SOPHOS

Cybersecurity-Fachkräftemangel in KMUs: Folgen und Lösungen

Wie wirkt sich der Fachkräftemangel im Bereich Cybersecurity auf kleine und mittlere Unternehmen in der Praxis aus? Wie können die Herausforderungen gelöst werden, ohne dabei das Budget zu sprengen oder Mitarbeiter zu überlasten? Antworten auf diese Fragen finden Sie in diesem Whitepaper.

Sophos-Whitepaper. Oktober 2024

Einleitung

Der globale Fachkräftemangel im Bereich Cybersecurity ist allgemein bekannt. Ein Ende ist auch nicht abzusehen. Daher müssen kleine und mittlere Unternehmen entsprechende Maßnahmen ergreifen, um einen effektiven Cyberschutz zu gewährleisten.

Um die damit verbundenen Herausforderungen anzugehen, muss zunächst einmal klar sein, wie diese konkret aussehen. Dieser Report liefert Ihnen Ergebnisse einer weltweiten, unabhängigen Umfrage unter IT-/Cybersecurity-Experten, die zeigen, wie sich der Fachkräftemangel auf kleine und mittlere Unternehmen im Alltag auswirkt. Auf Basis dieser Einblicke erhalten Sie praktische Tipps, wie Sie diese Herausforderungen im Rahmen begrenzter Ressourcen meistern können. Darüber hinaus werden Sophos-Lösungen vorgestellt, mit denen kleinere Unternehmen und Organisationen bessere Cybersecurity-Ergebnisse erzielen können.

Über die Studie

Sophos beauftragte eine unabhängige Umfrage unter 5.000 IT/Cybersecurity-Experten aus 14 Ländern. 1.402 der Befragten sind in Unternehmen/Organisationen mit 100 bis 500 Mitarbeitern tätig, was in diesem Report als kleine und mittlere Unternehmen (KMUs) bezeichnet wird. Die Studie wurde im ersten Quartal 2024 durchgeführt.

Der Fachkräftemangel trifft kleinere Unternehmen überproportional

Der Fachkräftemangel trifft KMUs stark – und überproportional. Laut Umfrage **bewerten Unternehmen mit weniger als 500 Mitarbeitern fehlendes Fachwissen/Fachpersonal im Bereich Cybersecurity als zweitgrößtes Cybersecurity-Risiko.** Nur Zero-Day-Bedrohungen werden als noch größere Gefahr betrachtet. Bei Unternehmen mit über 500 Mitarbeitern steht der Faktor „fehlendes Fachwissen/Fachpersonal" hingegen an siebter Stelle.

Frage: Was sind Ihrer Meinung nach die drei größten Cybersecurity-Risiken für Ihr Unternehmen? Relative Platzierung von „Fehlendes internes Fachwissen/Fachpersonal im Bereich Cybersecurity"

KMUs (Anzahl Antworten: 1.402)	GRÖSSERE UNTERNEHMEN (Anzahl Antworten: 3.598)	
100–500 MITARBEITER	501–1.000 MITARBEITER	1.001–5.000 MITARBEITER
Platz 2	Platz 7	Platz 7

Unternehmen mit weniger als 500 Mitarbeitern sehen fehlendes internes Fachwissen/Fachpersonal im Bereich Cybersecurity als ihr zweigrößtes Cybersecurity-Risiko. Bei Unternehmen mit mehr als 500 Mitarbeitern steht dieser Punkt erst an siebter Stelle.

Unternehmen und Organisationen aller Größen sind vom Fachkräftemangel betroffen. Es wird allerdings deutlich, dass KMUs die Auswirkungen am stärksten spüren. Größere Unternehmen und Organisationen betrachten „fehlende Cybersecurity-Tools" (Platz 2 bei Unternehmen mit 501–1.000 Mitarbeitern) und „gestohlene Zugangsdaten" (Platz 2 bei Unternehmen mit 1.001–5.000 Mitarbeitern) als größere Risiken. Für kleinere Unternehmen sind diese Punkte weniger relevant, da diese vorrangig damit zu kämpfen haben, wie sie mit wenig Fachpersonal ihre vorhandenen Systeme betreiben können.

