# Weitreichende Auswirkungen der Organisationsstruktur auf die Cybersicherheit

*Auf Basis einer Umfrage untersucht Sophos drei Organisationsszenarien und beurteilt deren Wirkung in der Cybercrime-Abwehr. Ein spezielles Cybersicherheitsteam als Teil der IT-Organisation erzielt die besten Ergebnisse.*

Ausgebildetes und erfahrenes Fachpersonal zu finden, ist eine der großen Herausforderungen in Unternehmen, um die Cybersicherheit zu gewährleisten. Vor dem Hintergrund dieser Diskussion ist es daher besonders wichtig, die wenigen verfügbaren Fachkräfte in die Lage zu versetzen, die größtmögliche Wirkung bei der Abwehr von Cyberrisiken zu erzielen. In diesem Zusammenhang geht Sophos in einer Umfrage bei rund 3.000 Führungskräften aus IT und Cybersicherheit in 14 Ländern auf die Frage ein, wie unterschiedliche Organisationsstrukturen Einfluss auf die Ergebnisse der Cybersicherheit haben.

**Auf den Blickwinkel kommt es an**
In der Analyse wurden die Erfahrungen in der Cybersicherheit unter Einbeziehung der Organisationsstruktur betrachtet. Ziel war es einen Zusammenhang zwischen Struktur und Ergebnissen zu finden und falls es diesen gibt, welche Struktur die besten Ergebnisse liefert. Sophos untersuchte drei Szenarien:
Szenario 1: Das IT-Team und das Cybersicherheitsteam sind getrennte Organisationen.
Szenario 2: Ein spezielles Cybersicherheitsteam ist Teil der IT-Organisation
Szenario 3: Kein spezielles Cybersicherheitsteam, das IT-Team verwaltet die Cybersicherheit

**Beste Ergebnisse für Szenario 2 – sofern Fähigkeiten und Kapazitäten vorhanden sind**
Die Analyse der Umfragedaten ergibt, dass Unternehmen mit einem speziellen Cybersicherheitsteam innerhalb eines umfassenderen IT-Teams im Vergleich zu den anderen beiden Szenarien die besten Gesamtergebnisse im Bereich Cybersicherheit erzielen. Die schlechtesten Resultate erlangen Unternehmen, bei denen die IT- und Cybersicherheitsteams getrennt agieren (Szenario 1).

Auch wenn die Cybersicherheit und der IT-Betrieb im weitesten Sinne getrennte Fachbereiche zu sein scheinen, lassen sich die Erfolge von Szenario 2 damit erklären, dass die Disziplinen eng miteinander verknüpft sind. Beispielsweise wirken sich Kontrollen der Cybersicherheit häufig direkt auf die IT-Lösungen aus, während die Umsetzung einer guten Cyberhygiene, wie das Patchen und Sperren von RDP, häufig vom IT-Team durchgeführt wird.

Allerdings zeigen die Analysen auch, dass die Art und Weise, wie Unternehmen ihre Teams strukturieren, kaum einen Einfluss auf die Sicherheitsergebnisse hat, wenn ihnen die grundlegenden Fähigkeiten und Kapazitäten im Bereich Cybersicherheit fehlen. Eine Option für dieses Problem sind externe Partner und Security-Dienstleister. Allerdings sollen Organisationen, die ihre Fähigkeiten durch spezialisierte externe Cybersicherheitsexperten (z. B. MDR-Anbieter oder MSSPs) ergänzen möchten, nach flexiblen Partnern suchen, welche als Erweiterung des gesamten internen Teams arbeiten anstatt ausschließlich für die Security-Teams.

**Struktur der Cybersicherheit hat Auswirkungen auf die Vorfälle**
Die Analyse vergleicht Erfahrungen in den drei Szenarien und deckt vier bemerkenswerte Ergebnisse auf.

1. Ursache von Ransomware-Angriffen

Interessanterweise variiert die Ursache von Ransomware-Angriffen je nach Organisationsstruktur. Bei Szenario 1 hat fast die Hälfte der Angriffe (47 Prozent) mit einer ausgenutzten Sicherheitslücke begonnen, während 24 Prozent auf kompromittierte Anmeldedaten zurückzuführen sind. Bei Szenario 2 sind ausgenutzte Sicherheitslücken (30 Prozent) und kompromittierte Zugangsdaten (32 Prozent) mit fast gleicher Wahrscheinlichkeit die Hauptursache für die Angriffe. Bei Unternehmen mit Szenario 3 wurden fast die Hälfte der Angriffe (44 Prozent) mit kompromittierten Anmeldedaten begangen und nur 16 Prozent mit einer ausgenutzten Sicherheitslücke.

2. Wiederherstellung nach einer Ransomware

Unternehmen des Szenario 1 zahlten weitaus häufiger Lösegeld als die anderen und meldeten zugleich den geringsten Anteil an Backups zur Wiederherstellung verschlüsselter Daten. Die Unternehmen des Modells 1 zahlten nicht nur am häufigsten Lösegeld, sondern höhere Summen, wobei der Mittelwert mehr als doppelt so hoch war wie bei den Szenarien 2 und 3.

3. Sicherheitsmaßnahmen

Eine der wichtigsten Erkenntnisse ist, dass Organisationen aus dem Szenario 2 bei der Durchführung von Sicherheitsmaßnahmen am besten abschneiden, während die meisten Organisationen eine Herausforderung darin sehen, eine effektive Security-Operations selbstständig zu etablieren. Zusammengefasst macht es kaum einen Unterschied, wie man das Team strukturiert, wenn es an den notwendigen Kapazitäten und Fähigkeiten mangelt.

4. Tägliches Cybersicherheitsmanagement

In diesem Bereich gibt es viele Gemeinsamkeiten zwischen den drei Szenarien und sie stehen alle vor ähnlichen Herausforderungen. Mehr als die Hälfte der Befragten aller Szenarien bestätigen, dass die Cyberbedrohungen inzwischen so weit fortgeschritten sind, dass ihre Organisation sie nicht mehr allein bewältigen kann (60 Prozent Szenario 1; 51Prozent Szenario 2; 54 Prozent Szenario 3).
Die drei Szenarien teilen zudem ähnliche Sorgen in Bezug auf Cyberbedrohungen und -Risiken. Datenexfiltration und Phishing (einschließlich Spear-Phishing) gehören bei allen zu den größten Cyberbedrohungen, und die Fehlkonfiguration von Sicherheitstools ist das am häufigsten wahrgenommene Risiko.

**Hinweis zur Analyse**

Diese Analyse bietet Einblicke in die Korrelation zwischen der IT-/ Cybersicherheitsstruktur und den Ergebnissen, untersucht aber nicht die Gründe hinter diesen Ergebnissen, also die Kausalität. Jedes Unternehmen ist anders und die Struktur der IT-/ Cybersicherheitsfunktion ist eine von vielen Variablen, die sich auf die Bereitschaft auswirken können, gute Sicherheitsergebnisse zu erzielen – einschließlich der Branche, des Qualifikationsniveaus der Teammitglieder, des Personalbestands, des Alters des Unternehmens und mehr.

Um mehr zu erfahren und die vollständige Analyse zu sehen, laden Sie bitte den kompletten Bericht „The Impact of Organizational Structure on Cybersecurity Outcomes„ herunter.

**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, 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