kaspersky

Momentum für MSPs – Potentiale und Herausforderungen in einer dynamischen IT-Sicherheitslandschaft

kaspersky

Momentum für MSPs – Potentiale und Herausforderungen in einer dynamischen IT-Sicherheitslandschaft

Einführung

Der Markt für Managed Service Provider (MSPs) bietet im Augenblick ein gutes Geschäft, hat sich aber im Laufe der Zeit stark gewandelt. Spielten MSPs anfangs fast ausschließlich die Rolle von IT-Resellern, die für ihre Kunden spezifische Lösungen bereitstellten, installierten und verwalteten, so sind sie heute ein integraler Bestandteil des Netzwerks ihrer Kunden, wenn es um Beschaffung und Support der Unternehmens-IT geht. In vielen Fällen wird der MSP als Erweiterung des internen IT-Teams angesehen; bei manchen Unternehmen liegt bereits die komplette IT in den Händen eines MSPs. Damit lässt sich die vielfach vorhandene Lücke an entsprechenden Fähigkeiten sowie personellen Ressourcen im Unternehmen schließen und ein glatter und reibungsloser IT-Betrieb sicherstellen.

Besonders kleine und mittlere Unternehmen (KMUs) verlassen sich auf Managed Service Provider und sehen in ihnen vertrauenswürdige Lotsen durch eine sich ständig verändernde IT-Landschaft. Denn häufig können interne Kapazitäten und Budgets mit der Entwicklung nicht mehr mithalten. Das stetige Wachstum an Cloud-Lösungen ist dabei nur ein Beispiel dafür, welche bedeutende Rolle Managed Service Provider bei der Unterstützung kleinerer Unternehmen spielen, damit diese von Cloud-basierten Anwendungen profitieren können.

Das Analystenhaus Gartner prognostiziert für den Markt öffentlicher Cloud-Dienstleistungen 2019 eine Wachstumsrate von 17,5 Prozent sowie ein Volumen von 214,3 Milliarden US-Dollar. Für die MSP-Branche eine große Chance, Unternehmen aktuell und zukünftig bei der erfolgreichen Umsetzung entsprechender Projekte zu unterstützen. Laut Gartner wird der Markt für Cloud-Dienste bis 2022 fast dreimal so stark wachsen wie die IT-Dienstleistungsbranche generell [1].

Passend dazu soll der Markt für Managed Services von derzeit 180,5 Milliarden bis 2023 auf 282 Milliarden US-Dollar bis zum Jahr 2013 anwachsen. Was sind die Gründe dafür? Zum einen möchten Unternehmen mit Hilfe der MSPs ihre Produktivität steigern, zum anderen nimmt die Nachfrage nach Cloud-basierten Managed Services weiter zu [2]. Ein dritter und wichtiger Grund für das Wachstum ist die Wertschöpfung durch das Outsourcen von IT- und Sicherheitsmanagementaufgaben.

Zweifellos nehmen schädliche Cyberangriffe auf Unternehmen zu. Letztere sind sich daher der Risiken und Folgen eines Datenverlustes oder Angriffes durch Ransomware stärker bewusst. Meist kommen nur die Datenlecks in großen Konzernen ans Licht der Öffentlichkeit. Doch kleinere Unternehmen und Zulieferer sind ebenso verwundbar und die Konsequenzen nicht weniger folgenreich.

Egal, wie groß ein Unternehmen ist oder welcher Branche es angehört: heute ist das Rückgrat jeder Firma die dort eingesetzte Technologie. Deshalb wird es immer herausfordernder, mit dem Tempo neuer Anwendungen und der Weiterentwicklung von Cybersicherheitsbedrohungen Schritt zu halten. Das gilt besonders für Unternehmen, die nicht über das Budget und die Möglichkeiten von Konzernen verfügen. Tatsächlich zeigt die aktuelle Kaspersky-Studie, dass sich Unternehmen mit weniger als 500 Mitarbeitern besonders häufig an externe Dienstleister wenden, wenn es um das Management und die Sicherheit ihrer IT-Infrastruktur geht. Vier von zehn legen ihr IT-Management und 33 Prozent die IT-Sicherheit in die Hände von Drittanbietern.

Diese hohen Werte belegen, dass mit enger werdenden Budgets und Ressourcen viele Unternehmen die beste Lösung in der Konsultation externer Experten sehen. Wie man am vorhergesagten globalen Marktwachstum erkennen kann, bietet diese Entwicklung enorme Chancen für Managed Service Provider. Gleichzeitig wird jedoch erwartet, dass diese die Lücke an nicht vorhandenem Know-how in den Unternehmen schließen und im Fall eines Datenlecks die Rolle des Sündenbocks übernehmen.

