Presseinformation

Studie: Mobiles Arbeiten wird zum Cybersecurity-Risiko

Sommerzeit: Cyberkriminelle nutzen Mitarbeitende als Einfallstor

Hamburg, 31. Juli 2024 – **Nicht einmal die Hälfte (48 Prozent) der Unternehmen in Deutschland schult ihre Belegschaft regelmäßig zum Thema Cybersicherheit. Das zeigt die Studie „Cybersecurity im Zeitalter von KI" von Sopra Steria. Gerade in den Sommermonaten benötigen Mitarbeitende eine besondere Sensibilisierung für Cyberrisiken. Denn in der warmen Jahreszeit und in den Schulferien weichen viele ins Homeoffice aus oder arbeiten von unterwegs. Das bedeutet, sie loggen sich über ihr privates WLAN oder einen öffentlichen Hotspot ins Firmennetzwerk ein. Die Folge: Das Gefahrenpotenzial für Phishing und Social Engineering nimmt zu.**

Im Sommer zieht es viele Beschäftigte zum Arbeiten raus aus den Büros. Dann wird vom heimischen Garten aus an wichtigen Projekten gearbeitet oder am Baggersee an Videokonferenzen teilgenommen. Vor allem große Unternehmen bieten zudem so genannte Workation-Modelle an. Sie geben ihren Mitarbeitenden die Möglichkeit, temporär vom Ausland aus zu arbeiten. Wenn die Grenzen zwischen Arbeit und Freizeit verschwimmen, erfordert dies von den Unternehmen mehr und spezifischere Aufklärungsarbeit, spezielle Arbeitsregelungen und technische Vorkehrungen.

Bislang besitzen jedoch nur vier von zehn Organisationen derartige Richtlinien für Arbeit im Homeoffice und Remote Work, die den Zugriff auf Unternehmensdaten von außen regeln, zeigt die Studie. Damit steigt die Gefahr, dass sensible Daten nicht ausreichend geschützt sind, auch weil Angriffe mithilfe von Künstlicher Intelligenz (KI) immer ausgeklügelter werden. 31 Prozent der Erwerbstätigen in Deutschland bestätigen, dass Phishing-Nachrichten kaum noch als solche zu erkennen sind.

Cyberkriminelle nutzen gerne die Urlaubszeit für speziell angepasste Kampagnen: Sie warten darauf, dass öffentliche WLAN-Netze genutzt werden und ohne VPN-Verbindung auf sensible Daten zugegriffen wird, um in die Netzwerke von Unternehmen und Behörden einzudringen. Zudem nutzen sie öffentliche Räume, um nützliche Informationen auf Bildschirmen von Laptops und Smartphones abzugreifen.

Ein Drittel fühlt sich nicht ausreichend informiert

Cyberkriminelle setzen gezielt auf Angriffsmethoden wie Phishing und Social Engineering, um Menschen zu täuschen und vertrauliche Daten zu stehlen", sagt Stefan Beck, Senior Manager im Team Cybersecurity bei Sopra Steria. „Mithilfe von Künstlicher Intelligenz generieren die Angreifer beispielsweise Nachrichten, die den Stil von Vorgesetzten, Kollegen und Geschäftspartnern imitieren und sehr überzeugend klingen. Sie setzen auch darauf, dass Empfänger abgelenkt oder unachtsamer sind als beim Arbeiten im Büro und deshalb eher auf einen Link klicken, einen Anhang herunterladen oder Daten preisgeben", so Beck.

Bislang sind 45 Prozent der Mitarbeitenden der Auffassung, dass ihr Arbeitgeber sie ausreichend über Risiken und Nutzen von KI in der Cybersecurity aufklärt und sensibilisiert.

