SOPHOS

Perspektiven für MSPs 2024

350 MSPs liefern Einblicke in Cybersecurity-Tools, Risiken, Herausforderungen und Geschäftschancen.

Sophos-Whitepaper, Mai 2024

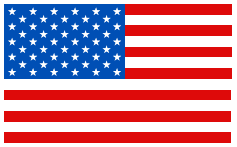
Einführung

Der Report **Perspektiven für MSPs 2024** konzentriert sich auf fünf zentrale Bereiche des MSP-Geschäfts:

- RMM- und PSA-Tools
- Cybersecurity-Management
- MDR Services
- Herausforderungen und Risiken für MSPs und ihre Kunden
- Auswirkungen von Cyberversicherungen

Die Ergebnisse basieren auf einer unabhängigen Befragung von 350 MSPs in den USA (200), Großbritannien (50), Deutschland (50) und Australien (50). Die Umfrage wurde von Sophos in Auftrag gegeben und vom Marktforschungsunternehmen Vanson Bourne im März 2024 durchgeführt.

350 MSPs
aus vier Ländern



USA
200 Befragte

UK
50 Befragte

Deutschland
50 Befragte

Australien
50 Befragte

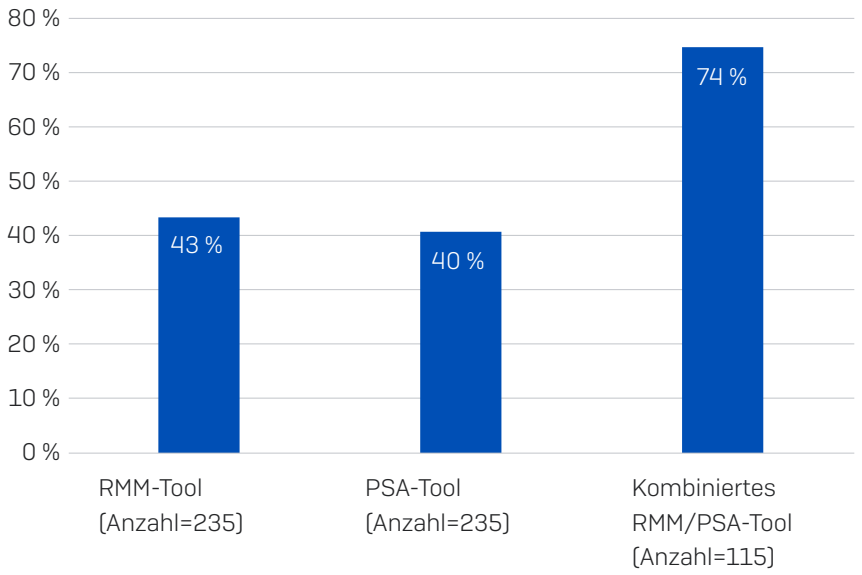
RMM- und PSA-Tools

Lösungen für Remote Monitoring and Management (RMM) und Professional Services Automation (PSA) ermöglichen eine effiziente und effektive Bereitstellung von MSP-Services. Zudem können MSPs mit diesen Tools ihre Betriebskosten reduzieren. Die Umfrage lieferte zwei interessante Erkenntnisse zu diesen wichtigen MSP-Technologien.

MSPs sind wesentlich zufriedener mit kombinierten RMM/PSA-Tools als mit eigenständigen Tools

Fast drei Viertel (74 %) der MSPs, die ein kombiniertes RMM/PSA-Tool nutzen, sind mit ihrer Lösung „sehr zufrieden", verglichen mit nur 43 % der MSPs mit eigenständigen RMM-Tools und 40 % mit eigenständigen PSA-Tools.

Befragte, die mit ihren vorhandenen RMM- und PSA-Tools „sehr zufrieden" sind

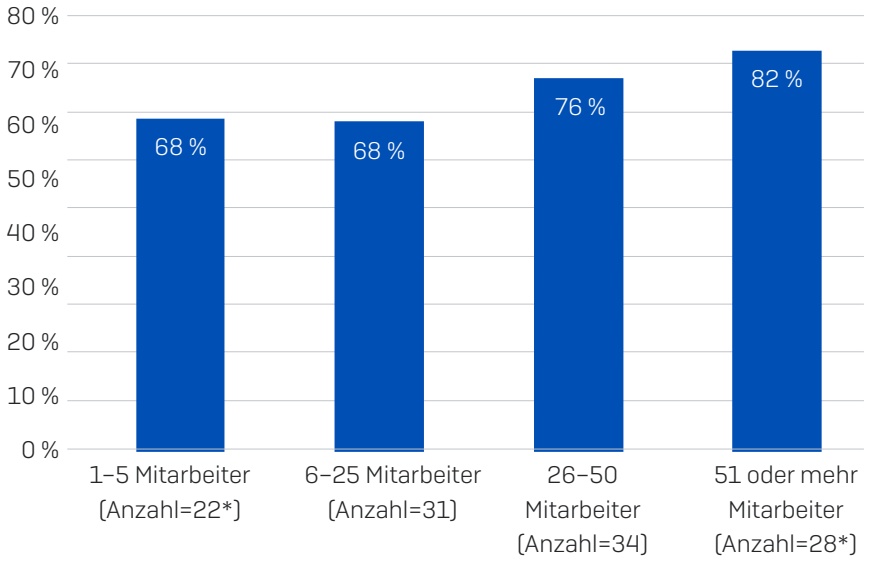


Wie zufrieden ist Ihr Unternehmen mit den vorhandenen RMM- und PSA-Tools? Anzahl der erhaltenen Antworten jeweils in Klammer