Um die derzeitigen Herausforderungen und Chancen für europäische MSPs auszuloten, beschäftigt sich diese Studie mit der wachsenden Marktdynamik und den Auswirkungen hinsichtlich des Wandels bei Kundenbeziehungen und -erwartungen in der Branche. Managed Service Provider erhalten darüber hinaus

Empfehlungen, wie sie von den neuen Möglichkeiten profitieren und langfristige Kundenbeziehungen aufbauen können – unabhängig von den Herausforderungen, die auf diesem Weg liegen.

Das Wichtigste in Kürze

- Die Tendenz zum Outsourcing von IT und speziell von IT-Sicherheit nimmt zu. Bei einem Drittel (33 Prozent) aller Unternehmen mit weniger als 500 Mitarbeitern in Europa wurde das IT-Sicherheitsmanagement bereits ausgelagert. Weitere 21 Prozent planen, dies innerhalb der nächsten zwölf Monate in Angriff zu nehmen.
- Gründe dafür sind fehlendes internes Know-how und der Wunsch, ein begrenztes IT-Budget möglichst effektiv einzusetzen. 51 Prozent der Unternehmen möchten über das Auslagern dieses Bereichs interne Wissenslücken schließen, 52 Prozent erhoffen sich davon eine Kostenreduktion im Bereich IT-Sicherheit.
- Im Fall von Budgetkürzungen ist für Unternehmen Outsourcing die kostengünstigste Möglichkeit, die optimale Wertstellung im Auge zu behalten und zukünftige Anforderungen an das IT-Sicherheitsmanagement sicher zu stellen.
- Drei von vier MSPs (75 Prozent) sehen in der Erfüllung der Kundenbedürfnisse eine zentrale Herausforderung. So fürchten 68 Prozent der MSPs um ihre Rentabilität, da die Anforderungen der Kunden zu viele zusätzliche Ressourcen binden. Insbesondere wenn Sicherheitsprobleme durch internes Fehlverhalten verursacht wurden.
- Eine hohe Reputation am Markt ist der Schlüssel, um neue Kunden zu gewinnen und bestehende Partnerschaften zu festigen. Zur Vergrößerung ihres Kundenstamms setzen 83 Prozent der befragten MSPs auf Mundpropaganda, Weiterempfehlungen, direkte Ansprache durch Vertriebsmitarbeiter (50 Prozent) und Event-Sponsoring (48 Prozent).
- Ähnliches gilt für MSPs bei der Wahl ihres Partners im Bereich IT-Sicherheit. 92 Prozent haben neben dem Preis auch dessen Reputation im Blick. Um ihren Kunden einen Mehrwert bieten zu können, benötigen Managed Service Provider einen Verbündeten, der nicht nur über passende Lösungen verfügt und Hilfestellung geben kann, sondern diese Leistungen auch zum bestmöglichen Preis anbietet.
- Die derzeitigen Erwartungen an MSPs sind wie folgt: 84 Prozent der Kunden sehen sie vor allem als Experten für das Thema Cloud-Infrastruktur an. Auch Cybersicherheit steht bei den Auftraggebern hoch im Kurs: 74 Prozent betrachten die Expertise im Bereich IT-Sicherheit als Schüsselqualifikation ihres MSP-Partners.
- Unerwartete Ereignisse können für MSPs eine Belastungsprobe in der Kundenbeziehung darstellen und finanzielle Einbußen zur Folge haben, da das Umsatzwachstum gebremst wird. So erwarten 78 Prozent der Kunden, dass ihr MSP auch Aufgaben übernimmt, die außerhalb des vertraglich vereinbarten Spektrums liegen. 65 Prozent der MSPs kümmern sich demnach auch um Sicherheitsprobleme, die durch Fehlverhalten der Nutzer verursacht wurden und nicht im Zusammenhang mit den vereinbarten Dienstleistungen stehen.
- Aus diesem Grund werden MSPs oft Sicherheitsvorfälle angelastet, für die sie keine Verantwortung tragen. 43 Prozent aller Unternehmen, bei denen ein Datenleck aufgetreten ist, machten dafür ihren MSP verantwortlich. 27 Prozent führten den Vorfall auf mangelndes Sicherheits-Know-how ihres Service-Providers zurück.

