Juli 2025

Marktbericht

Der MSP Customer Insight Report 2025

Was Unternehmen weltweit von ihren Cybersecurity Managed Service Povidern benötigen

Barracuda®
Your business, secured.

Inhalt

Einleitung

In diesem Bericht wird untersucht, was Unternehmen weltweit in Bezug auf Cybersecurity-Dienste von ihren Managed Service Providers (MSPs) benötigen und erwarten. Er stützt sich auf die Ergebnisse einer neuen internationalen Umfrage unter MSP-Kunden, die von Vanson Bourne in Auftrag gegeben wurde.

MSPs sind entscheidend für das Geschäft geworden. Die meisten der befragten Unternehmen lagern bereits einige oder alle ihrer Cybersecurity-Bedürfnisse an MSPs aus, und andere erkunden Möglichkeiten.

Dieser Bericht soll MSPs dabei helfen, zu verstehen, was ihre bestehenden Kunden jetzt und in Zukunft von ihnen erwarten, wie ihre potenziellen Kunden aussehen und wo sie zu finden sind, und was Kunden zu einem Wettbewerber treibt.

Insgesamt zeigen die Ergebnisse, dass:

- Kunden MSPs benötigen, um ihnen bei der Verwaltung ihrer Security zu helfen, während sie wachsen.
- In den nächsten Jahren werden die Kunden insbesondere Unterstützung bei der Implementierung von KI-Anwendungen und Machine Learning sowie der Netzwerksicherheit benötigen — und sie sind bereit, dafür mehr zu bezahlen.

Methodik

Barracuda beauftragte das unabhängige Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer globalen Umfrage unter 2.000 leitenden Sicherheitsexperten in IT- und Geschäftsfunktionen in Unternehmen mit 50 bis 2.000 Mitarbeitern aus einer Vielzahl von Branchen in den USA, dem Vereinigten Königreich, Frankreich, DACH (Deutschland, Österreich, Schweiz), Benelux (Belgien, Niederlande, Luxemburg), den nordischen Ländern (Dänemark, Finnland, Norwegen, Schweden), Australien, Indien und Japan. Die Umfrage wurde im April und Mai 2025 durchgeführt.

Einleitung

- Die meisten MSP-Kunden ziehen einen Anbieterwechsel in Erwägung. Zu den Gründen gehören Bedenken hinsichtlich der Fähigkeit des MSP, ihnen bei der Behebung und Wiederherstellung nach einem Cyberangriff zu helfen.

Wir hoffen, dass dieser Bericht den MSPs dabei hilft, ihre zukünftigen Strategien zu gestalten, neue Möglichkeiten zu erkennen und etwaige Lücken zu schließen. Barracuda steht Ihnen bei jedem Schritt zur Seite. Gemeinsam können wir sicherstellen, dass mehr Unternehmen angesichts der Herausforderungen durch sich ständig weiterentwickelnde Bedrohungen cyberresilient und geschützt sind.

Zentrale Ergebnisse

85 %

von Unternehmen mit 1.000 bis 2.000 Mitarbeitern verlassen sich auf MSPs für Security-Unterstützung, verglichen mit 61 % derjenigen mit 50 bis 100 Mitarbeitern

48 %

von Unternehmen wenden sich an MSPs, um rund um die Uhr Security-Unterstützung zu erhalten

52 %

von Unternehmen wenden sich an MSPs, wenn die Anzahl der Security-Tools unüberschaubar wird — der am häufigsten genannte Grund

51 %

von Unternehmen wenden sich an MSPs, um ihnen bei der Weiterentwicklung ihrer Security-Strategien zu helfen, während sie wachsen — die zweithäufigste Nennung

39 %

von Unternehmen erwarten, dass sie in den nächsten Jahren MSP-Unterstützung für KI- und Machine-Learning-Tools und -Anwendungen benötigen — der am häufigsten genannte Grund

92 %

von Unternehmen sind bereit, mehr für Unterstützung bei der Integration von Security-Tools zu zahlen

45 %

werden den MSP wechseln, wenn sie keine Nachweise für Fähigkeiten, Fachwissen und die Fähigkeit sehen, sie mit 24/7 Security zu unterstützen — der am häufigsten genannte Grund

Kundenstamm für MSPs

Cyberbedrohungen entwickeln sich weiter, da Angreifer künstliche Intelligenz-Tools und kriminelle Dienste auf Abruf nutzen, um zunehmend ausgefeiltere Angriffe zu starten — schneller, in größerem Umfang und mit größerer Präzision.

IT- und Security-Fachleute sind einem ständigen Bombardement solcher Bedrohungen ausgesetzt. Um die Organisation und ihre Vermögenswerte zu schützen, benötigen sie Sicherheitslösungen sowie Überwachungs-, Management- und Abwehrfunktionen rund um die Uhr und ein tiefes Verständnis der Bedrohungslandschaft. Nur wenige Unternehmen können all diese Anforderungen intern erfüllen.

Wichtige Erkenntnis: 73 % der befragten Unternehmen lagern Security-Dienste an einen MSP aus

96 % der befragten Unternehmen sind entweder bereits mit einem MSP verbunden oder erwägen die Zusammenarbeit mit einem solchen: 73 % geben an, dass sie Sicherheitsdienste bereits an einen MSP auslagern, weitere 18 % evaluieren derzeit Anbieter, und weitere 5 % ziehen die Möglichkeit in Betracht, einen MSP zu nutzen.