Zufriedenheit mit kombinierten RMM/PSA-Tools steigt mit der Unternehmensgröße des MSPs

Etwas mehr als zwei Drittel (68 %) der MSPs mit bis zu 25 Mitarbeitern sind mit ihrer kombinierten RMM/PSA-Lösung sehr zufrieden. Bei den MSPs mit 26–50 Mitarbeitern sind es 76 % und bei MSPs mit 51 oder mehr Mitarbeitern 82 %. Da größere MSPs wahrscheinlich auch mehr Kunden betreuen, lassen die Zahlen darauf schließen, dass der Nutzen von kombinierten RMM/PSA-Tools proportional zur Kundenanzahl steigt.

Befragte, die mit ihrem kombinierten RMM- und PSA-Tool „sehr zufrieden" sind



Wie zufrieden ist Ihr Unternehmen mit den vorhandenen RMM- und PSA-Tools? Anzahl der erhaltenen Antworten jeweils in Klammer.
* Aufgrund der geringen Anzahl der Befragten in diesem Segment sollten die Ergebnisse als Richtwerte und nicht als statistisch signifikant verstanden werden.

Empfehlung: Für MSPs, die eigenständige RMM/PSA-Tools verwenden, kann es sinnvoll sein, zu einer kombinierten RMM/PSA-Lösung zu wechseln, um die Zufriedenheit zu erhöhen – insbesondere wenn sie ihren Kundenstamm erweitern möchten.

Cybersecurity-Management

Partnerschaften mit Cybersecurity-Anbietern

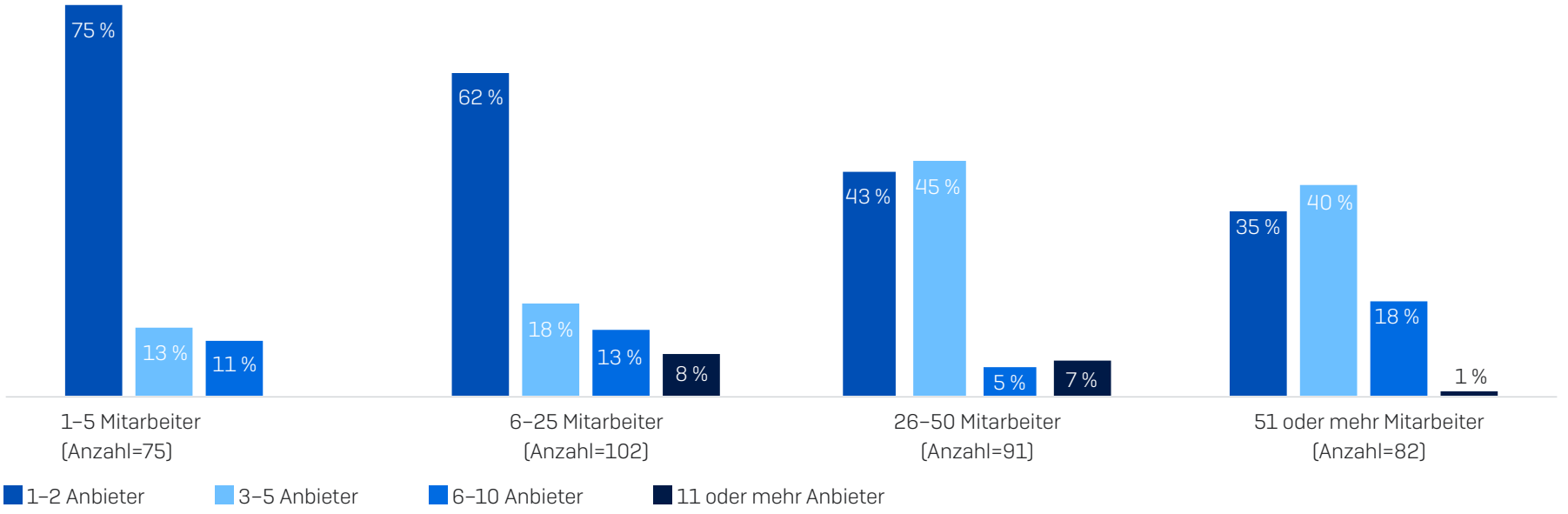
Cybersecurity zählt zum Kernangebot der meisten MSPs. Aus der Umfrage geht hervor, dass MSPs in der Regel mit einer kleinen Anzahl an Cybersecurity-Anbietern zusammenarbeiten, um ihre Kunden zu schützen:

- 53 % nutzen einen oder zwei Cybersecurity-Anbieter
- 83 % arbeiten mit einem bis fünf Cybersecurity-Anbietern zusammen
- 4 % verwenden elf oder mehr Cybersecurity-Anbieter

Die Daten zeigen auch, dass die Anzahl der Cybersecurity-Anbieter im Allgemeinen mit der Größe des MSP-Unternehmens steigt. 75 % der kleinsten MSPs (1–5 Mitarbeiter) arbeiten mit einem oder zwei Cybersecurity-Anbietern zusammen. Bei MSPs mit 51 oder mehr Mitarbeitern liegt der prozentuale Anteil lediglich bei 35 %.