Methodologie

Die hier beschriebenen Ergebnisse basieren auf folgenden zwei Quellen:

- Insgesamt wurden 101 Mitarbeiter von Managed Service Providern in Großbritannien, Frankreich, Deutschland, Spanien, Italien, Österreich, Schweden und Dänemark zwischen Juli und August 2019 telefonisch befragt.
- Außerdem wurde der Kaspersky Corporate IT Security and Risks Survey 2019 hinzugezogen. Dabei handelt es sich um eine jährlich stattfindende Online-Befragung unter IT-Entscheidern in Unternehmen aus 23 Ländern, die im Juni 2019 durchgeführt wurde. Hierbei kamen lediglich die Antworten von Befragten in europäischen Unternehmen mit weniger als 500 Mitarbeitern zur Auswertung.

IT-Outsourcing verändert die Dynamik am MSP-Markt

Die europäische Perspektive

Die Rolle des Managed Service Providers hat sich verändert. Aus dem einfachen Lösungsanbieter für Unternehmen ist ein vertrauensvoller Berater mit einer zentralen Rolle für den Geschäftserfolg geworden. IT-Outsourcing wird zum Normalfall. Unternehmen setzen auf Experten, die bei Fragen zu einer sich immer weiter entwickelnden IT-Infrastruktur und den damit verbundenen Facetten beratend zur Seite stehen und diese verwalten.

40 Prozent der von Kaspersky europaweit befragten Unternehmen mit weniger als 500 Mitarbeitern nutzen derzeit Drittanbieter für ihr IT-Management. Ein Drittel (33 Prozent) hat auch das Thema IT-Sicherheitsmanagement ausgelagert. Ein wichtiges Teilgebiet der IT, an dem zu erkennen ist, wie groß das Vertrauen der Unternehmen in die Zuverlässigkeit ihrer Provider inzwischen geworden ist.

In Europa ist dieser Trend weit verbreitet, wobei die Niederlande hierbei führend sind. Dort haben bereits 45 Prozent der Unternehmen ihre IT-Sicherheit ausgelagert. Mit wenig Abstand folgen Schweden und Italien (jeweils 39 Prozent). In einigen europäischen Ländern sehen Unternehmen starken Nachholbedarf und wollen in den nächsten zwölf Monaten mit der Auslagerung ihres IT-Sicherheitsmanagements beginnen. Das gilt vor allem für Polen (35 Prozent), Deutschland (34 Prozent), die Tschechische Republik (24 Prozent), Frankreich und Spanien (jeweils 22 Prozent).

