KMUs schneiden bei der Cyberresilienz schlecht ab

Eine Studie von Sophos bestätigt ein überdurchschnittliches Risikopotenzial für kleine und mittelständische Unternehmen vor allem aufgrund des Fachkräftemangels.

Sophos veröffentlicht einen neuen Bericht über die Auswirkungen des Fachkräftemangels im Bereich Cybersicherheit. Dem Bericht liegt eine umfangreiche Studie unter 5.000 IT-/Cybersecurity-Experten in 14 Ländern zugrunde. Er zeigt teils gravierende Auswirkungen auf kleine und mittlere Unternehmen (KMUs) beziehungsweise Unternehmen mit 100 bis 500 Mitarbeitern.

Die wichtigsten Ergebnisse sind:

- **KMUs sind unverhältnismäßig stark vom Fachkräftemangel betroffen:** Der Mangel an interner Cybersecurity-Fähigkeit/-Expertise wird als zweitgrößtes Cyber-Security-Risiko eingestuft, das nur noch von Zero-Day-Bedrohungen übertroffen wird.
- **KMUs haben bei Ransomware-Angriffen eine höhere Rate an Datenverschlüsselung:** Bei 74 Prozent der Ransomware-Angriffe auf KMUs gelingt es den Angreifern, die Daten zu verschlüsseln.
- **Kein Monitoring:** In 33 Prozent der Fälle gibt es in KMUs niemanden, der aktiv überwacht, untersucht und auf Warnungen reagiert.
- **Untersuchung verdächtiger Sicherheitswarnungen ist eine Herausforderung:** 96 Prozent der Mitarbeiter in KMUs finden mindestens einen Aspekt der Untersuchung verdächtiger Sicherheitswarnungen schwierig.
- **KMUs haben Schwierigkeiten, bösartige Warnungen/Vorfälle zu beseitigen:** 75 Prozent der KMUs finden es schwierig, bösartige Warnungen oder Vorfälle rechtzeitig zu beheben.

Aaron Bugal, Field CTO bei Sophos, hierzu: „Der Mangel an internen Cybersecurity-Fähigkeiten ist heute eines der größten Risiken für Unternehmen. Wenn man diese wachsende Qualifikationslücke mit der großen, zusätzlichen Burnout-Krise unter Cybersecurity-Fachleuten kombiniert, sind kleine Unternehmen noch anfälliger für Angriffe. Da 91 Prozent der Ransomware-Angriffe außerhalb der üblichen Geschäftszeiten stattfinden, müssen KMUs in der Lage sein, ihre Netzwerke rund um die Uhr zu überwachen, um bösartige Aktivitäten zu erkennen, bevor ein Angreifer Daten exfiltrieren oder verschlüsseln kann."

Unternehmen sollten eine Bestandsaufnahme ihrer Sicherheitskapazitäten vornehmen und nach Möglichkeiten zur Verbesserung ihrer allgemeinen Cyberresilienz suchen. Es ist ein empfindliches Gleichgewicht zwischen Menschen, Prozessen und Technologie. Wenn Unternehmen die Stärken und Grenzen ihres Teams verstehen, können sie diese mit externem Fachwissen ausgleichen und die Sicherheitslage verbessern.

Der vollständige Report steht hier zum Download bereit.

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