Umgekehrt nutzen die größten MSPs fast doppelt so häufig sechs oder mehr Cybersecurity-Anbieter wie die kleinsten (20 %, gerundet, ggü. 11 %). Zwar lässt sich das Service-Portfolio durch die Zusammenarbeit mit mehr Cybersecurity-Anbietern erweitern, doch geht dies in der Regel mit höheren Kosten für das Anbieter-Management und Herausforderungen bei der Integration unterschiedlicher Technologien einher.

Anzahl der Cybersecurity-Anbieter zum Schutz von MSP-Kunden



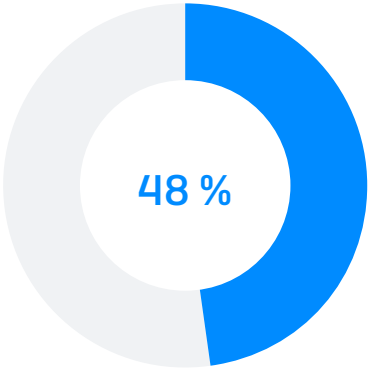
Wie viele Cybersecurity-Anbieter nutzt Ihr Unternehmen derzeit zum Schutz seiner Kunden? Anzahl=350. Anzahl der erhaltenen Antworten jeweils in Klammer. Ohne „Weiß nicht"-Angaben.

Cybersecurity-Plattform-Konsolidierung

Die Umfrage zeigt: Durch die Konsolidierung von Cybersecurity-Plattformen können MSPs wesentlich effizienter arbeiten und ihre Kosten gleichzeitig senken.

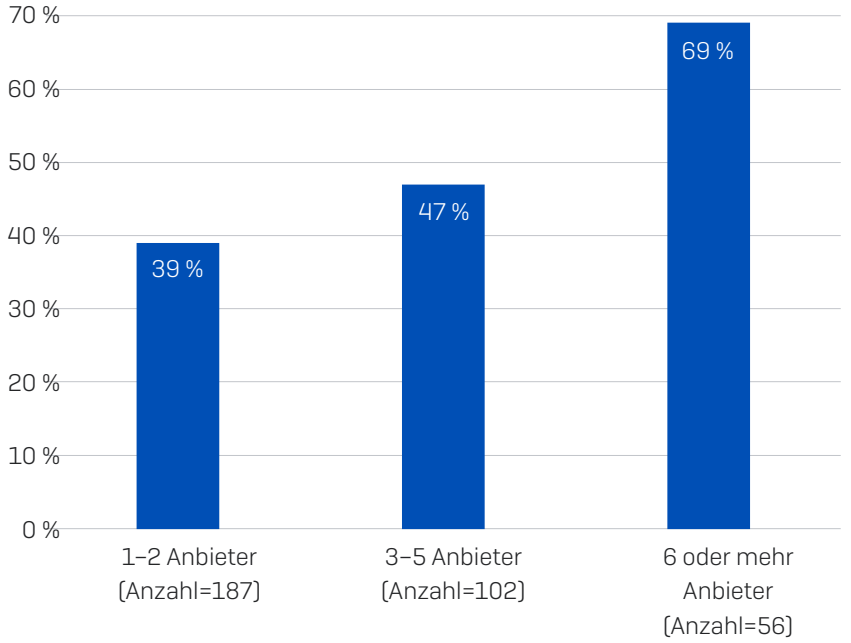
MSPs, die derzeit mehrere Plattformen nutzen, schätzen, dass sie im Durchschnitt 48 % ihrer täglichen Verwaltungszeit einsparen würden, wenn sie alle ihre Cybersecurity-Tools über eine einzige Plattform verwalten könnten.

Geschätzte Zeitersparnis bei der täglichen Verwaltung durch Konsolidierung auf einer einzigen Cybersecurity-Plattform



Die potenzielle Zeitersparnis bei der Verwaltung steigt mit der Anzahl der aktuell genutzten Cybersecurity-Anbieter. MSPs, die mit sechs oder mehr Cybersecurity-Anbietern arbeiten, gehen davon aus, dass sie ihre tägliche Verwaltungszeit um mehr als zwei Drittel (69 %) reduzieren würden, wenn sie alle Cybersecurity-Tools über eine einzige Plattform verwalten könnten. Eine Reduzierung des Verwaltungsaufwands in dieser Größenordnung kann sich erheblich auf die Profitabilität auswirken und gleichzeitig Kapazitäten für umsatzgenerierende Aktivitäten freisetzen.

Durchschnittliche geschätzte Zeitersparnis bei der täglichen Verwaltung durch die Konsolidierung auf einer einzigen Cybersecurity-Plattform – aufgeschlüsselt nach der Anzahl der verwendeten Anbieter



Wie viel Zeit könnte Ihr Unternehmen Ihrer Meinung nach bei der täglichen Verwaltung einsparen, wenn es alle seine Cybersecurity-Tools über eine einzige Plattform verwalten könnte? Anzahl der erhaltenen Antworten jeweils in Klammer.