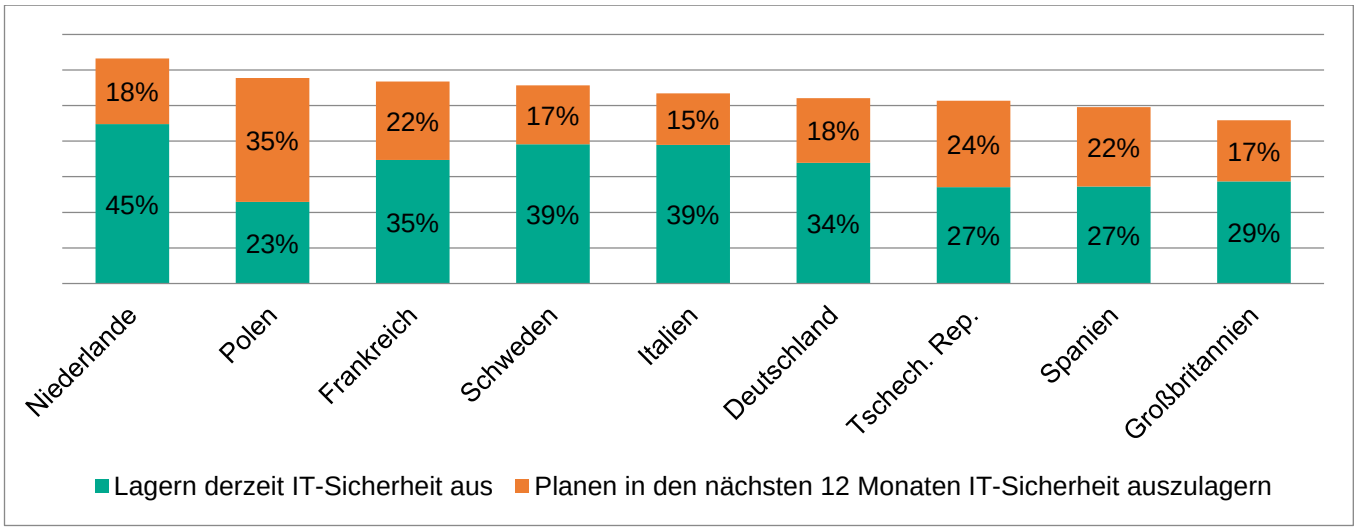


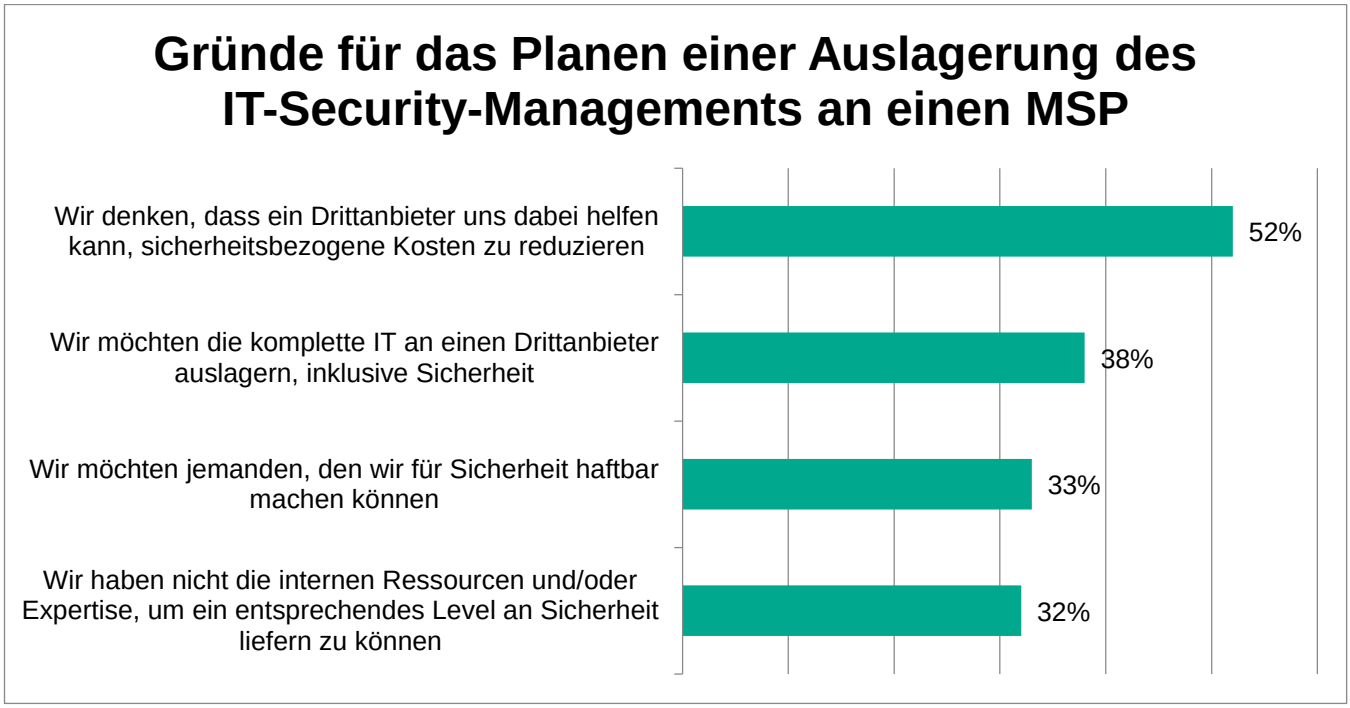
Abbildung 1: Outsourcing der IT-Sicherheit – derzeitiger Stand und geplantes Vorgehen in den nächsten zwölf Monaten

Entscheidet sich ein Unternehmen für Outsourcing, sind die Modelle der Zusammenarbeit oft abhängig von den jeweiligen Geschäftsanforderungen. Eine knappe Mehrheit der MSPs (51 Prozent) gibt an, dass Kunden eine Partnerschaft oder einen gemischten Ansatz anstreben, mit dem intern vorhandene Know-how-Lücken über Outsourcing geschlossen werden, und das IT-Sicherheitsmanagement wieder stabilisiert werden kann. 29 Prozent und damit fast ein Drittel der MSPs sagen aber auch, dass Unternehmen am liebsten ihre komplette IT inklusive IT-Sicherheit auslagern würden.

Die relevanten Entscheidungskriterien

Wie bei vielen geschäftlichen Entscheidungen ist auch beim Outsourcing des IT-Sicherheitsmanagements die Einsparung von Kosten der treibende Faktor. Mehr als die Hälfte der Unternehmen (52 Prozent), die eine Auslagerung ihres IT-Security-Managements planen, verspricht sich davon eine spürbare Kostenreduktion. 38 Prozent wollen ohnehin ihre komplette IT (und damit auch die IT-Sicherheit) externen Spezialisten überantworten. Interessanterweise sieht ein Drittel (33 Prozent) der Unternehmen im Outsourcing eine Möglichkeit, auch die Themen Service-Level-Agreement (SLA) und Rechenschaftspflicht abhaken zu können. Etwa derselbe Anteil von Unternehmen (32 Prozent) räumt ein, mangels geeigneter interner Ressourcen und Expertise nur so die Fortführung der Geschäftstätigkeit hinreichend sicher gewährleisten zu können.