Fachkräftemangel: Ein zweifaches Problem

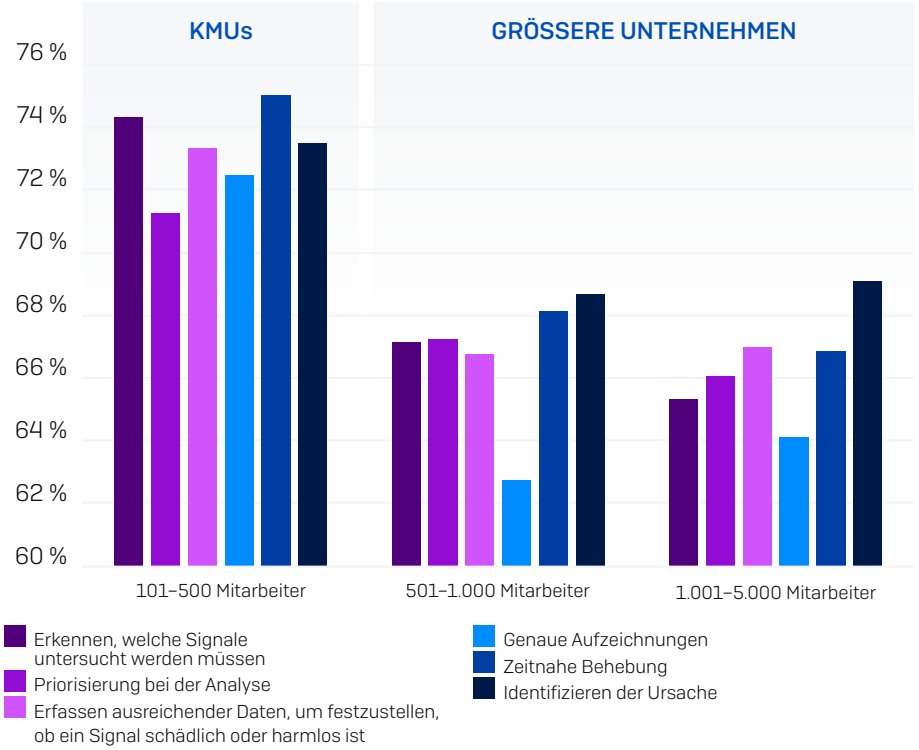
Der Grund für das fehlende Fachwissen ist einfach: Es gibt nicht genug qualifizierte Fachkräfte für Cybersicherheit. Dies wirkt sich in zweierlei Hinsicht auf KMUs aus.

Mangelnde Expertise

Um für eine effektive Cybersecurity zu sorgen, ist umfassende Expertise erforderlich – und die Anforderungen steigen stetig. Cyberangriffe werden immer komplexer, sodass ein hohes Maß an Erfahrung und Fachwissen vorhanden sein muss, um sie zu stoppen.

Die Umfrage zeigt: **96 % der Befragten aus kleineren Unternehmen tun sich schwer mit der Analyse von Warnmeldungen**. Zwar haben auch größere Unternehmen Probleme in diesem Bereich, doch für KMUs ist die Lage am schwierigsten.

Herausforderungen von Unternehmen bei der Analyse von Warnmeldungen



Für KMUs ist es besonders schwierig, intern ausreichend Cybersecurity-Expertise aufzubauen. Wenn das IT-/Sicherheitsteam nur wenige Mitarbeiter umfasst, können diese nicht regelmäßig aus dem Alltagsbetrieb herausgenommen werden und ihre Zeit für Weiterbildungen aufwenden. Und mit weniger Kollegen haben Mitarbeiter auch weniger Möglichkeiten, gegenseitig voneinander zu lernen.