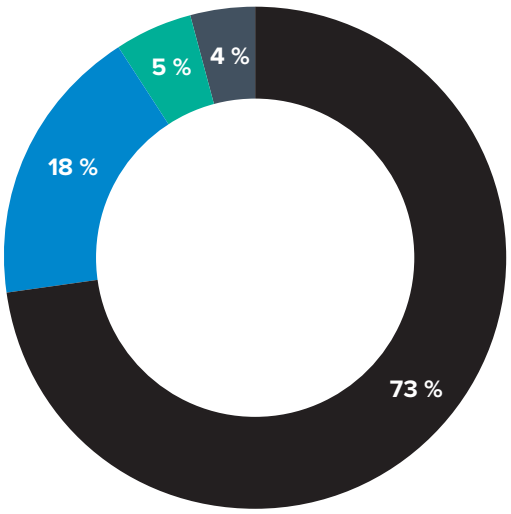

ABBILDUNG 1

Lagert Ihre Unternehmen IT-Sicherheitsaktivitäten an einen Managed Service Provider (MSP) aus?

n=2.000

- Ja
- Wir evaluieren derzeit Anbieter
- Wir ziehen die Möglichkeit in Betracht
- Nein

Hinter diesen Zahlen gibt es einige interessante Variationen.

Zum Beispiel nutzen die größten befragten Unternehmen eher MSPs als die kleineren.

Wichtige Erkenntnis: 85 % der Befragten mit 1.000 bis 2.000 Mitarbeitern verlassen sich auf MSPs für Security-Unterstützung, verglichen mit 61 % der Befragten mit 50 bis 100 Mitarbeitern

Dieses höhere Maß an MSP-Engagement spiegelt möglicherweise die Tatsache wider, dass größere Unternehmen eine größere Security-Komplexität und eine breitere Palette von Werkzeugen zu verwalten haben.

Beispielsweise machen sich die befragten größeren Unternehmen tendenziell mehr Sorgen als kleinere über die zunehmende Komplexität ihrer Security-Umgebung (42 %) und die zunehmende Komplexität von Cyberangriffen (46 %). Für die kleinsten untersuchten Unternehmen lauten die entsprechenden Zahlen 32 % und 34 %.

Etwas beunruhigend ist, dass 10 % der befragten kleineren Unternehmen keine Pläne haben, einen MSP zu engagieren, der ihnen bei der Cybersecurity hilft. Kleinere Unternehmen haben in der Regel weniger interne Ressourcen für den Schutz zur Verfügung, sodass dieser Ansatz sie anfällig für Angriffe machen könnte.

Die Branchen, die am ehesten die Cybersecurity an MSPs auslagern, sind die Kommunalverwaltungen (84 %) und das Bildungswesen (78 %). Es gibt ein geringeres Maß an Engagement in den Bereichen Freizeit und Unterhaltung (60 %), Einzelhandel (65 %) und Fertigung (57 %).

Unter den befragten Ländern arbeiten Unternehmen im Vereinigten Königreich und den Benelux-Staaten am häufigsten mit einem MSP zusammen (79 % bzw. 81 %). Die niedrigsten Ebenen der Zusammenarbeit sind in den nordischen Ländern (54 %) und in Japan (59 %) zu beobachten.

Kunden benötigen MSPs, die ihnen bei der Verwaltung der Security helfen, während sie wachsen

Die Forschung zeigt, dass der ideale MSP-Partner aus der Perspektive der Kunden sowohl praktischen, produkt- und technologieorientierten Support als auch strategische Unterstützung in Bezug auf Sicherheitspläne und Compliance bietet.

Ein Blick auf die beiden wichtigsten Ergebnisse deutet darauf hin, dass MSPs eine Schlüsselrolle dabei spielen, Unternehmen bei der Bewältigung der Security-Auswirkungen des Geschäftswachstums zu unterstützen.

