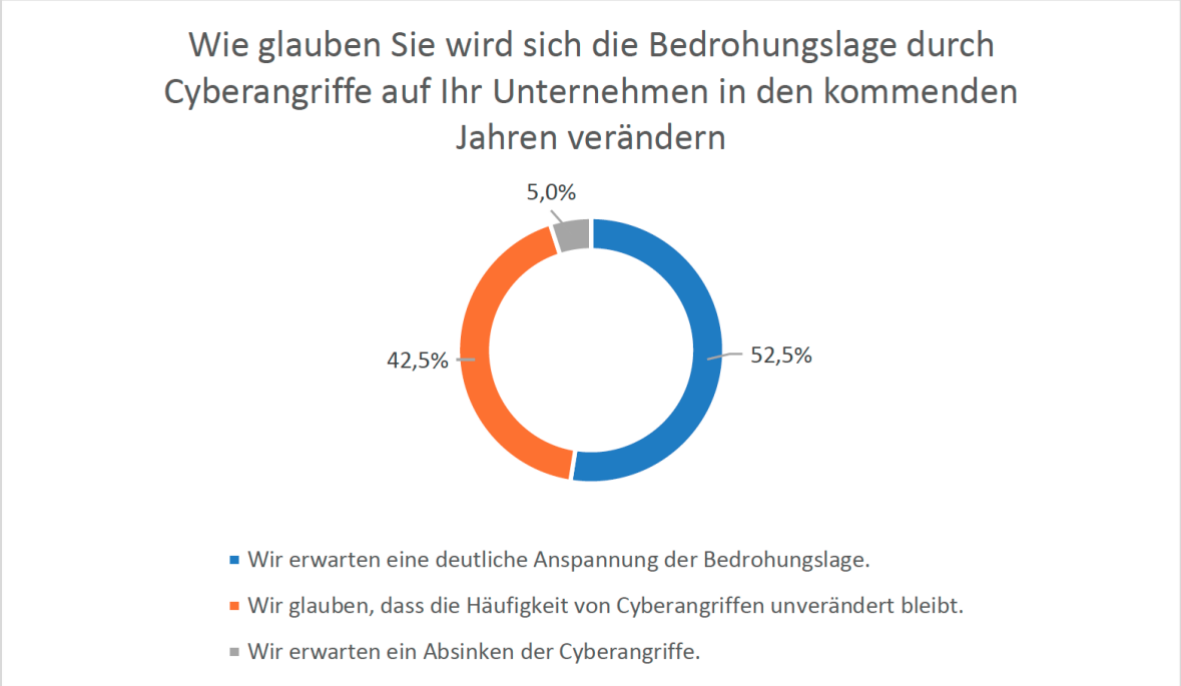
Cybersicherheit in Unternehmen:
70 Prozent erwarten eine Auslagerung ihrer Cybersicherheit

- *IT-Verantwortliche erwarten mehrheitlich eine Verschärfung der Bedrohungslage.*
- *Unternehmen setzen zunehmend auf Sicherheitskonzepte, Sensibilisierung von Beschäftigten, externe Dienstleistungen und Versicherungen.*
- *Die Mehrzahl rechnet mittel- bis langfristig damit, die Cybersicherheit auszulagern.*

Besonders zum Jahresauftakt machen Analysen der Cyberkriminalität des vergangenen Jahres ebenso wie Ausblicke auf das aktuelle neue Jahr dir Runde. Wie Unternehmen selbst die Bedrohungslage einschätzen und welche weiteren Maßnahmen zur Cybersicherheit sie planen, wollte Sophos im Rahmen einer Studie herausfinden.

Mehr als die Hälfte der im Rahmen einer Cybersecurity as a Service-Studie von Sophos befragten Unternehmen (53 Prozent) erwartet demnach künftig eine deutliche Zunahme der Cyberbedrohungen. 43 Prozent dagegen glauben, dass das aktuelle Niveau an Cyberangriffen konstant bleiben wird. Lediglich fünf Prozent der Befragten gehen davon aus, dass die Anzahl der Angriffe abnehmen wird.



Wie Unternehmen sich wappnen wollen

Ein so genanntes Security Operations Center (SOC) ist ein entscheidendes Element einer modernen, proaktiven Sicherheitsstrategie. Es fokussiert sich auf die Erkennung, Analyse und Reaktion von Sicherheitsvorfällen, um die entsprechenden Risiken zu minimieren und Daten sowie geschäftskritische Prozesse in Unternehmen bestmöglich zu schützen.