Fehlende Kapazitäten

Angreifer folgen keinem geregelten Arbeitsalltag, sodass Cyberschutz rund um die Uhr vorhanden sein muss. Tatsächlich beginnen 91 % der Ransomware-Angriffe außerhalb der normalen Geschäftszeiten, da Angreifer die Abwehr unerkannt überlisten möchten[1].

Laut Experten sind mindestens vier oder fünf Vollzeitmitarbeiter erforderlich, um 24/7 für Cybersecurity zu sorgen und Urlaub, Krankheitstage und Wochenenden abzudecken. In den meisten KMUs kann dies durch interne Mitarbeiter allein einfach nicht geleistet werden.

Aus der Umfrage geht auch hervor, dass **in KMUs während eines Drittels der Zeit (33 %) niemand Warnungen aktiv überwacht, analysiert oder darauf reagiert.** Ohne Mitarbeiter, die aktiv auf Bedrohungen reagieren, sind kleinere Unternehmen und Organisationen Angriffen weitestgehend schutzlos ausgesetzt.

33 %
der Zeit ist in KMUs niemand da, der Sicherheitswarnungen überwacht und auf sie reagiert

Wie viel Zeit (in Prozent) hat ein Mitarbeiter in Ihrem Unternehmen im letzten Jahr (nachts, an Wochenenden und Feiertagen) aktiv für die Überwachung und Analyse von Sicherheitswarnungen aufgewandt? Anzahl der Antworten: 1.402 Unternehmen mit 100–500 Mitarbeitern

1 So stoppen Sie aktive Angreifer: Neueste Erkenntnisse aus der Cybersecurity-Praxis – Sophos

Auswirkungen des Fachkräftemangels auf kleine Unternehmen

Das fehlende Fachwissen hat vielerlei Auswirkungen auf KMUs. In diesem Segment ist es am wahrscheinlichsten, dass Daten im Rahmen eines Ransomware-Angriffs verschlüsselt werden – in 74 % der Vorfälle kommt es zu einer Datenverschlüsselung. Dies ist liegt mit großer Wahrscheinlichkeit daran, dass es KMUs schlechter gelingt, Angreifer zu erkennen und zu stoppen, bevor Ransomware Schaden anrichten kann.

Ransomware-Angriffe, bei denen es zu einer Datenverschlüsselung kam

KMUs (Anzahl der Antworten: 1.402)	GRÖSSERE UNTERNEHMEN (Anzahl der Antworten: 3.598)	
100–500 MITARBEITER	501–1.000 MITARBEITER	1.001–5.000 MITARBEITER
74 %	72 %	66 %

Quelle: Ransomware-Report 2024, Sophos. Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Ja.

Da die Cybersecurity-Aufgaben unter weniger Mitarbeitern aufgeteilt werden, ist zudem das Burnout-Risiko hoch. In separaten, von Sophos beauftragten Studien **gaben 85 % der Unternehmen an, dass ihre Cybersecurity- und IT-Experten sich müde und erschöpft fühlen**, wobei beinahe ein Viertel (23 %) „häufig" und 62 % „gelegentlich" davon betroffen ist. Ebenfalls beunruhigend: 90 % der Unternehmen geben an, dass Fälle von Burnout und Erschöpfung in den letzten 12 Monaten angestiegen sind. 30 % berichten sogar, dass diese Fälle „deutlich" angestiegen sind.

85 %
melden Erschöpfung und Burnout unter ihren Cybersecurity- oder IT-Experten

Lösungen für das fehlende Fachwissen

Die meisten KMUs können nicht einfach mehr Mitarbeiter einstellen. Die Einstellung zusätzlicher Cybersecurity-Experten bedeutet beträchtliche Mehrausgaben, was sich in kleineren Unternehmen sehr viel stärker auf das Personalbudget auswirkt als in größeren. Gleichzeitig konkurrieren Unternehmen und Organisationen um die wenigen Fachkräfte mit den erforderlichen Qualifikationen. Experten mit den gefragtesten Kompetenzen haben die freie Wahl. Sie ziehen häufig eine Stelle in größeren Unternehmen vor, da sie dort bessere Entwicklungschancen sehen.