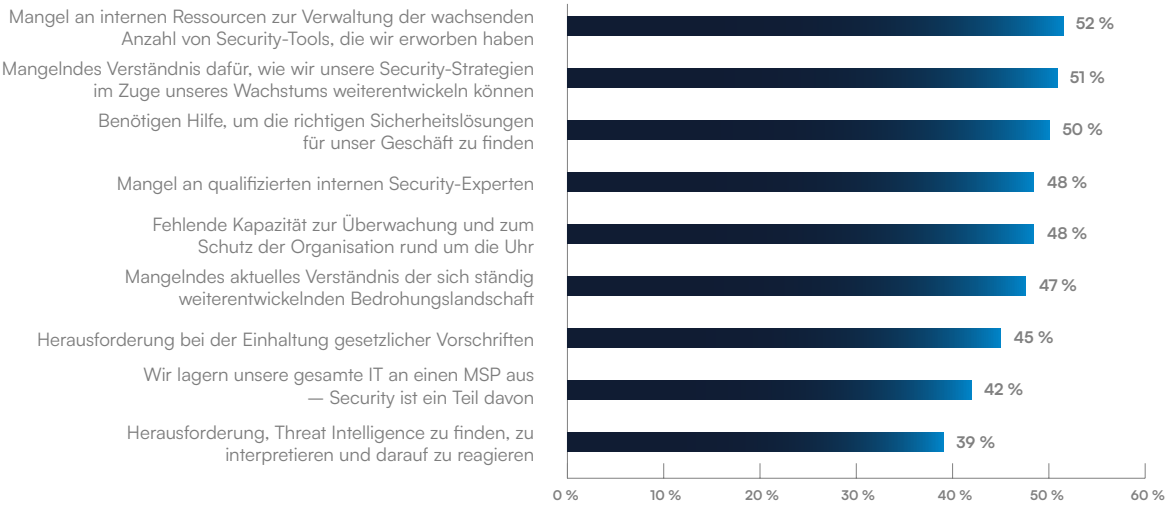

ABBILDUNG 2

Die Gründe für das Outsourcing der Security an einen MSP

n=2.000

Wichtige Erkenntnis: 52 % der Unternehmen wenden sich an MSPs, wenn die Anzahl der Security-Tools unüberschaubar wird

Die Unterstützung beim Jonglieren mit einer ständig wachsenden Anzahl von Security-Produkten war der am häufigsten genannte Grund für die Inanspruchnahme von MSPs. Viele dieser Tools stammen wahrscheinlich von verschiedenen Anbietern, und die meisten lassen sich nicht miteinander verknüpfen.

Diese Zahl steigt bei den Befragten im verarbeitenden Gewerbe auf 60 %. Fertigungsunternehmen haben wahrscheinlich eine erhebliche Anzahl von vernetzten Systemen und IoT-Geräten und daher eine höhere Wahrscheinlichkeit für eine Ausbreitung von Security-Tools.

Weitere Erkenntnisse aus der Studie zeigen, dass die fehlende Integration das Sicherheitsrisiko und die Gefährdung erhöhen kann, was es schwieriger und teurer macht, die Security zu verwalten und Bedrohungen zu erkennen und zu mindern.

Wichtige Erkenntnis: 51 % der Unternehmen wenden sich an MSPs, um ihre Security-Strategien im Zuge ihres Wachstums weiterzuentwickeln

Der am zweithäufigsten genannte Grund, sich an einen MSP für Security-Support zu wenden, spiegelt die sich entwickelnde Rolle der Dienstleister als Sicherheitsberater wider: 51 % verlassen sich auf ihren Partner, um ihre Security-Strategien weiterzuentwickeln und zu aktualisieren, wenn das Unternehmen wächst und sich verändert. Bildungs- und GesundheitsUnternehmen nannten dies besonders häufig als Grund für die Beauftragung eines MSP (jeweils 55 %).

Bildungseinrichtungen gehören ebenfalls zu denjenigen, die sich am meisten Sorgen über die zunehmende Komplexität ihrer IT-Security machen (48 % im Vergleich zu 38 % insgesamt), was darauf hindeutet, dass sie Schwierigkeiten haben, eine wachsende Anzahl digitaler Vermögenswerte zu schützen. Für sie ist es ein natürlicher Schritt, sich an einen MSP zu wenden.

Wichtige Erkenntnis: 48 % der Unternehmen wenden sich an MSPs, um 24-Stunden-Security-Unterstützung zu erhalten

Die meisten Unternehmen erkennen, dass Cybersecurity eine rund um die Uhr erforderliche Tätigkeit ist, die Personal und Investitionen erfordert, die viele von ihnen nicht intern haben. Die Inanspruchnahme eines MSP zur Unterstützung bei der Überwachung und Reaktion auf Bedrohungen und Sicherheitswarnungen rund um die Uhr ist ein weiterer wichtiger Treiber für das Engagement.

Viele MSPs betreiben jetzt, oft zusammen mit Security-Anbietern, ein Managed Security Operations Center (SOC), das eine solche Expertenabdeckung bietet. Um die umfassendste Security zu erreichen, kann dies mit einer verwalteten Extended Detection and Response (XDR)-Lösung kombiniert werden, die die gesamte Angriffsfläche abdecken kann, einschließlich Endpunkten, E-Mail, Cloud, Anwendungen und Netzwerken.

Für viele der befragten Unternehmen ist die Zusammenarbeit mit MSPs auch eng mit dem Mangel an internen Cybersecurity-Fachleuten verbunden — ein Grund, der von 48 % genannt wurde. Der Fachkräftemangel scheint eine universelle Herausforderung zu sein, da der Anteil über alle Unternehmensgrößen hinweg konstant bleibt.

Bei 42 % der Befragten wird die Security an einen MSP ausgelagert und mit anderen IT-Dienstleistungen gebündelt. Dies stellt sowohl eine Chance als auch ein Risiko für MSPs dar, insbesondere wenn es um Kunden geht, die sich entscheiden, ihr Geschäft zu verlagern — siehe den Abschnitt über Ausschlusskriterien.