Empfehlung: MSPs, die mehrere Cybersecurity-Plattformen nutzen, sollten Konsolidierungsoptionen und Einsparungen bei den Gesamtbetriebskosten prüfen, die sie durch die Verwaltung all ihrer Cybersicherheits-Tools über eine einzige Plattform erzielen könnten.

MDR Services

Akzeptanz von MDR Services

Die Nachfrage nach Managed Detection and Response Services (MDR) wächst schnell, da sowohl Cyberbedrohungen als auch die Tools zu ihrer Abwehr immer komplexer werden. Aktuellen Daten von Gartner zufolge beläuft sich der Gesamtmarktwert auf 7,5 Milliarden US-Dollar und die durchschnittliche jährliche Wachstumsrate auf 25,8 %.

Vor diesem Hintergrund ist es nicht verwunderlich, dass die Mehrheit (81 %) der MSPs bereits zu einem gewissen Grad MDR Services anbietet und die meisten anderen planen, ihr Angebot kurz- und mittelfristig um MDR zu erweitern. Die Umfrage ergab jedoch erhebliche Unterschiede beim Reifegrad von MDR-Services in den vier beteiligten Ländern.

Das Gros der MSPs in den USA (94 %) hat bereits einen MDR Service im Angebot, gefolgt von Deutschland (70 %), Großbritannien (62 %) und Australien (58 %). Weltweit planen fast alle MSPs, die derzeit keine MDR Services anbieten, diese in den kommenden Jahren in ihr Portfolio aufzunehmen. Fast ein Drittel (32 %) der britischen MSPs möchte MDR noch im Jahr 2024 einführen.

				
Bieten derzeit MDR Services an	**94 %**	**62 %**	**70 %**	**58 %**
Planen MDR im Jahr 2024 anzubieten	5 %	32 %	20 %	18 %
Planen, MDR im Jahr 2025 oder später einzuführen	2 %	6 %	10 %	22 %

Bietet Ihr Unternehmen seinen Kunden derzeit einen Managed Detection and Response (MDR) Service an? Anzahl=350 (USA 200, Großbritannien 50, Deutschland 50, Australien 50). Einige Antwortmöglichkeiten wurden übersprungen.

Angebot von MDR Services

Es gibt drei Hauptmodelle für die Bereitstellung von MDR Services durch MSPs: über das eigene Security Operations Center (SOC), über einen Drittanbieter und gemeinsam durch das SOC des MSPs und den Drittanbieter.

Wie aus der Umfrage hervorgeht, nutzen 66 % einen Drittanbieter für die Bereitstellung ihrer MDR Services, 20 % ihr eigenes SOC und 15 % einen Drittanbieter in Verbindung mit ihrem eigenen SOC. Insgesamt arbeiten 80 % (gerundet) der MSPs bei der Bereitstellung ihres MDR Services mit einem Drittanbieter zusammen.

34 % (gerundet) der MSPs verfügen über ein internes SOC, das MDR Services anbietet – entweder eigenständig oder gemeinsam mit einem Drittanbieter. Die interne Bereitstellung bewegt sich über alle Unternehmensgrößen hinweg im gleichen Bereich: Lediglich vier Prozentpunkte liegen zwischen dem Segment mit 26–50 Mitarbeitern, die am ehesten über ein internes SOC verfügen (37 %), und allen anderen Gruppen (33 %).

Bereitstellung von MDR Services

Eigenes SOC des MSPs	MDR Services von Drittanbietern	Eigenes SOC des MSPs und MDR Services von Drittanbietern
20 %	66 %	15 %

Bietet Ihr Unternehmen derzeit einen Managed Detection and Response Service (MDR) für seine Kunden an? Anzahl=282, die einen MDR Service anbieten. Einige Antwortmöglichkeiten wurden übersprungen.

Erforderliche Kernkompetenzen von MDR-Anbietern

Wie wir bereits gesehen haben, nutzen vier von fünf MSPs Drittanbieter für die Bereitstellung ihrer MDR Services. Angesichts der beträchtlichen und wachsenden Nachfrage nach MDR Services spielt die Auswahl des richtigen Anbieters eine entscheidende Rolle für MSPs und ihre Kunden.

MDR-Anbieter fungieren als verlängerter Arm des MSPs. Die Servicequalität und Kompetenz des Anbieters wirken sich also direkt auf den MSP aus. Außerdem beeinflusst das Leistungsspektrum des MDR-Anbieters nicht nur die Service-Palette, die der MSP seinen Kunden anbieten kann, sondern auch den Arbeitsaufwand und Grad der Beteiligung des MSPs.

24/7 Incident Response Services stehen ganz oben auf der Liste der Kernkompetenzen eines MDR-Anbieters. 36 % stufen diese als „wesentlich" ein, bei MSPs mit 1–5 Mitarbeitern sind es sogar 49 %. Da 91 % der Ransomware-Angriffe außerhalb der üblichen Geschäftszeiten erfolgen,[1] ist eine 24/7-Abdeckung für den effektiven Schutz eines Unternehmens unerlässlich. Die Zusammenarbeit mit einem MDR-Anbieter, der 24/7-Betreuung durch ein Expertenteam bietet, gibt MSPs die Gewissheit, dass ihre Kunden immer geschützt sind, ohne dass sie das gleiche Know-how intern aufbauen müssen.