Eine Möglichkeit, den Mangel an Fachpersonal und Kapazitäten abzufedern, ist die Zusammenarbeit mit externen Sicherheitsexperten. Außerdem empfiehlt sich der Einsatz von Cybersecurity-Lösungen, die speziell für KMUs entwickelt wurden.

Externe Sicherheitsexperten

Das Zurückgreifen auf externe Cybersecurity-Experten ist oft die einfachste und kosteneffizienteste Methode, das fehlende Fachwissen zu kompensieren. Dabei wird am häufigsten auf Managed Detection and Response (MDR) Services und Managed Service Provider (MSP) gesetzt.

Bei **MDR-Services** übernimmt ein Expertenteam rund um die Uhr die Aufgaben Threat Hunting, Detection und Response. Spezialisierte Analysten halten 24/7 proaktiv Ausschau nach Bedrohungen, reagieren auf verdächtige Aktivitäten und beseitigen Angriffe, bevor Schaden für Ihr Unternehmen entsteht.

Wählen Sie einen Anbieter, der sich an Ihre Anforderungen und Ihre gewünschte Arbeitsweise anpasst: Vielleicht möchten Sie die Bedrohungserkennung und -reaktion komplett auslagern, oder aber mit den Analysten Ihres Anbieters. zusammenarbeiten. Da Budgets in der Regel knapp sind, sollten Sie sich für einen Service entscheiden, der Ihre vorhandenen Sicherheitstechnologien nutzen kann – so vermeiden Sie die zusätzlichen Kosten und Unterbrechungen, die bei einem Komplettaustausch anfallen würden.

Um Budget für einen MDR-Service freizusetzen, können Sie versuchen, günstigere Tarife bei Ihrem Cyberversicherungsanbieter zu erzielen. Kunden, die MDR-Services nutzen, erhalten bei Versicherungsanbietern oft deutlich günstigere Konditionen, da bei ihnen das Risiko geringer ist, dass sie Ansprüche geltend machen. Diese Einsparungen können dann für die Finanzierung des MDR-Service verwendet werden.

Managed Service Provider (MSPs) bieten seit vielen Jahren IT- und Cybersecurity-Support für kleine Unternehmen und agieren als ihr internes Team. Da Cyberbedrohungen stetig komplexer werden, entscheiden sich mittlere Unternehmen und Organisationen immer häufiger für die Zusammenarbeit mit MSPs, die dann die Arbeit ihrer internen Mitarbeiter ergänzen.

MDR-Services und MSPs schließen einander nicht aus. Eine separate Sophos-Studie ergab, dass die meisten MSPs (81 %) MDR-Services anbieten,[2] sodass Sie beide Support-Ebenen von einem einzigen Anbieter erhalten können. Einige MSPs bieten MDR-Services ausschließlich aus dem eigenen Unternehmen an, während andere spezialisierte MDR-Drittanbieter einsetzen.

Lösungen, die speziell auf KMUs zugeschnitten sind

Die meisten Cybersecurity-Lösungen wurden für größere Unternehmen und Organisationen mit großen Teams entwickelt, die diese Lösungen dann bereitstellen und verwalten. Es mag im ersten Moment zwar nach einer guten Idee klingen, umfassende Unternehmenslösungen einzusetzen. Allerdings bemerken kleinere Unternehmen dabei oft keine Vorteile in puncto Sicherheit und Rendite, da sie diese Lösungen nicht optimal nutzen können. Sehen Sie sich stattdessen nach Sicherheitstools um, die zwar technisch fortgeschritten sind, aber so konzipiert wurden, dass überlastete IT-Teams sie in der Praxis einfach nutzen können.

Durch den Einsatz neuer Lösungen sollten Ihre Ausgaben nicht steigen. Im Gegenteil: Die Tools sollten Ihnen ermöglichen, Ihre Technologie- und Verwaltungsausgaben zu reduzieren. Prüfen Sie bei der Suche nach der richtigen Sicherheitslösung sowohl die Plattform als auch die Produktfunktionen.