Kunden werden in Zukunft mehr Unterstützung bei KI und Netzwerksicherheit benötigen

In den nächsten zwei Jahren werden die Kunden am ehesten die Hilfe von MSPs bei der Implementierung von KI-und Machine-Learning-Tools und -Anwendungen in Anspruch nehmen. Darauf folgt Unterstützung für Netzwerk-Security-Implementierungen wie Zero-Trust-Maßnahmen und SASE-(Secure Access Service Edge-)Lösungen.

Wichtige Erkenntnis; 39 % der Unternehmen erwarten, in den nächsten zwei Jahren MSP-Unterstützung bei KI- und Machine-Learning-Tools und -Anwendungen zu benötigen

KI und Netzwerksicherheit sind Bereiche mit wachsendem Geschäftsfokus, Sicherheitsschwachstellen und technischer Komplexität. Sie können schwer zu verstehen sein, insbesondere für die 48 % der unterbesetzten Unternehmen.

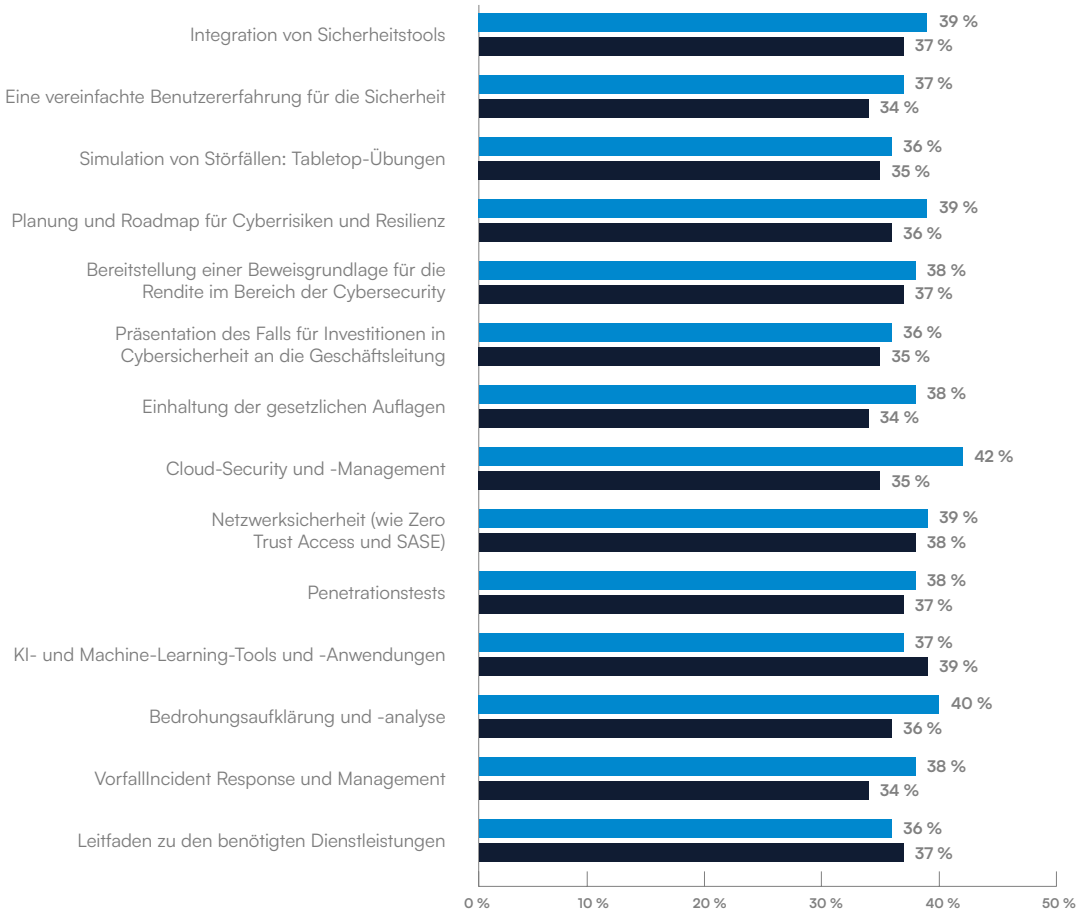

ABBILDUNG 3

Security-Chancen für MSPs: Wo Unternehmen in den nächsten 1 bis 2 Jahren Unterstützung von Dienstleistern erwarten

n=2.000

- Bereits von MSP genutzt
- Es wird erwartet, dass Unterstützung benötigt wird

Die Ergebnisse heben die unterschiedlichen Wege hervor, die Unternehmen verschiedener Größen beschreiten.

Zum Beispiel steigt bei Unternehmen mit 50 bis 100 Mitarbeitern der Anteil derer, die in Zukunft Unterstützung bei KI suchen, auf 44 %, während 29 % bereits Support erhalten. Bei den größten Unternehmen arbeiten 44 % mit MSPs im Bereich KI zusammen, und 37 % erwarten, dass sie in den nächsten zwei Jahren Unterstützung benötigen.

Dies deutet darauf hin, dass die größeren Unternehmen bereits die Grenzen des eigenständigen Umgangs mit KI und maschinellem Lernen verstehen — und aktiv mit MSPs zusammenarbeiten, um ihren KI-Einsatz sowohl in der IT als auch in der Security zu optimieren. Ein ähnliches Bild, jedoch mit geringeren Unterschieden, zeigt sich bei der Netzwerksicherheit.