Umgekehrt gibt es gute Gründe, weshalb Firmen sich noch scheuen, ihre IT-Sicherheit in die Hände externer Experten zu geben. Diese sollten Managed Service Provider im Auge behalten, wenn sie ihr Geschäft ausweiten wollen und eine langfristige Bindung ihrer Kunden anstreben. Trotz dem oft als Hauptgrund für die Zusammenarbeit mit einem Drittanbieter angeführten Expertentum, sind 40 Prozent der Unternehmen – die sich gegen das Outsourcing von IT-Sicherheitsmanagement aussprechen – der Auffassung, selbst intern über genügend Fachwissen zu verfügen, um ihre eigene IT-Sicherheit zu verwalten. Für 33 Prozent sind es hierbei insbesondere die erwarteten hohen Kosten, die einem Outsourcing des IT-Sicherheitsmanagements im Wege stehen.



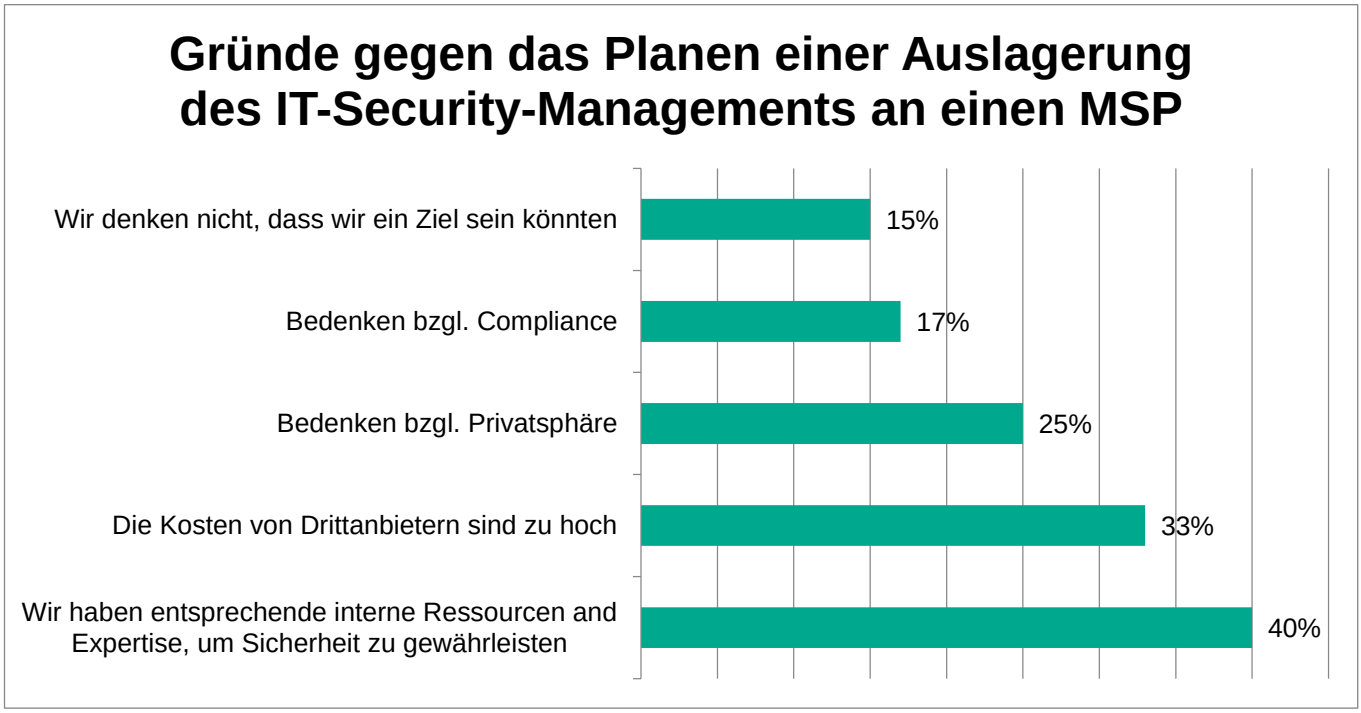


Abbildung 2: Für und Wider bei der Auslagerung des IT-Sicherheitsmanagements an einen MSP

