Sophos Management Studie: Robotik, KI oder Firmenwagen – wo Unternehmensführungen in Zukunft Cybergefahren sehen

Deutsche und Schweizer C-Level Manager sehen besonders für das Home-Office Handlungsbedarf, um dort in der Zukunft sensible Daten besser zu schützen. Die Österreicher halten Smart-Building-Technologien für anfällig. In Deutschland erachtet man den Firmenwagen als wichtig und ist bei Zukunftstechnologien eher skeptisch.

Wiesbaden, 23. Mai 2024 – Sophos stellt heute weitere Ergebnisse seiner großangelegten Management-Studie „Chef, wie hältst du es mit der Cybersicherheit“ für Deutschland, Österreich und die Schweiz vor. Ein Teilbereich der Analyse beleuchtet die Frage, wo im Unternehmen C-Level-Verantwortliche künftig verstärkten Bedarf an IT-Sicherheitsmaßnahmen sehen. Befragt wurden Chefinnen und Chefs in Deutschland, Österreich und der Schweiz, die Erhebung richtete sich ausdrücklich nicht an IT-Personal. Die Ergebnisse zeigen, dass in den drei Ländern teilweise deutlich unterschiedliche Einschätzungen bestehen.

Welche Bereiche im Unternehmen sind wegen sensibler Daten besonders anfällig?
Netzwerke, Clouds, Smartphones, Laptops sind als Standards mittlerweile gut im Unternehmen geschützt. Sophos wollte von den Verantwortlichen jedoch auch wissen, welche Bereiche sie für den Schutz sensibler Daten zukünftig als besonders kritisch erachten. Die überwiegende Mehrheit in Deutschland (67,7 Prozent), Österreich (60 Prozent) und der Schweiz (72 Prozent) sieht diesen Bedarf beim mobilen Arbeiten bzw. im Home-Office. Und zwar mehr oder weniger einheitlich über alle befragten Branchen (Handel, Dienstleistung, verarbeitendes Gewerbe) hinweg.

Firmenwagen in Deutschland, Smart Building in Österreich, Smart Factory in der Schweiz
An zweiter Stelle sensibler Sektoren stehen aus Sicht der Managerinnen und Manager die KI-Technologien mit 45,8 Prozent Nennung in Deutschland und 54 Prozent in der Schweiz. Österreich hält Smart Building (intelligente Gebäudetechnik) mit 46 Prozent für wichtiger, hier schafft es KI mit 42 Prozent nur auf den dritten Platz. Das Thema Smart Building rangiert für die befragten deutschen (36,4 Prozent) und Schweizer Unternehmen (38 Prozent) nur an vierter Stelle. Für wichtiger wird in Deutschland die Sicherheit von Firmenwagen erachtet, die mit 37 Prozent der Nennungen hier auf Platz drei rangiert. In Österreich (34 Prozent) und der Schweiz (32 Prozent) landet der Firmenwagen auf Platz fünf der zukünftig vermehrt sicherheitsrelevanten Bereiche.

Unterschiedliche Einschätzung auch bei Automatisierungstechnologien
Automatisierungen und intelligente Vernetzungen in der Produktion – kurz Smart Factory – verdienen für die Schweizer Verantwortlichen ein höheres Sicherheitslevel, mit 46 Prozent steht es bei ihnen nach Remote-Arbeit und KI an dritter Stelle. Die Befragten aus Österreich vergeben hierfür den vierten Platz mit 40 Prozent und Deutschland geht in der Befragung noch einen Punkt herunter, mit 35,8 Prozent Platz fünf.

Ladetechnologien bei Fahrzeugen werden mit den Plätzen 6 (D: 28,9 Prozent) und 7 (AT: 30 Prozent, CH: 24 Prozent) eher nicht so anfällig für zukünftige Cybergefahren gesehen. Dass die eigene und IT-gestützte Energieproduktion, wie etwa Solarpaneele auf den Firmendächern, sensible Daten weitergeben könnte, können sich am ehesten die Österreicher

vorstellen (32 Prozent), Deutschland sieht mit 28,4 Prozent hier etwas weniger Gefahr und die Schweiz hält das mit nur 17 Prozent für eher unrealistisch.

Irgendwie Neuland: Virtuelle Welten und Robotik als unwahrscheinliche Cyberszenarien
Überhaupt gehen bei den virtuellen Themen die Vorstellungskraft der Managerinnen und Manager in den drei deutschsprachigen Ländern weit auseinander:

Gefahr durch virtuelle Welten wie Metaverse oder Avatar-Kommunikation laufen für die Deutschen mit 18,4 Prozent auf Platz acht. Für wenig wahrscheinlich halten es die Österreicher mit Platz neun und 12 Prozent. Nur die Schweiz mit 22 Prozent (Platz acht) kann hier ein gewisses Bedrohungspotenzial erkennen.

Dinge wie Google Brillen, Headup-Display-Brillen, Augmented Reality sind wiederum für die Schweizer mit Platz zehn (12 Prozent) wenig wahrscheinlich. Auch Deutschland kann hier keine große Gefahr erkennen (17,9 Prozent, Platz neun). Lediglich die Befragten in österreichischen Unternehmen können sich in diesem Bereich mit 22 Prozent (Platz acht) einen bestimmten Security-Bedarf vorstellen.

Während das Thema Robotik im Büroalltag, wie zum Beispiel Kaffee-Roboter, für deutsche Managerinnen und Manager als potenzielles Sicherheitsrisiko wenig denkbar erscheint (letzter Platz, 11,9 Prozent), hält man das in der Schweiz zu 26 Prozent für gar nicht so unrealistisch. Dazwischen liegt bei diesem Thema Österreich mit 22 Prozent und Platz acht.

Über die Umfrage:
Ipsos hat im Auftrag von Sophos 201 C-Level-Managerinnen und -Manager aus Handel, Dienstleitung und verarbeitendem Gewerbe 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

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter fortschrittlicher Lösungen zur Abwehr von Cyberangriffen, darunter Managed Detection and Response (MDR) sowie Incident Response Services. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 600.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr. Die Dienste und Produkte von Sophos sind über die cloudbasierte Management-Konsole Sophos Central verbunden und werden vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen.
Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung. Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.
Weitere Informationen unter: www.sophos.de

Pressekontakt:

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

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de