Es ist auch erwähnenswert, dass strategische Dienstleistungen wie die Planung von Cyberrisiken und Resilienz, die Simulation von Incident Response-Maßnahmen und die Darstellung des ROI der Cybersecurity weit verbreitet genutzt und nachgefragt werden.

Kunden sind bereit, mehr für die Dienstleistungen zu zahlen, die sie wünschen

Die Umfrage ergab, dass fast alle MSP-Kunden bereit sind, in den nächsten zwei Jahren mehr für die zusätzlichen Dienste zu bezahlen, die sie benötigen, und rund 70 % sind bereit, bis zu 10 % oder 25 % mehr zu zahlen.

Wichtige Erkenntnis: 92 % der Unternehmen sind bereit, mehr für Unterstützung bei der Integration von Security-Tools zu zahlen

Zu den Diensten, für die sie am ehesten bereit sind, mehr Geld auszugeben, gehören KI- und Machine-Learning-Tools und -Anwendungen sowie Cloud-Security und Netzwerksicherheit. Die Ergebnisse bleiben über alle Unternehmensgrößen hinweg einheitlich.

Insgesamt schneiden operative Werkzeuge und Aktivitäten bei zusätzlichen Ausgaben besser ab. Es besteht eine gewisse Zurückhaltung, zusätzliche Ausgaben für „weichere“ Dienstleistungen wie die Simulation von Vorfällen, die Präsentation von Argumenten für Cybersecurity-Investitionen oder die Beratung über die benötigten Dienstleistungen zu tätigen.

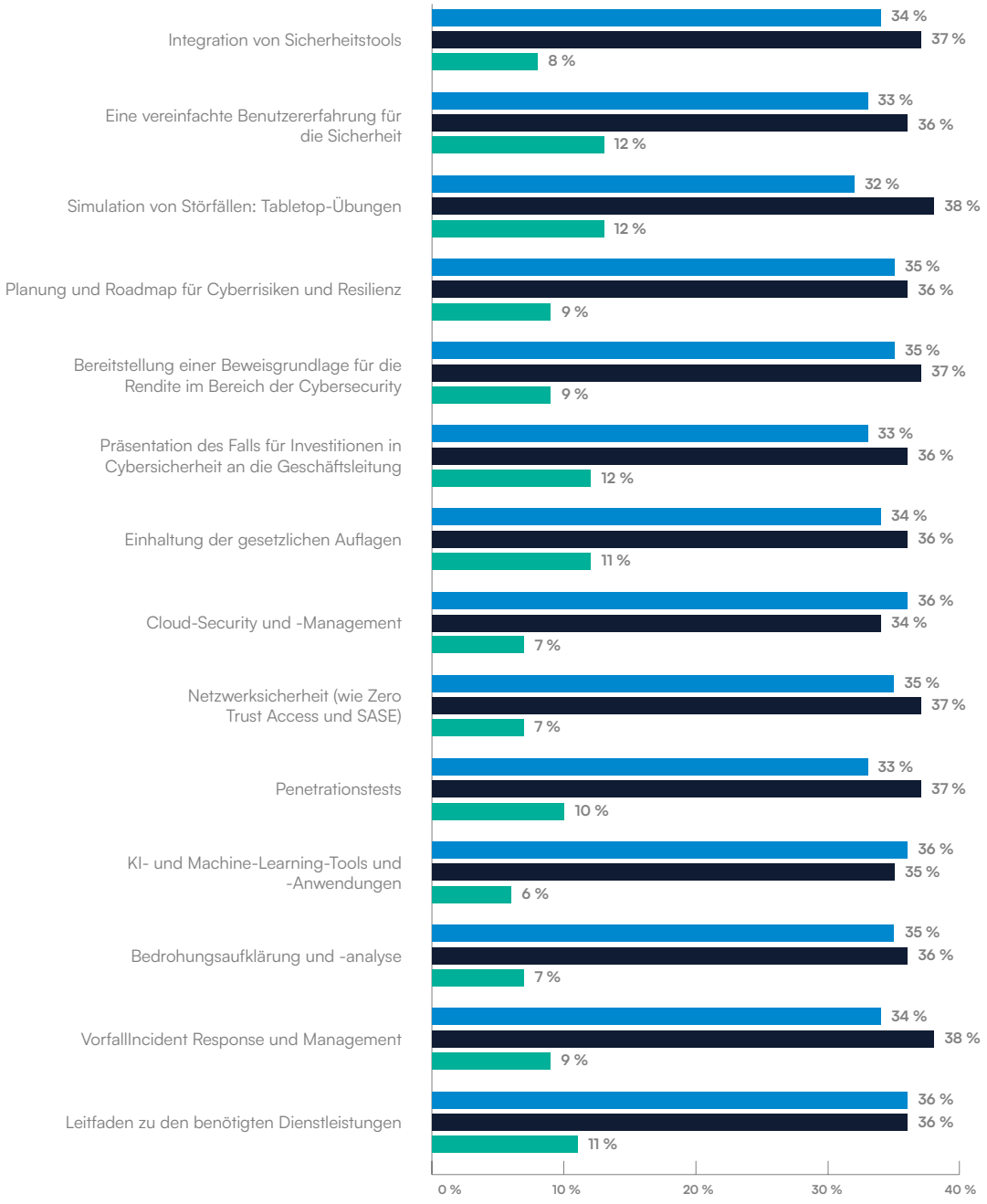

ABBILDUNG 4

Zusätzliche Kosten für Unternehmen sind bereit, in den nächsten 1 bis 2 Jahren für diese Dienstleistungen von MSPs zu zahlen

n=2.000

- Bereit, bis zu 25 % mehr zu zahlen
- Bereit, bis zu 10 % mehr zu zahlen
- Ich bin nicht bereit, dafür mehr zu bezahlen

