärken Künstlicher Intelligenz zunutze – mit weitreichenden Folgen. Rund drei Viertel der Unternehmen und Behörden sehen eine verschärfte Bedrohungslage durch den böswilligen Einsatz von KI. Im Gegenzug plant jede dritte Organisation, in den kommenden zwölf Monaten eine KI-basierte Cybersecurity-Strategie zu erarbeiten. Jede vierte nutzt bereits KI-gesteuerte Systeme zur Erkennung von Cyberangriffen. Das sind Ergebnisse der Studie „Cybersecurity im Zeitalter von KI" im Auftrag von Sopra Steria.**

In Unternehmen und Behörden hat das Bedrohungspotenzial durch Cyberattacken massiv zugenommen: Durch lahmgelegte Computersysteme, Datenlecks und Lösegelderpressung entstand der deutschen Wirtschaft allein im vergangenen Jahr ein Schaden von 148 Milliarden Euro, so der Branchenverband Bitkom. Durch den Einsatz von KI wird sich nach Ansicht der befragten Fach- und Führungskräfte die Bedrohungslage weiter verschärfen: 45 Prozent rechnen beispielsweise mit zunehmendem Datendiebstahl in den kommenden zwölf Monaten.

„Cybersicherheit ist für Organisationen von entscheidender Bedeutung: Sie wird zwingend benötigt, um die Digitalisierung voranzutreiben, sensible Daten zu schützen, die Verfügbarkeit digitaler Assets zu garantieren und die Aufrechterhaltung des Geschäftsbetriebs zu sichern. Allerdings rüsten Cyberkriminelle mit KI weiter auf, so dass sich Unternehmen und Behörden neu aufstellen müssen. Eine neue, die Möglichkeiten von KI in den Fokus rückende Cybersecurity-Strategie sollte darauf ausgelegt sein, automatisiertes und schnelles Lernen unmittelbar in verbesserte Cyberabwehr umzumünzen", sagt Olaf Janßen, Head of Cybersecurity bei Sopra Steria.

Speziell generative Künstliche Intelligenz (GenAI) verstärkt den Veränderungsdruck deutlich. „Cyberkriminelle nutzen diese, um ihre Attacken zu personalisieren und zu automatisieren. Ein Beispiel: GenAI lässt den Enkeltrick 2.0 mit Sprachgenerierung noch authentischer wirken und analysiert Beziehungen in sozialen Netzwerken, um Angriffe individueller zu gestalten. Mit Sprachmodellen (Large Language Models) können Websites derart angegriffen werden, dass eine KI von der Reaktion auf einen Angriff lernt und ihre Angriffsvektoren wie Phishing oder das Ausnutzen von Sicherheitslücken für eine zweite, verbesserte Attacke anpasst", so Olaf Janßen.

Präventiv statt reaktiv handeln

Angesichts der neuen Möglichkeiten steigt bei den befragten Unternehmen und Behörden die Sorge, dass sich die Kräfteverhältnisse in Richtung der Angreifer verschieben. 71 Prozent der Fach- und Führungskräfte sind der Auffassung, dass Cyberkriminelle KI deutlich besser zum Angriff nutzen, als dies Unternehmen zur Abwehr tun. Doch es gibt auch positive Signale: So wächst in den befragten Organisationen das Bewusstsein für eine KI-basierte Cybersecurity. 81 Prozent planen generell, in den kommenden zwölf Monaten in die Verbesserung ihrer Cybersicherheit zu investieren. Immerhin jede dritte Organisation hat erkannt, dass es durch KI neue Möglichkeiten zum Schutz von IT-Systemen gibt. 54 Prozent sehen ohne den Einsatz von KI künftig keine Chance gegen Cyberangriffe.

„Mit dem Einsatz von KI in der Threat Detection können Unternehmen und Behörden zusätzlich eine auf dem Erkennen von Anomalien basierende Überwachung etablieren und so neuartige Angriffe früher aufspüren. Hierbei handelt es sich vor allem um vorhandene Lücken im System, die aber noch unbekannt und damit von einer regelbasierten Überwachung nicht zu erkennen sind", sagt Janßen. „Ein Grund hierfür ist, dass KI zehntausende Events pro Sekunde auf Anomalien analysieren kann und im Gegensatz zum Menschen immer einsetzbar und nie gestresst oder abgelenkt ist."

Schwachstelle Mensch weiterhin höchstes Risiko

Die größte Gefahr für erfolgreiche Cyberangriffe bleibt auch im KI-Zeitalter der Mensch, so die Umfrageergebnisse. 43 Prozent der Fach- und Führungskräfte sehen unangemessene Reaktionen der Mitarbeitenden auf Phishing-Angriffe als größte Schwachstelle ihrer Organisation – die Top-Nennung in der Befragung. Bei Unternehmen ab 5.000 Mitarbeitenden gab das sogar die Hälfte der Befragten an. Falsche Reaktionen auf KI-gestützte Social-Engineering-Angriffe stellen für 34 Prozent ein erhebliches Risiko dar.

„Phishing-E-Mails sind unter anderem deswegen so gefährlich, da sie kaum mehr als solche zu erkennen sind. Zielgruppengerechte Schulungen und konkrete Handlungsanweisungen sind unerlässlich, um die eigene Organisation vor Phishing-Attacken zu schützen", sagt Stefan Beck, Senior Manager im Team Cybersecurity bei Sopra Steria. „Allerdings kann das Einfallstor Mensch nie ganz geschlossen werden, so dass auch technische Elemente genutzt werden müssen. Durch entsprechende Tools und Prozesse landen Phishing-E-Mails nicht im Postfach, und der Klick auf einen Malware-Link führt nur in eine sogenannte Sandbox, in der Angreifer keinen Schaden anrichten können."

Weitere Gefahren lauern in der ungeregelten Verwendung von KI-Tools (26 Prozent) sowie unzureichenden Regelungen und Sicherheitsbestimmungen für die Arbeit im Homeoffice (23 Prozent), die weit verbreitet ist. Beispielsweise nutzen schon 65 Prozent der Erwerbstätigen KI-Tools im Beruf, allerdings gaben nur 41 Prozent an, dass ihr Arbeitgeber die Nutzung über Schulungen, Leitlinien oder Empfehlungen regelt.

Über die Studie

Der Report „Cybersecurity im Zeitalter von KI" kombiniert eine repräsentative Erwerbstätigenbefragung mit einer Unternehmensbefragung. Der Marktforscher F.A.Z. Business Media | research hat im April und Mai 1.003 Erwerbstätige ab 15 Jahren in Deutschland repräsentativ befragt. Im April hat das Institut zudem 564 Fach- und Führungskräfte der Branchencluster Finance (Banken und Versicherer), Automotive (inkl. Zulieferern) und öffentliche Verwaltung online befragt.

Zur Studienseite geht es hier: www.soprasteria-discover.de/cybersecurity-ki/

Der Studienreport steht hier zum Download zur Verfügung: www.soprasteria-discover.de/cybersecurity-ki/download/

Pressekontakt
Sopra Steria: Nils Ritter, Tel.: +49 (0) 151 40625911, E-Mail: nils.ritter@soprasteria.com
PER-Agency: Maya Engelmann, Tel.: +49 (0) 40 253185-143, E-Mail: maya.engelmann@per-agency.com