Beleuchtet man den Prozess der Entscheidungsfindung tiefergehend und betrachtet einzelne Branchen, so zeigen sich unterschiedliche Motivationsgründe. Zwar ist in den meisten Geschäftsfeldern tatsächlich die erwartete Kosteneinsparung ausschlaggebend. Im Gesundheitswesen wird jedoch hauptsächlich auf Grund von Datenschutz-Bedenken auf Outsourcing verzichtet, während Bildungseinrichtungen das Gefühl haben, die Kosten für die Einbindung von Lösungen eines Dienstleisters seien zu hoch. Die Kostenfrage ist sicher die größte Herausforderung für Managed Service Provider und Unternehmen. Auffallend ist, dass Unternehmen mit einem wachsenden Budget für IT-Sicherheit diese zusätzlichen Ressourcen lieber in die Aufstockung ihres eigenen IT-Teams mit entsprechenden Spezialisten investieren. Umgekehrt suchen Unternehmen bei einem enger werdenden Budget ihr Heil für die zukünftige IT-Sicherheit in der Unterstützung durch MSPs.

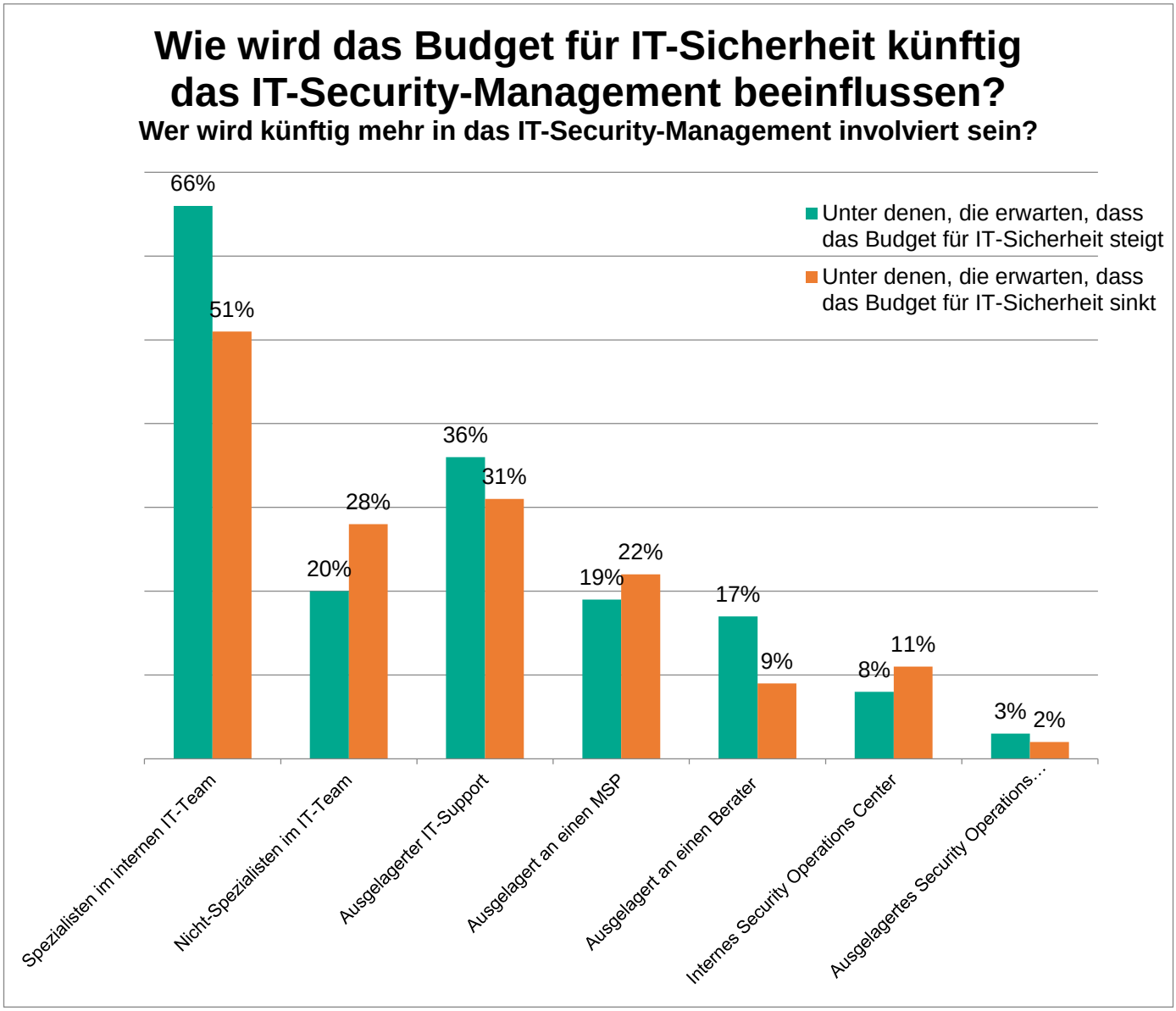


Abbildung 3: So wirken sich Veränderungen des Budgets für IT-Sicherheit auf das IT-Security-Management aus