Jedoch sehen die Prioritäten der Kunden und ihre Bereitschaft zu investieren ganz anders aus, wenn sie durch die Linse eines Security-Vorfalls betrachtet werden — wie etwa eines E-Mail-basierten Vorfalls oder eines Ransomware-Angriffs — siehe den Abschnitt über die Auswirkungen eines Security-Vorfalls weiter unten.

MSPs riskieren, Kunden zu verlieren, wenn sie kein Fachwissen nachweisen können

Die Ergebnisse zeigen, dass die Loyalität gegenüber einem MSP-Partner begrenzt ist und vom Vertrauen des Kunden in die Fachkompetenz, Qualität und Geschäftsstabilität des Dienstanbieters abhängt. Nur 2 % der Befragten gaben an, dass sie sich einen Wechsel zu einem anderen MSP nicht vorstellen könnten. Für alle anderen gibt es einige klare Ausschlusskriterien.

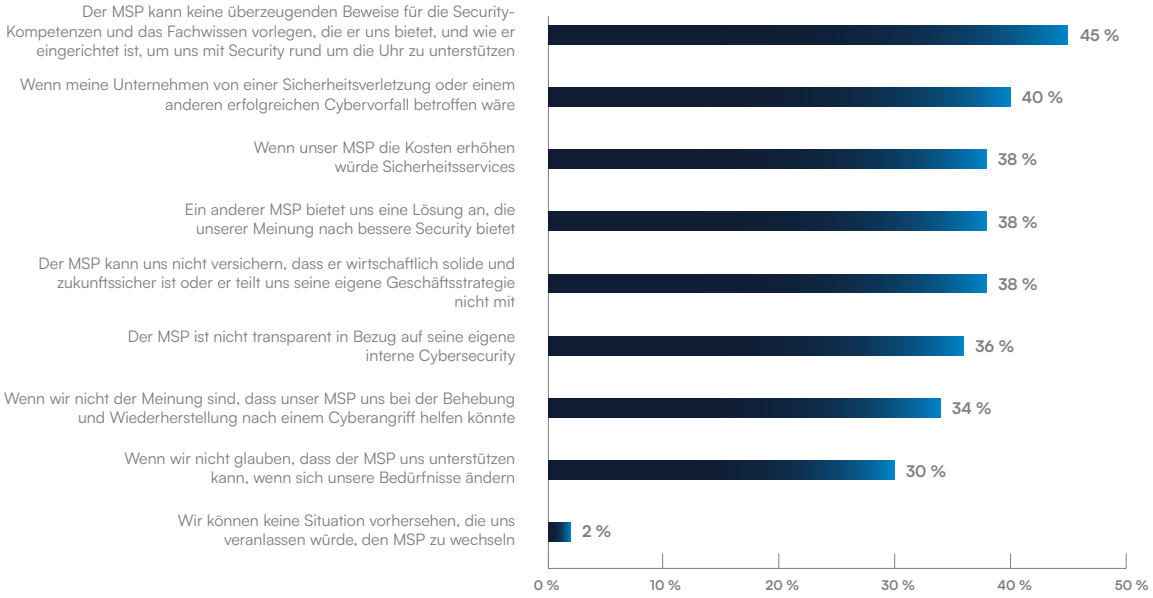

ABBILDUNG 5

Was würde Sie dazu bringen, einen Wechsel zu einem anderen MSP für Cybersecurity-Unterstützung in Betracht zu ziehen?

n=2.000

Ein Sicherheitsvorfall ist ein klarer Beziehungskiller, und für mehr als ein Drittel (38 %) der MSP-Kunden würde eine Preiserhöhung oder ein besseres Angebot eines anderen MSP dazu führen, dass sie die Seiten wechseln.

Wichtige Erkenntnis: 45 % werden den MSP wechseln, wenn sie keine Nachweise für Fähigkeiten, Fachwissen und die Fähigkeit sehen, sie mit Security rund um die Uhr zu unterstützen

Für die betroffenen MSPs ist es nicht nur eine Frage des Verlusts des Cybersecurity-Geschäfts — 89 % der abwandernden Kunden, die IT-Dienste mit Security-Lösungen gebündelt haben, werden diese Aktivitäten ebenfalls einstellen, entweder gleichzeitig (46 %) oder später (42 %).

Es ist erwähnenswert, dass 38 % der MSP-Kunden angeben, dass sie wechseln werden, wenn der MSP die Kosten erhöht. Zusammen mit den Ergebnissen zur Investitionsbereitschaft deutet

dies darauf hin, dass MSP-Kunden gerne mehr für die Dienstleistungen zahlen, die sie wünschen und benötigen, sich aber weniger wohl fühlen, wenn ihnen vom MSP willkürlich Preiserhöhungen auferlegt werden.