An zweiter Stelle steht *die Erkennung von Übernahmeversuchen von E-Mail-Konten in Microsoft 365 und/oder Google Workspace.* Ein Drittel (33 %) der MSPs hält dies für eine „wesentliche" Voraussetzung und 43 % für „sehr wichtig".

Die *Option, zusätzliche Sicherheitstools – insbesondere Firewalls/Netzwerksicherheit und Endpoint Protection – vom MDR-Anbieter zu beziehen*, wird ebenfalls stark nachgefragt: Drei Viertel der Befragten stufen dies als „wesentlich oder sehr wichtig" ein. Die Option, Cybersecurity-Tools und MDR Services bei einem einzigen Anbieter zu beziehen, reduziert den Verwaltungsaufwand und optimiert Betriebsabläufe.

Gleichzeitig zeigt die Umfrage ganz klar, dass MSPs Wert auf Flexibilität legen. MSPs möchten weder bei der Auswahl der Tools eingeschränkt werden, noch verpflichtet sein, Cybersecurity-Tools bei ihrem MDR-Anbieter zu erwerben. 71 % stufen es als „wesentlich oder sehr wichtig" ein, dass der Anbieter *Telemetriedaten von bestehenden Security-Tools für die Erkennung und Abwehr von Bedrohungen nutzen kann.*

Das Angebot von 24/7 Incident Response ist die wichtigste Kompetenz von MDR-Anbietern

FUNKTION	„WESENTLICH"	„WESENTLICH" ODER „SEHR WICHTIG"
24/7 Incident Response Service	36 %	74 %
Erkennung von Übernahmeversuchen von E-Mail-Konten in **Microsoft 365 und/oder Google Workspace**	33 %	77 %
Möglichkeit, **Firewall-/ Netzwerksicherheit** vom MDR-Anbieter zu beziehen	31 %	74 %
Möglichkeit, **Endpoint Protection** vom MDR-Anbieter zu beziehen	28 %	75 %
Eine zentrale Konsole für MDR- und andere Sicherheitslösungen	28 %	74 %
Breach **Warranty**	26 %	70 %
Option zur Nutzung von Telemetriedaten **vorhandener Sicherheits-Tools** für die Bedrohungserkennung und -reaktion	25 %	71 %

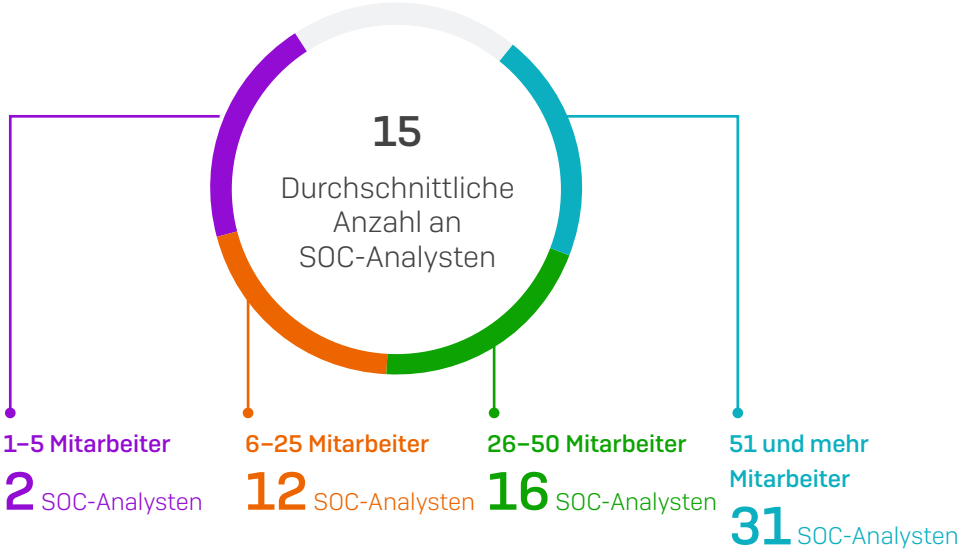
Wie wichtig sind für Ihr Unternehmen folgende Kompetenzen/Funktionen bei der Auswahl eines MDR-Anbieters? Anzahl=350 (USA 200, Großbritannien 50, Deutschland 50, Australien 50). Einige Antwortmöglichkeiten wurden übersprungen.

Interne SOC-Analysten

34 % der MSPs, die einen MDR Service anbieten, verfügen über ein internes SOC und benötigen daher spezialisierte Analysten. Der Umfrage zufolge umfassen SOCs von MSPs im Schnitt 15 Analysten. Hinter dieser Zahl verbergen sich jedoch erhebliche Unterschiede in Abhängigkeit von der Unternehmensgröße.

MSPs mit 1–5 Mitarbeitern beschäftigen durchschnittlich zwei Analysten, die Kundenumgebungen überwachen, Bedrohungen erkennen und darauf reagieren. Die Zahl der Analysten steigt mit der Größe des Unternehmens kontinuierlich an: Die größten MSPs umfassen im Schnitt 31 SOC-Analysten. Hinweis: Aufgrund der relativ geringen Anzahl der Befragten in den einzelnen Segmenten sollten die Ergebnisse als Richtwerte und nicht als statistisch signifikant verstanden werden.