35 Prozent wünschen sich mehr und bessere Aufklärung, zeigt die Studie. „Es wichtig, dass Arbeitgeber die Sensibilisierungsmaßnahmen stärker auf die individuellen Bedürfnisse ausrichten sollten. Zudem ist Aufklärung in kürzeren Abständen erforderlich, auch saisonal angepasst an die aktuell vorherrschenden Maschen der Kriminellen", sagt Stefan Beck. Denn die Zahl der betrügerischen Nachrichten im Posteingang nimmt zu. Vier von zehn Erwerbstätigen sagen, dass sie heute deutlich mehr Phishing-Nachrichten (E-Mails, WhatsApp, SMS) erhalten als noch vor zwölf Monaten. Aktuell zielen Cyberkriminelle zum Beispiel mit ihren Phishing-Attacken auch auf buchungswillige Urlauberinnen und Urlauber: Sie stellen gefälschte Seiten von Hotels und Reisebüros ins Netz oder verschicken dank generativer KI (GenAI) hochpersonalisierte Reisebestätigungen oder Reise-Rabattangebote.

„Die Angreifer nutzen inzwischen GenAI, wie zum Beispiel ChatGPT, um Phishing-Nachrichten deutlich besser auf ihre Zielpersonen zuzuschneiden", bestätigt Stefan Beck. „Sie lernen automatisiert aus fehlgeschlagenen Angriffen und lassen diese Erkenntnisse sofort in die nächsten Cyberattacken einfließen. Damit erhöhen sie ihre Chance auf einen Treffer, der dann oft ausreicht, um Schaden anzurichten."

Um Cyberangriffe erfolgreich abzuwehren, müssen auch Unternehmen KI einsetzen. So kann zum Beispiel eine KI-basierte Angriffserkennung im Security Operations Center (SOC) einen wertvollen Beitrag leisten. „Bereits in naher Zukunft werden Abwehrstrategien ohne KI-Einsatz keinen ausreichenden Schutz mehr bieten. Hier besteht dringender Handlungsbedarf", prognostiziert Stefan Beck.

Grundverständnis für KI-Gefahren verankern

Um mit den Angreifern Schritt zu halten, sind Unternehmen gleichzeitig gefordert, Aufklärung und Sensibilisierung an die Bedrohungslage im KI-Zeitalter anzupassen. Das Bewusstsein ist vorhanden: 73 Prozent der befragten Unternehmen und Behörden weisen auf verbesserte Phishing-Attacken hin, so die Studie. Unklar ist, in welcher Form, in welcher Häufigkeit und zu welchen speziellen Anlässen.

„Aufklärung und Stichprobentests allein reichen heute ebenso wenig aus wie pauschale Maßnahmen", sagt Cybersecurity-Experte Stefan Beck von Sopra Steria. „Schließlich fällt nicht jeder Mitarbeitende auf dieselben Tricks herein. Nur individuelle und saisonal angepasste Programme können das Bewusstsein für Sicherheitsrisiken nachhaltig stärken. Darüber hinaus sollten Unternehmen auch technische Möglichkeiten ausschöpfen. Lernende KI-Tools können beispielsweise Awareness-Kampagnen an neue oder unbekannte Angriffsmuster anpassen."

Infos und Material zur 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.

Studie zum Download

Infografik

Themenwebsite „Sopra Steria Discover – Cybersecurity im Zeitalter von KI"

Pressefoto Stefan Beck

Über Sopra Steria

Sopra Steria ist ein führendes europäisches Technologieunternehmen mit anerkannter Expertise in den Geschäftsfeldern Consulting, Digital Services und Softwareentwicklung. Der Konzern unterstützt seine Kunden dabei, die digitale Transformation voranzutreiben und konkrete und nachhaltige Ergebnisse zu erzielen. Sopra Steria bietet umfassende End-to-End-Lösungen, die große Unternehmen und Behörden wettbewerbs- und leistungsfähiger machen – und zwar auf Grundlage tiefgehender Expertise in einer Vielzahl von Branchen, innovativer Technologien und eines kollaborativen Ansatzes. Das Unternehmen stellt die Menschen in den Mittelpunkt seines Handelns mit dem Ziel, die Digitalisierung für seine Kunden zu nutzen, um eine positive Zukunft für alle zu gestalten. Mit 56.000 Mitarbeitenden in rund 30 Ländern erzielte der Konzern 2023 einen Umsatz von 5,8 Milliarden Euro.

Die Sopra Steria Group (SOP) ist an der Euronext Paris (Compartment A) gelistet – ISIN: FR0000050809.

Für weitere Informationen besuchen Sie bitte unsere Website www.soprasteria.com.

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