Die gute Nachricht ist, dass die potenziellen Stolpersteine fast ausschließlich Bereiche sind, die MSPs durch Investitionen in ihre eigene geschäftliche und Security-Resilienz sowie die ihrer Kunden und durch die Stärkung von Vertrauen und Transparenz angehen können.

Von einem Sicherheitsvorfall betroffene Unternehmen investieren mehr in Security und Outsourcing

Ein erfolgreicher E-Mail-Verstoß oder Ransomware-Angriff verschiebt die Security-Prioritäten.

Die Unterschiede zwischen denjenigen, die betroffen sind, und denjenigen, die nicht betroffen sind, werden deutlich, wenn man sich die Dienstleistungen ansieht, für die sie bereit sind, mehr zu bezahlen, und die Tätigkeiten, die sie nicht mehr effizient intern verwalten können. Diese Erkenntnisse beleuchten die Bereiche, in denen sich die Opfer möglicherweise besonders exponiert fühlen.

Wichtige Erkenntnis: 91 % der Angriffsopfer sind bereit, für eine vereinfachte Security-Nutzererfahrung mehr zu bezahlen, verglichen mit 77 % der Nichtopfer

Beispielsweise sind 91 % der Opfer bereit, für eine vereinfachte User-Erfahrung im Bereich Security mehr zu bezahlen, verglichen mit 77 % derjenigen, die nicht betroffen sind. Die Gesamtzahl beträgt 88 %. Dies deutet darauf hin, dass bei vielen Opfern menschliches Versagen oder Fehlkonfigurationen — beides leicht durch komplexe Benutzeroberflächen ausgelöst — eine Rolle bei dem Angriff gespielt haben könnten.

Opfer sind außerdem eher bereit, mehr für Cyber-Resilienz-Dienste zu zahlen, wie etwa für die Planung der Incident Response, das Verständnis von Vorschriften und Compliance sowie für strategische Beratung zu Security-Diensten. Dies deutet darauf hin, dass die Opfer bereit sind, in Bereiche zu investieren, die sie besser auf zukünftige Angriffe vorbereiten und ihnen helfen, sich davon zu erholen.

Wenn es um Aktivitäten geht, die intern oder extern durchgeführt werden, zeigt sich dieselbe Ungleichheit — diejenigen, die nicht direkt von einem Vorfall betroffen waren, haben eher das Gefühl, dass sie die Dinge selbst bewältigen können.

Wichtige Erkenntnis: 81 % der Angriffsopfer planen, die Cloud-Security und das Management auszulagern, verglichen mit 73 % der Nichtopfer

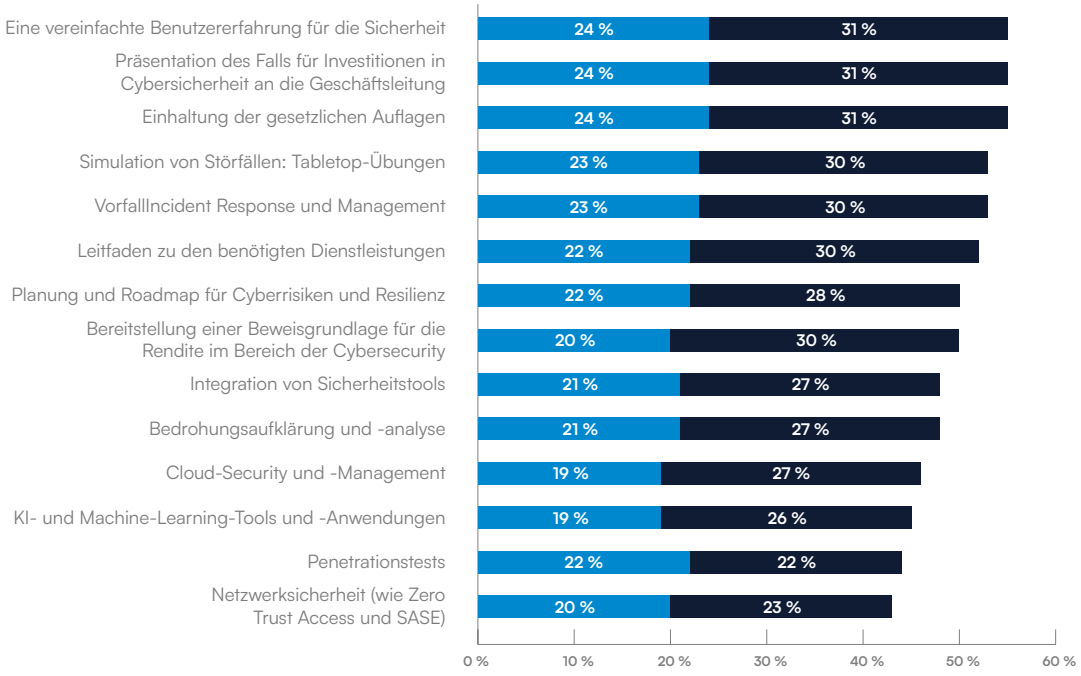

ABBILDUNG 6

Unternehmen, die in den nächsten 1 bis 2 Jahren jeden der folgenden Aspekte intern verwalten möchten

n=2.000

- Hat im letzten Jahr einen E-Mail-Verstoß oder einen erfolgreichen Ransomware-Angriff erlebt
- Hat im letzten Jahr keine E-Mail-Datenpanne oder keinen erfolgreichen Ransomware-Angriff erlebt

Fazit

Die Ergebnisse zeigen, dass MSPs im Jahr 2025 vor vielen vielversprechenden Chancen stehen — aber es gibt auch einige Herausforderungen.