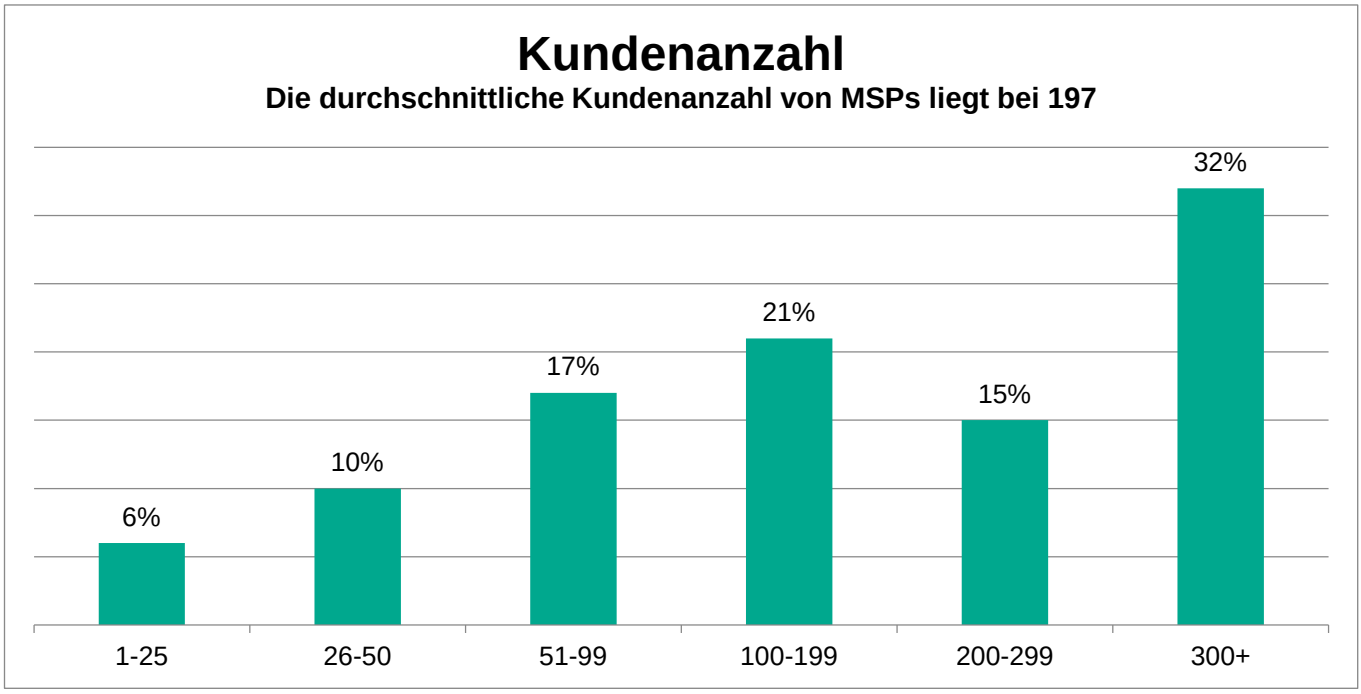
Es zeigt sich, dass vor allem zwei Faktoren das Wachstum der Managed Service Provider bestimmen: Zum einen die optimale Nutzung vorhandenen Budgets und zum anderen der Wunsch sicherzustellen, dass die richtigen Ressourcen allokiert und die entsprechenden Sicherheitsvorkehrungen getroffen werden. Dieselben Gründe können aber viele Unternehmen und ganze Branchen auch davon abhalten, sich externe Unterstützung zu holen.

Die europäische MSP-Landschaft: Prioritäten und Herausforderungen

Unterüberschrift>> Definition eines „typischen“ Managed Service Providers heute

Wie bereits festgestellt, sind gegenwärtig sowohl Rolle als auch Verantwortlichkeiten von MSPs einem Wandel unterworfen. Um die spezifischen Chancen und Herausforderungen dieser stattfindenden Veränderungen valide zu bewerten, muss das bisherige Bild eines Managed Service Providers neu gedacht werden.