Da Cyberkriminelle ihre Angriffe bewusst abends, an Wochenenden und an Feiertagen ausführen, ist eine 24/7-Abdeckung für einen effektiven MDR Service von entscheidender Bedeutung. Die interne Bereitstellung von MDR Services setzt kleinere MSPs mit weniger Analysten unter enormen Druck.



Wie viele Analysten, die verdächtige Ereignisse in den Umgebungen Ihrer Kunden überwachen und darauf reagieren, beschäftigen Sie im SOC Ihres Unternehmens?

Empfehlung: MSPs, die derzeit keine MDR Services anbieten, sollten diese möglichst zeitnah in ihr Portfolio aufnehmen, um nicht ins Hintertreffen zu geraten. Bei der Auswahl eines Drittanbieters für MDR Services sollten Sie die für Sie wichtigen Kompetenzen und Funktionen ermitteln und das Leistungsangebot potenzieller Anbieter danach bewerten.

Herausforderungen und Cyberrisiken

Die aktuell größten Herausforderungen für MSPs

Die MSP-Welt steht nicht still. Da sich Bedrohungen kontinuierlich weiterentwickeln, ändern sich auch Cybersecurity-Lösungen und Kundenanforderungen.

Der Umfrage zufolge besteht die größte Herausforderung für MSPs darin, ***mit den neuesten Cybersecurity-Lösungen/-Technologien Schritt zu halten*** – Platz 1 sowohl in der Kategorie „größte Herausforderung insgesamt" als auch bei den Top-3-Herausforderungen.

Angesichts der hohen Innovationsgeschwindigkeit in diesem Bereich überrascht es kaum, dass viele MSPs Mühe haben, mitzuhalten. Da Bedrohungen immer komplexer werden, entwickeln sich auch die entsprechenden Schutztechnologien beständig weiter. Der Funktionsumfang vorhandener Lösungen wird regelmäßig erweitert und es kommen immer wieder völlig neue Produkte auf den Markt. Mit diesen Entwicklungen Schritt zu halten, ist schwierig und zeitaufwändig.

Die zweitgrößte Herausforderung für MSPs ist die Anwerbung und Bindung von Cybersecurity-Analysten:

- ***Die Service-Abdeckung außerhalb der Geschäftszeiten (einschließlich abends und an Wochenenden)*** stufen MSPs als zweitgrößte Herausforderung insgesamt ein
- ***Die Anwerbung neuer Cybersecurity-Analysten, um mit dem Wachstum Schritt zu halten***, steht auf Platz 2 der Liste der Top-3-Herausforderungen

Spezialisierte Cybersecurity-Analysten sind Mangelware und werden hoch bezahlt. Erschwerend kommt hinzu, dass eine lückenlose 24/7-Abdeckung mindestens 5–6 Analysten erfordert – viele MSPs stoßen hier an ihre Grenzen.

Größte Herausforderung insgesamt

Nr. 1	Schritthalten mit den neuesten Cybersecurity-Lösungen/-Technologien
Nr. 2	Abdeckung außerhalb der Geschäftszeiten (abends, an Wochenenden und Feiertagen)
Nr. 3	Neukundengewinnung

Top-3-Herausforderungen

Nr. 1	Schritthalten mit den neuesten Cybersecurity-Lösungen/-Technologien
Nr. 2	Anwerbung von neuen Cybersecurity-Analysten bei Kundenwachstum
Nr. 3	Schritthalten mit aktuellen Cyberbedrohungen

Was sind die größten Herausforderungen, denen sich Ihr Unternehmen tagtäglich stellen muss? Geben Sie bitte Ihre Top 3 an. Anzahl=350

Cyberrisiken

Die Umfrage untersucht, welche Faktoren MSPs als größte Cyberrisiken einstufen – sowohl für ihr eigenes Unternehmen als auch für ihre Kunden. Dabei zeigen sich sowohl Gemeinsamkeiten als auch Unterschiede.

Zwei Punkte stehen bei MSPs und ihren Kunden ganz oben auf der Liste:

- Gestohlene Zugangsdaten und Anmeldeinformationen
- Kompetenzlücken/fehlendes Fachpersonal im Bereich Cybersecurity in Unternehmen

Angreifer brechen nicht in Unternehmen ein – sie loggen sich ein. Mit gestohlenen Zugangsdaten, die sie häufig im Dark Web bei einem Initial Access Broker (IAB) erworben haben, geben sie sich als legitime Mitarbeiter aus. So verschaffen sie sich Zugriff zu den Netzwerken ihrer Opfer. Wie aus unserem Ransomware-Report 2024 hervorgeht, gingen 29 % der Ransomware-Angriffe im vergangenen Jahr von kompromittierten Zugangsdaten aus – ein klarer Beleg für die Dimension des Problems.