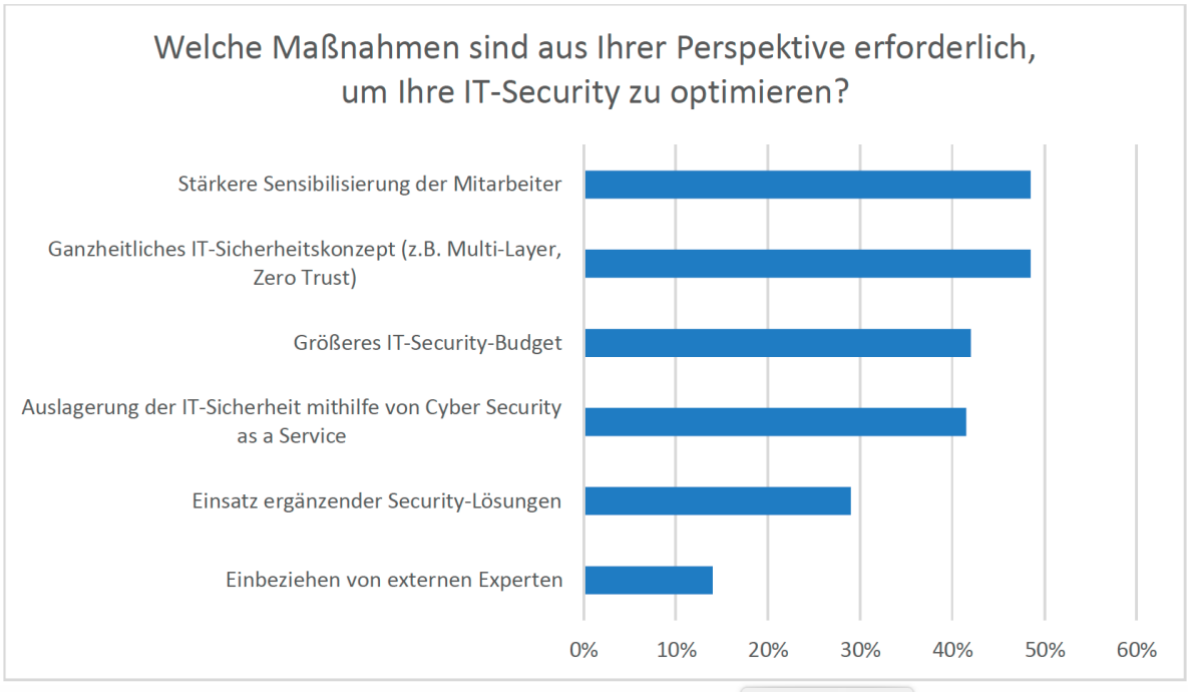
Die Ergebnisse der Befragung zeigen, dass die Mehrheit der Unternehmen die Vorteile eines SOCs bereits erkannt und entsprechende Maßnahmen umgesetzt haben. So sind in fast drei von vier Unternehmen (73 Prozent) Security Operations Center aktiv im Einsatz. 41 Prozent setzen dabei auf externe SOC-Services von Dienstleistern, während 32 Prozent ihre SOCs

intern betreiben. Gleichzeitig verzichtet fast ein Viertel der Unternehmen (24 Prozent) auf ein SOC und drei Prozent können hierzu keine Angaben machen.

Konzipieren, sensibilisieren, auslagern und versichern
Für die weitere Optimierung seiner IT-Sicherheit bewertet fast jedes zweite Unternehmen (49 Prozent) die stetige Mitarbeitersensibilisierung als essenziell. Ihr Ziel ist es, Beschäftige über potenzielle Sicherheitsrisiken und entsprechende Verhaltensregeln aufzuklären.

49 Prozent der befragten Unternehmen betonen zudem die Bedeutung eines ganzheitlichen IT-Sicherheitskonzepts. Ein derartiges Konzept sollte fortschrittliche Ansätze integrieren wie die Multi-Layer-Sicherheit, die verschiedene Abwehrmechanismen auf unterschiedlichen Ebenen vorsieht, sowie das Zero-Trust-Prinzip, welches grundsätzlich keinem Zugriff vertraut und stets Verifizierungen erfordert.

Für 42 Prozent der Unternehmen stellt die Auslagerung der IT-Security durch Cyber Security as a Service ein Mittel zur Stärkung der Sicherheitsinfrastruktur dar. Als weitere Maßnahmen werden größere IT-Budgets (42 Prozent), Einsatz ergänzender Security-Lösungen (29 Prozent) sowie das Einbeziehen von externen Experten (14 Prozent) genannt. Insgesamt zeigt sich, dass Unternehmen die strategische Relevanz einer robusten Sicherheitsinfrastruktur erkennen und in entsprechende Lösungen und Bildungsmaßnahmen investieren.



Zusätzlich dazu lässt sich ein positiver Trend im Bereich der Cyberversicherungen beobachten. Bereits 85 Prozent der Unternehmen haben proaktiv eine Cyberversicherung abgeschlossen, um sich gegen finanzielle Risiken von Sicherheitsvorfällen abzusichern. Bemerkenswert ist, dass die Hälfte dieser versicherten Unternehmen (50 Prozent) innerhalb der letzten 12 Monate bessere Konditionen aushandeln konnte, nachdem sie ihre Sicherheitsmaßnahmen verstärkt haben. Dennoch bleibt eine Minderheit von 10 Prozent der Befragten, die sich gegen Cyberangriffe noch nicht versichert haben.

Blick in die Zukunft: 70 Prozent wollen die Cybersicherheit perspektivisch auslagern
Zusätzlich zu Cyberversicherungen setzen Unternehmen auf verschiedene Strategien, um ihre IT-Sicherheit zu gewährleisten. So sind rund 70 Prozent der befragten IT-Verantwortlichen der Ansicht, dass die Sicherheit ihrer IT-Systeme mittel- bis langfristig externen Sicherheitsdienstleistern anvertraut werden sollte. Zusätzlich dazu setzen 60 Prozent der

Befragten auf technologiegetriebene Sicherheitslösungen, die durch verhaltensbasierte Erkennungsmethoden und künstliche Intelligenz (KI) ergänzt werden. Diese Kombination ermöglicht eine präzisere und proaktive Bedrohungserkennung. Alarmierend ist allerdings, dass 57 Prozent zugeben, erst nach einem tatsächlichen Sicherheitsvorfall in umfassende Sicherheitsmaßnahmen zu investieren. Ein reaktiver Security-Ansatz, bei dem Maßnahmen erst nach einem Sicherheitsvorfall ergriffen werden, kann langfristige Schäden verursachen und die Unternehmensreputation gefährden.

Über die Studie:
Die Befragung wurde mit 200 IT-Verantwortlichen und -Entscheidern aus deutschen Unternehmen mit 100 bis 999 Beschäftigten von techconsult im Auftrag von Sophos durchgeführt.

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, PR-Manager Central & Eastern Europe
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