Plattform

- Mit einer Cybersecurity-Plattform können Sie mehrere Cybersecurity-Lösungen zentral bereitstellen, im Blick behalten und verwalten, z. B. Ihre Endpoint-/Antivirus-, E-Mail-Sicherheits- und Firewall-Lösungen.
- Wenn Sie Ihre Cybersecurity-Lösungen in einer zentralen Plattform konsolidieren, reduziert sich der tägliche Verwaltungsaufwand deutlich, denn Sie müssen nicht mehr von Konsole zu Konsole springen. Und wenn Sie mit weniger Anbietern arbeiten, verringern Sie die Kosten für das Anbietermanagement.
- In einer leistungsstarken Plattform können Ihre Sicherheitslösungen auch zusammenarbeiten und Telemetriedaten, Erkenntnisse, nutzerbasierte Richtlinien etc. gemeinsam nutzen, um Ihre Cyberabwehr zu stärken.

Produktfunktionen

- Anbieter präsentieren auf ihren Websites oft lange Listen mit Funktionen. Nehmen Sie sich vor der Auswahl von Lösungen ausreichend Zeit, um genau zu ermitteln, was Sie benötigen und was nicht. So vermeiden Sie, für Lösungen zu zahlen, die Ihnen keinen Mehrwert bieten.
- Um das volle Potenzial Ihrer Cybersecurity-Lösungen auszuschöpfen, müssen Sie sie effektiv bereitstellen und nutzen können. Entscheiden Sie sich für Lösungen, die von Anfang an empfohlene Einstellungen automatisch bereitstellen. So entfallen zeitaufwendige und riskante manuelle Konfigurationen. Achten Sie außerdem auf intuitive und benutzerfreundliche Bedienelemente, die den Praxistest bestehen.
- Falsch konfigurierte Sicherheitstools sind eines der Hauptrisiken in KMUs. Deswegen ist ein guter Sicherheitsstatus das A und O für den laufenden Betrieb. Wählen Sie daher Lösungen, bei denen sich eine suboptimale Bereitstellung einfach erkennen lässt und die Support zur schnellen Lösung von Problemen bieten.
- Wenn Sie ein kleineres Unternehmen sind, kann sich Ihr Team vermutlich nicht ausschließlich mit dem Thema Cybersecurity befassen. Genau deshalb ist es so wichtig, Lösungen zu wählen, die automatisch auf Bedrohungen reagieren und entsprechende Maßnahmen ergreifen, bis Sie einschreiten können.

2 Perspektiven für MSPs 2024 – Sophos

So kann Sophos helfen

Sophos bietet umfassende Expertise beim Schutz kleiner und mittlerer Unternehmen vor komplexen Cyberbedrohungen. Viele unserer Produkte und Services sind speziell auf ihre Anforderungen ausgerichtet.

Externe Sicherheitsexperten

MDR-Service

Sophos schützt mit seinem vielfach ausgezeichneten MDR-Service mehr kleine Unternehmen als jeder andere Anbieter. Wir verfügen über umfassende Kenntnisse zu Angriffen auf kleine Unternehmen und nutzen Telemetriedaten aus unserer gesamten Kundenbasis, um den Schutz für alle Nutzer zu optimieren.