Trotz ständiger Innovationen bei Cybersecurity-Technologien und künstlicher Intelligenz steht der Mensch nach wie vor im Mittelpunkt einer effektiven Cybersecurity. Qualifizierte Fachleute müssen Technologielösungen konfigurieren, bereitstellen, verwalten, nutzen und aktualisieren. Technologie-Lösungen allein können nicht alle Cyberbedrohungen automatisch stoppen. Der Mangel an qualifizierten Fachkräften ist bekannt. Unternehmen wenden sich zunehmend an MSPs, um die Lücken zu schließen, wodurch sich die Problematik verschärft.

Was die größten Risiken betrifft, sind sich MSPs und ihre Kunden einig. Lediglich bei der Bewertung zeigen sich Unterschiede.

Unsichere WLANs stufen MSPs als eines der größten Cyberrisiken ein (geteilter erster Platz in der Kategorie „größtes Einzelrisiko" und Platz 3 bei den „Top-3-Risiken"). Die Nutzung unsicherer Netzwerke birgt viele Gefahren, z. B. das Abfangen von Daten und das Auslesen von Zugangs- und Passwortinformationen, mit denen Cyberkriminelle auf private und geschäftliche Konten zugreifen können.

Auch die ***Fehlkonfiguration von Sicherheitstools*** zählen MSPs zu den Hauptrisiken. Firewalls, Endpoint-Schutz und andere Tools funktionieren nur, wenn sie richtig konfiguriert sind.

Ungepatchte Sicherheitslücken gelten als eines der größten Risiken für MSP-Kunden (Platz 2 in der Kategorie „größtes Einzelrisiko", Platz 3 der „Top-3-Risiken"). 32 % der Ransomware-Angriffe gingen im vergangenen Jahr von ausgenutzten ungepatchten Sicherheitslücken aus: Das Risiko darf also nicht unterschätzt werden.

MSPs

Größtes Einzelrisiko		Top-3-Risiken	
Nr. 1	Kompetenzlücken/fehlendes Fachpersonal im Bereich Cybersecurity in Unternehmen	Nr. 1	Gestohlene Zugangsdaten und Anmeldeinformationen
Nr. 1	Unsichere WLANs	Nr. 2	Fehlkonfiguration von Sicherheitstools
Nr. 3	Mangel an Cybersecurity-Tools	Nr. 3	Unsichere WLANs

MSP-Kunden

Größtes Einzelrisiko		Top-3-Risiken	
Nr. 1	Kompetenzlücken/fehlendes Fachpersonal im Bereich Cybersecurity in Unternehmen	Nr. 1	Gestohlene Zugangsdaten und Anmeldeinformationen
Nr. 2	Ungepatchte Sicherheitslücken	Nr. 2	Mangel an Cybersecurity-Tools
Nr. 3	Remote-Access-Tools	Nr. 3	Ungepatchte Sicherheitslücken

Wer oder was sind Ihrer Meinung nach die größten Cybersecurity-Risiken für Ihr Unternehmen/Ihre Kunden? Anzahl=350

Empfehlung: Um angesichts dieser komplexen Risiken und Herausforderungen den täglichen Verwaltungsaufwand zu minimieren, sollten MSPs nach Cybersecurity-Partnern suchen, die eine umfassende Palette an Services und Tools anbieten. Lösungen, die robusten, adaptiven Schutz vor neuen Bedrohungen bieten – ohne komplexe Konfigurationen und Bereitstellungen – machen es einfacher, Schritt zu halten. Darüber hinaus können MSPs ihre interne Cybersecurity-Kompetenz mit Hilfe eines MDR-Anbieters erweitern und ausbauen. Dabei sollten sich MSPs auf Partner konzentrieren, die ihr Geschäftsmodell unterstützen und sich an neue Anforderungen und Unternehmenswachstum anpassen können.

Auswirkungen von Cyberversicherungen

Immer mehr Unternehmen greifen zum Transfer von Cyberrisiken auf Cyberversicherungen zurück. Laut einer Studie von Sophos verfügen 90 % der mittelständischen Unternehmen inzwischen über Cyberversicherungs-Schutz. 50 % haben eine gesonderte Cyberversicherung. Bei 40 % ist Cyberschutz Teil einer umfassenderen Police (z. B. der Betriebshaftpflicht).

Die zunehmende Akzeptanz von Cyberversicherungen spiegelt sich auch in den Vertriebskanälen wider: 99 % der MSPs meldeten eine steigende Nachfrage nach Unterstützung sowie Lösungen, um die Anforderungen von Versicherern zu erfüllen.

Am häufigsten sind Kunden dabei an MDR Services interessiert (47 %), um bessere Konditionen beim Versicherungsschutz zu erhalten, dicht gefolgt von Anfragen von Kunden, die Hilfe beim Ausfüllen ihres Versicherungsantrags benötigen (45 %). Durch das Angebot von MDR Services und die Abrechnung von Fachdienstleistungen lassen sich in beiden Bereichen enorme Umsatzpotenziale für MSPs erschließen.

KUNDENANFORDERUNG	WELTWEIT				
Konditionen beim Versicherungsschutz **mit MDR** verbessern	**47 %**	49 %	38 %	56 %	36 %
Unterstützung beim Ausfüllen eines **Versicherungsantrags**	**45 %**	49 %	46 %	30 %	42 %
Konditionen beim Versicherungsschutz **mit EDR** verbessern	**34 %**	31 %	32 %	28 %	52 %
Konditionen beim Versicherungsschutz mit **Nicht-EDR/MDR**-Technologien und -Services verbessern	**33 %**	31 %	22 %	48 %	40 %

Hat Ihr Unternehmen einen gesteigerte Kundennachfrage nach Unterstützung und Lösungen zur Erfüllung von Cybersecurity-Anforderungen festgestellt? Anzahl=350 (USA 200, Großbritannien 50, Deutschland 50, Australien 50).

