



## **Neue weltweite Studie von Sophos bestätigt: 93 Prozent der Unternehmen haben Probleme mit grundlegenden Sicherheitsaufgaben**

*Risiko: 75 Prozent (65 Prozent in DACH) der Befragten haben Schwierigkeiten, die Ursachen eines Vorfalls zu identifizieren.*

**Wiesbaden, 4. April 2023** – Sophos veröffentlicht heute die neue Studie ["The State of Cybersecurity 2023: The Business Impact of Adversaries on Defenders"](#). In der neuesten internationalen Studie wurde festgestellt, dass weltweit 93 Prozent der Unternehmen die Durchführung grundlegender Sicherheitsaufgaben, wie beispielsweise die Suche nach Bedrohungen, als schwierig empfinden. Zu den Herausforderungen gehört auch das Verständnis, wie es zu einem Angriff gekommen ist. Aus weltweiter Perspektive haben 75 Prozent der Befragten Schwierigkeiten, die Ursache eines Vorfalls zu identifizieren – in DACH bestätigen dies 65 Prozent. Dies kann eine angemessene Reaktion erschweren und Unternehmen anfällig für wiederholte oder [mehrfache Angriffe](#) durch denselben oder unterschiedliche Angreifer machen. Verschärft wird die Situation zudem dadurch, dass 71 Prozent der Befragten weltweit und 60 Prozent in DACH Probleme mit der rechtzeitigen Abhilfe bestätigen.

Weiterhin geben weltweit 71 Prozent der Befragten an, dass es für sie schwierig ist, Signale/Warnungen zu erkennen und zu untersuchen. In DACH bestätigen dies mit 62 Prozent etwas weniger. Ebenfalls 71 Prozent berichten von Problemen bei der Priorisierung von Untersuchungen, womit 64 Prozent der Unternehmen in DACH ihre Schwierigkeiten haben.

„Nur ein Fünftel der Befragten betrachtet Schwachstellen und Remote-Dienste als ein Top-Cybersecurity-Risiko für 2023. Doch die Wahrheit ist, dass diese routinemäßig von [aktiven Angreifern \(Active Adversaries\)](#) ausgenutzt werden. Diese Kaskade an operativen Problemen bedeutet, dass Organisationen nicht das gesamte Bild sehen und möglicherweise auf der Grundlage falscher Informationen handeln. Es gibt nichts Schlimmeres, als mit Sicherheit falsch zu liegen. Externe Audits und Überwachung können zwar helfen, blinde Flecken zu beseitigen. Wir hingegen haben eine Sicht auf die Dinge, wie ein Angreifer sie hat“, sagt John Shier, Field CTO, Commercial, Sophos.

### **Weitere Ergebnisse der Studie:**

- 52 Prozent weltweit und sogar 54 Prozent in DACH der befragten Unternehmen geben an, dass Cyberbedrohungen mittlerweile zu weit fortgeschritten sind, als dass ihr Unternehmen sie alleine bewältigen könnte.
- 64 Prozent international und 61 Prozent in DACH wünschen sich, dass das IT-Team mehr Zeit für strategische Fragen und weniger Zeit für die Brandbekämpfung aufwenden muss. 55 Prozent (56 Prozent in DACH) geben an, dass der Zeitaufwand aufgrund von Cyberbedrohungen die Arbeit des IT-Teams an anderen Projekten beeinträchtigt.
- 94 Prozent weltweit und 96 Prozent in DACH geben an, dass sie mit externen Spezialisten zusammenarbeiten, um ihre interne Abteilung zu skalieren. Gleichzeitig befasst sich jedoch nach wie vor die Mehrheit selbst mit der Bewältigung von Bedrohungen, anstatt auch hier einen ausgelagerten Ansatz zu wählen.

„Die Bedrohungen von heute erfordern eine rechtzeitige und koordinierte Reaktion. Leider verharren zu viele Unternehmen im reaktiven Modus. Dies wirkt sich nicht nur auf die Prioritäten im Kerngeschäft aus, sondern fordert auch einen beträchtlichen menschlichen Tribut: Mehr als die Hälfte der Befragten gibt an, dass ihnen Cyberangriffe schlaflose Nächte

bereiten. Durch die Beseitigung des Rätselratens und die Anwendung defensiver Kontrollen, die auf verwertbaren Informationen basieren, können sich IT-Teams auf die Unterstützung des Business konzentrieren, anstatt zu versuchen, den Dauerbrand aktiver Angriffe zu löschen“, so Shier.

Die vollständige Studie „The State of Cybersecurity 2023: The Business Impact of Adversaries on Defenders“ steht bei Sophos [hier](#) zum Download bereit.

#### **Über die Studie:**

Die Daten der Studie „The State of Cybersecurity 2023: The Business Impact of Adversaries on Defenders“ stammen aus einer unabhängigen Befragung, die im Januar und Februar 2023 unter 3.000 IT- und Cybersicherheitsverantwortlichen in 14 Ländern durchgeführt wurde.

#### **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 [!\[\]\(a870788d6ed9b8fd294b7654a8c8526b\_img.jpg\)](#) und [!\[\]\(18065afa4ef6662bca9f3f6088f7de30\_img.jpg\)](#)

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

Twitter: [@sophos\\_info](#)

## **Über Sophos**

Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. 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 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.

Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und 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](http://www.sophos.de)

## **Pressekontakt:**

Sophos

Jörg Schindler, PR-Manager Central & Eastern Europe

[joerg.schindler@sophos.com](mailto: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](mailto:sophos@tc-communications.de)