Der Sophos MDR-Service erhält regelmäßig erstklassige Bewertungen von Kunden und Analysten. Zu den aktuellen Auszeichnungen zählen:

- zwei Jahre in Folge „Customers' Choice" von Gartner® Peer Insights™, mit einer Bewertung von 4,8/5 auf Basis von 647 Bewertungen (Stand 17. September 2024)
- G2 Leader für MDR, mit u. a. der vom Mittelstand am besten bewerteten MDR-Lösung
- IDC MarketScape zeichnete Sophos im Vendor Assessment 2024 als Leader in der Kategorie „Worldwide Managed Detection and Response Services" aus

„Wenn Organisationen einen MDR-Anbieter mit fundierter Sicherheitsexpertise und einem von Experten bereitgestellten Service suchen, der sie von Anfang an bis zur Behebung eines Vorfalls begleitet, ist Sophos eine überzeugende Option."
- Richard Thurston, Research Manager, European Security Services, IDC

MSP-Partner

Sophos hat ein großes und schnell wachsendes MSP-Partnernetz, das Produkte und Services von Sophos – u. a. Sophos MDR – für KMUs auf der ganzen Welt bereitstellt.

Lösungen speziell für KMUs

Plattform

Sophos Central ist die branchenweit größte cloudnative Plattform. Sie ist KI-gestützt und lässt sich optimal skalieren. Sophos Central verwaltet alle Next-Gen-Cybersecurity-Lösungen von Sophos, u. a. Sophos Endpoint, Sophos Firewall, Sophos XDR, Sophos MDR, Sophos Email und Sophos ZTNA. Da sie in viele unterschiedliche Technologien anderer Anbieter (z. B. Microsoft und Google) integriert werden kann, können Kunden auch weiterhin alle Vorteile ihrer bestehenden Sicherheitssysteme nutzen.