Ein Drittel (34 %) der MSPs gab an, dass Kunden ihre Sicherheitslösungen um Endpoint Detection and Response (EDR) erweitern möchten, um bessere Konditionen beim Versicherungsschutz zu erhalten. Interessanterweise ist die versicherungsbedingte Nachfrage nach MDR – mit Ausnahme von Australien – wesentlich höher als nach EDR. Mit einem spezialisierten 24/7 MDR Service lassen sich Risiken wesentlich einfacher und effizienter minimieren, als mit einem überlasteten internen Team.

Ein Drittel (33 %) der Befragten verzeichnete eine erhöhte Nachfrage nach Nicht-EDR/MDR-Technologien und -Services von Kunden, die bessere Konditionen bei Cyberversicherungen erzielen möchten. Im Rahmen unserer Umfrage wurden diese Technologien zwar nicht näher untersucht, wahrscheinlich handelt es sich unter anderem um MFA-Tools (Multi-Faktor-Authentifizierung) oder E-Mail- und Netzwerksicherheitslösungen, da diese sich positiv auf den Versicherungsschutz auswirken.

Empfehlung: Services und Technologien, die die Konditionen beim Versicherungsschutz optimieren, bieten MSPs lukrative Vertriebschancen. Um ihr Umsatzpotenzial zu maximieren, sollten MSPs ihr Angebot in diesem Bereich erweitern.

Fazit

Der Schutz vor unvermeidbaren Cyberangriffen ist von entscheidender Bedeutung und eröffnet MSPs enorme Wachstumschancen und Umsatzpotenziale. Von der Reduzierung des täglichen Verwaltungsaufwands durch die Konsolidierung von Management-Plattformen über die optimierte Zusammenarbeit mit MDR-Anbietern für ein erweitertes Service-Portfolio bis hin zur Ausrichtung der Aktivitäten an den Anforderungen von Cyberversicherern: MSPs können ihr Geschäft vorantreiben und gleichzeitig den Schutz ihrer Kunden vor Ransomware und Sicherheitspannen optimieren.

Der MSP-Markt ist oft hart umkämpft. Nutzen Sie die Erkenntnisse in unserem Report, um Ihr Wachstum zu beschleunigen und Ihren Umsatz zu steigern.

Sophos MSP-Programm

Sophos hilft MSPs dabei, ihr Geschäft auszubauen und die Profitabilität zu steigern. Innovative, adaptive Schutzmechanismen und ein komplettes Cybersecurity-System für MSPs sorgen für Cybersicherheit, damit Sie die Weichen auf Erfolg stellen können.

- Mit einem umfassenden Portfolio an Cybersecurity-Services und -Produkten werden Sie den aktuellen und zukünftigen Anforderungen Ihrer Kunden gerecht
- Minimieren Sie den täglichen Verwaltungsaufwand und setzen Sie Ressourcen frei, indem Sie die Sicherheit aller Kunden über unsere zentrale Security-Plattform Sophos Central verwalten
- Mit dem Sophos MSP-Programm profitieren Sie von attraktiven Gewinnmargen, lukrativen Incentives und aggregierten Abrechnungsmodellen

1 Active Adversary Report für Business Leader, Sophos, 2023

Mehr Informationen zum Sophos MSP-Programm finden Sie unter www.sophos.de/MSP. Sie möchten mehr über Sophos MDR erfahren? Besuchen Sie www.sophos.de/MDR

Sophos MDR: 24/7 Incident Response als Standard

Sophos MDR ist der Managed Detection and Response-Service, dem weltweit die meisten Kunden vertrauen. Mit 24/7 manueller Detection und Response als Standard können sich MSPs und ihre Kunden darauf verlassen, dass die Experten von Sophos Angriffe rund um die Uhr abwehren. Einige Highlights:

- 24/7 gezielte Bedrohungsbehebung durch Experten
- Umfassende Reaktion auf Vorfälle
- 24/7 direkter Telefon-Support
- Dedizierter Ansprechpartner
- Mehrere Reaktionsmodi
- Breach Warranty
- Proaktives Threat Hunting
- Funktioniert mit Endpoint-Schutz von Sophos und anderen Anbietern
- Erkennt die Übernahme von E-Mail-Konten in Microsoft 365 und Google Workspace
- Und vieles mehr.

Ganz gleich, ob Sie MDR als vollständig ausgelagerte Service-Leistung oder als flexible Ergänzung zu Ihrem internen SOC anbieten möchten – Sophos MDR hilft Ihnen dabei, Ihre Umsätze zu steigern.

„Sophos MDR hat mehrere Kunden vor potenziell katastrophalen Geschäftsausfällen bewahrt. Unsere Gewinnmargen sind um 100 % gestiegen, unser Umsatz sogar um 300 %."

James Wagner, President, The ITeam

2024-05-21 (WP-NP)

SOPHOS