Viele Kunden wünschen sich beispielsweise Hilfe bei der Bewältigung des Wildwuchses der Sicherheit. Allerdings kann es für Anbieter schnell überwältigend werden, wenn sie mehrere Kunden mit mehreren Produkten betreuen müssen. Security-Anbieter spielen eine wichtige Rolle bei der Unterstützung von MSPs, um Management-, Reaktions- und Berichtsaktivitäten durch zentralisierte Dashboards und Produktkonsolidierung zu integrieren. Ebenso können Anbieter MSPs dabei helfen, die klare Nachfrage nach einer 24/7-Security-Überwachung mit verwalteten SOCs zu erfüllen.

Dann besteht die Notwendigkeit, Kunden bei der Einhaltung von Vorschriften und Bestimmungen sowie bei der Implementierung von KI- und Machine-Learning-Tools und -Anwendungen zu unterstützen.

Darüber hinaus müssen sich MSPs darauf vorbereiten, dass Kunden proaktivere und vorausschauendere Dienstleistungen wünschen, wie z. B. Bedrohungsaufklärung, Incident Response-Planung, Risikomanagement und strategische Beratung.

Und als ob das nicht genug wäre, müssen MSPs auch ihre eigene wirtschaftliche Rentabilität im Auge behalten und Fachwissen sowie ein robustes Geschäftsmodell nachweisen — andernfalls riskieren sie, Kunden an die Konkurrenz zu verlieren. Dies erfordert ein Produktportfolio, das fortschrittlich und innovativ ist, aber auch für die Kunden einfach zu kaufen, bereitzustellen und zu verwenden ist. Es erfordert auch Security-Anbieter, die sich zu einer Partnerschaft verpflichten.

Fazit

Wie Barracuda Sie unterstützen kann

Bei Barracuda sind wir zu 100 % dem Vertriebskanal verpflichtet und darauf fokussiert, unseren Partnern zum Erfolg und Wachstum zu verhelfen.

BarracudaONE™

BarracudaONE ist eine KI-gestützte Cybersecurity-Plattform, die integrierte Produkte über ein zentrales Dashboard bereitstellt, um den Schutz und die Cyber-Resilienz zu maximieren und gleichzeitig einfach zu kaufen, bereitzustellen und zu verwenden ist.

Die Plattform vereinfacht die Verwaltung von Security-Tools für einen MSP bei all seinen Kunden und stellt sicher, dass die Tools ordnungsgemäß konfiguriert sind, Warnmeldungen zentralisiert werden und Berichte bereitgestellt werden, die den Wert zeigen, den ein MSP seinen Kunden im Bereich Security bietet.

BarracudaONE ist ohne zusätzliche Kosten für MSPs, andere Vertriebspartner und Kunden verfügbar, die bereits Barracuda Email Protection, Barracuda Cloud-to-Cloud Backup und Barracuda Data Inspector nutzen. Die Plattform bietet eine zentralisierte Schnittstelle für MSPs und Partner zur einfachen Verwaltung von Lösungen und Lizenzen.

Barracuda Managed XDR™

MSPs, Partner und Endnutzer können ihre Sicherheitslage mit Barracuda Managed XDR, einem 24/7-Dienst, der professionelle Bedrohungserkennung und -reaktion bietet, unterstützt durch das preisgekrönte SOC von Barracuda, weiter stärken.

Über Barracuda

Barracuda ist ein weltweit führendes Cybersecurity-Unternehmen, das Unternehmen jeder Größe umfassenden Schutz vor komplexen Bedrohungen bietet. Unsere KI-gestützte Plattform sichert E-Mails, Daten, Anwendungen und Netzwerke mit innovativen Lösungen, einem verwalteten XDR-Service und einem zentralen Dashboard, um den Schutz zu maximieren und die Cyber-Resilienz zu stärken. Von Hunderttausenden von IT-Experten und Managed Service Providern weltweit als vertrauenswürdig angesehen, bietet Barracuda leistungsstarke Abwehrmaßnahmen, die einfach zu kaufen, bereitzustellen und zu verwenden sind.

Informationen Vanson Bourne

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung im Technologiesektor. Der Ruf des Unternehmens für robuste und glaubwürdige forschungsbasierte Analysen beruht auf strengen Forschungsprinzipien und der Fähigkeit, die Meinungen hochrangiger Entscheidungsträger in allen technischen und geschäftlichen Funktionen, in allen Geschäftsbereichen und allen wichtigen Märkten einzuholen. Weiter Informationen erhalten Sie unter vansonbourne.com.