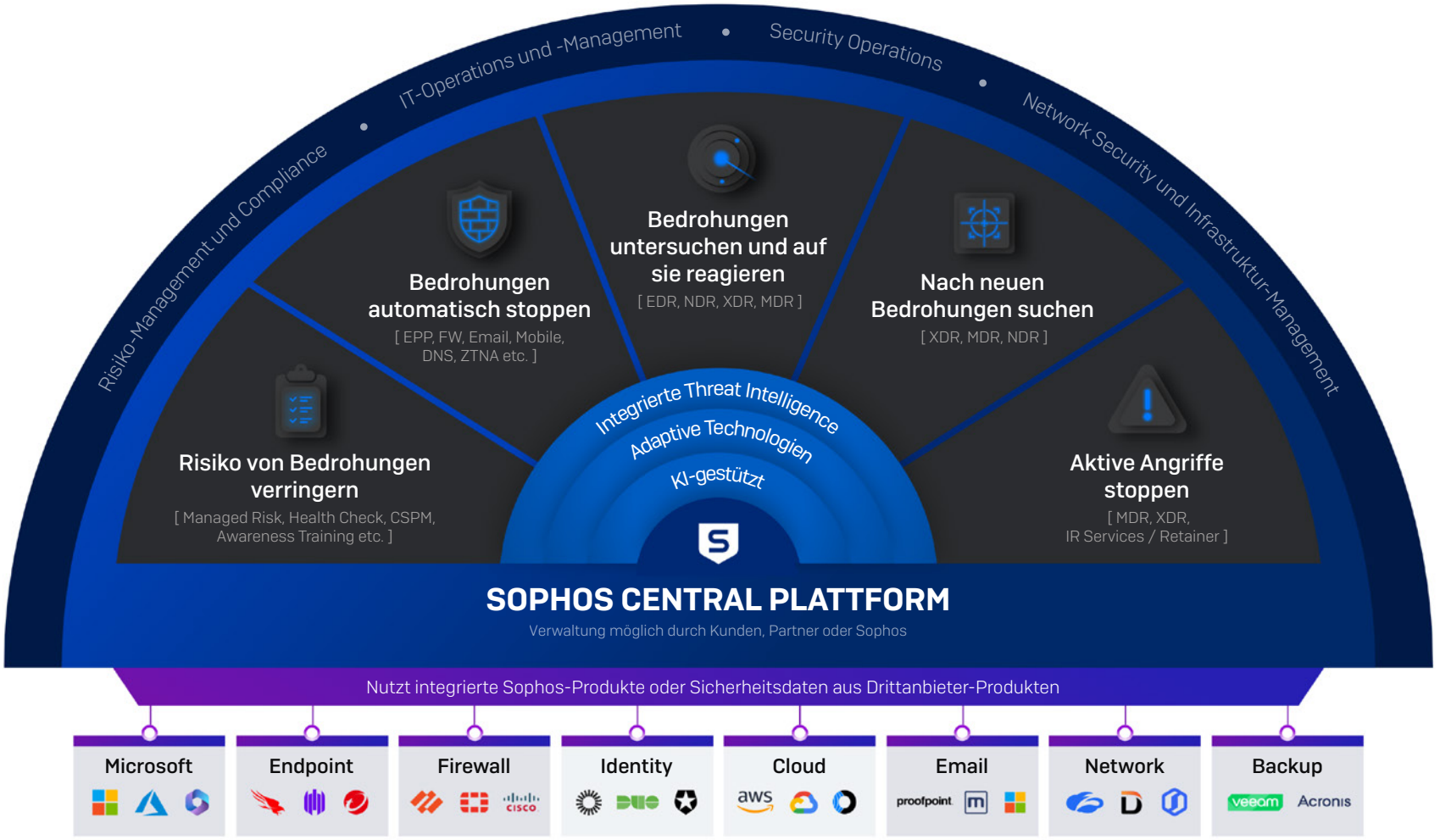
Produktfunktionen

Sophos bietet modernste Lösungen, die auf unserer jahrzehntelangen Erfahrung im Bereich Cybersicherheit basieren. Unsere Lösungen sind benutzerfreundlich gestaltet, damit Unternehmen und Organisationen unabhängig von Größe und Ressourcen sie optimal nutzen können.

Beispiele:

- **Sophos Endpoint** wird automatisch mit empfohlenen Einstellungen bereitgestellt, u. a. mit unserem marktführenden Ransomware-Schutz und Anti-Exploit-Funktionen – manuelle Anpassungen entfallen.
- Über das zentrale Management und Reporting der **Sophos Firewall** können Sie mehrere Firewalls zentral verwalten, was sich insbesondere für Unternehmen mit verteilten Standorten eignet.
- **Sophos Endpoint** umfasst eine adaptive Abwehr, die Angreifer in Ihrer Umgebung erkennt und automatisch abwehrt. So sind Sie besser geschützt und können sich Zeit verschaffen, um auf Angriffe zu reagieren.
- Der integrierte Sicherheits-Check in **Sophos Endpoint** bietet eine klare Echtzeit-Übersicht zum Sicherheitsstatus und umfasst zusätzlich die Schaltfläche „Automatisch beheben", mit der Sie mit nur einem Klick zu den empfohlenen Einstellungen zurückkehren.
- Die Integration der **Sophos Firewall** in die erweiterte Sophos-Plattform sorgt dafür, dass aktive Bedrohungen automatisch blockiert werden und eine Reaktion über alle Endpoints, ZTNA sowie Switches und Wireless Access Points koordiniert wird. Dadurch werden laterale Bewegungen verhindert.

Die Cybersecurity-Plattform von Sophos



Fazit

Die Umfrage zeigt, dass der Fachkräftemangel im Bereich Cybersecurity schwer auf kleinen und mittleren Unternehmen lastet. Die mangelnde Expertise sowie fehlende Kapazitäten haben gravierende Auswirkungen darauf, ob sich Unternehmen erfolgreich gegen Angriffe schützen können.

Da in puncto Fachkräftemangel noch kein Ende in Sicht ist, sollten kleinere Unternehmen und Organisationen mit den passenden Maßnahmen für effektiven Cyberschutz sorgen. Hier bietet sich die Zusammenarbeit mit externen Experten an sowie der Einsatz von Lösungen, die speziell für ihre Unternehmensgröße und -Anforderungen entwickelt wurden.

Weitere Informationen zu Lösungen von Sophos für kleine und mittlere Unternehmen erhalten Sie bei Ihrem Sophos-Ansprechpartner oder auf sophos.de.

2024-10-08 EN-WP (PC)

SOPHOS