Die Mehrheit (57 Prozent) der von Kaspersky befragten MSPs beschäftigt zwischen zwei und 20 Mitarbeiter. Obwohl es sich um kleine Unternehmen handelt, betreut ein Drittel (32 Prozent) davon Kunden mit über 300 Angestellten. Die Hälfte arbeitet mit einer Vielzahl von Auftraggebern aus unterschiedlichen Branchen zusammen, wovon sich ein Drittel (35 Prozent) hingegen nahezu ausschließlich auf die Unterstützung von kleinen und mittleren Unternehmen konzentriert.



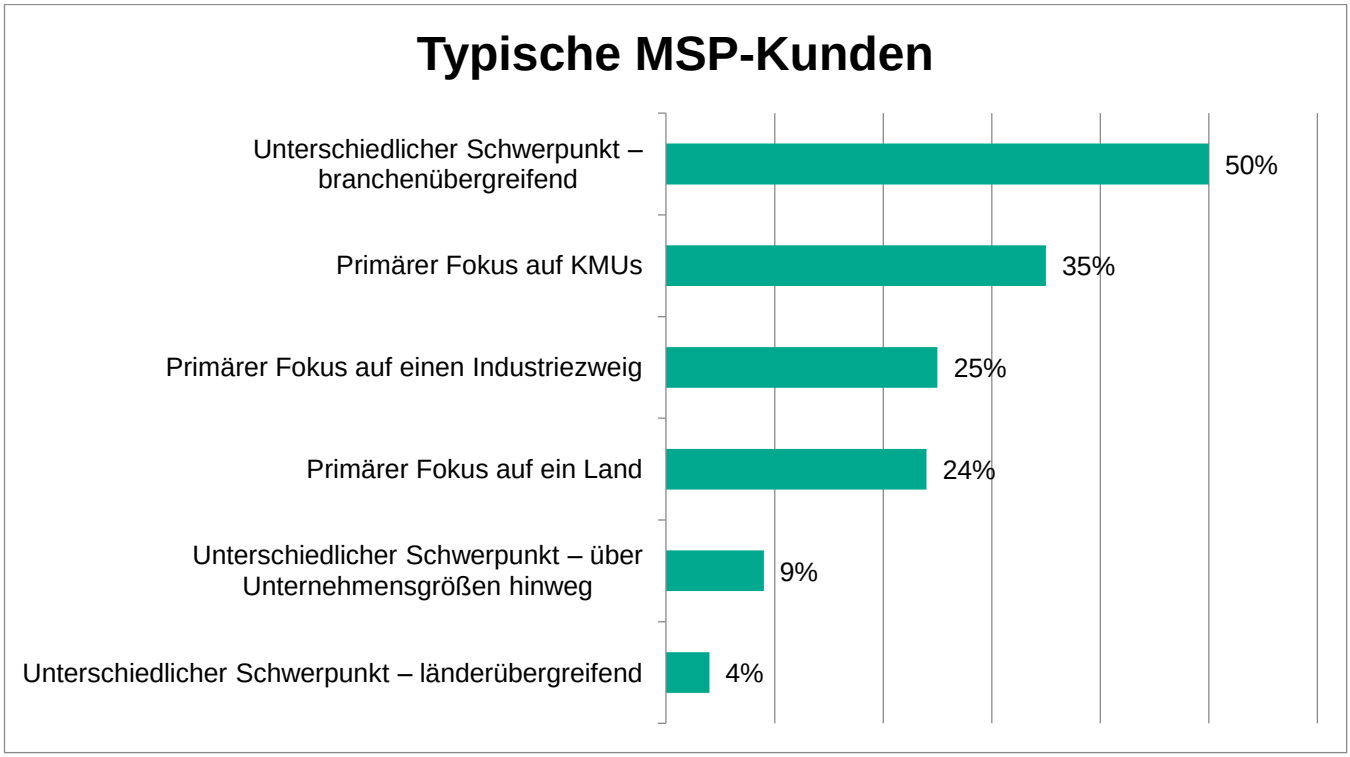


Abbildung 4: Anzahl von MSP-Kunden und typische MSP-Kunden

Eine derart breite Kundenbasis stellt für MSPs eine nicht zu unterschätzende Herausforderung dar. Denn sie müssen spezifische Besonderheiten einer Branche und mögliche, geschäftsspezifische Komplikationen, mit denen diese konfrontiert ist, verstehen, um dann ihre Kunden tatsächlich unterstützen zu können. Daher müssen MSPs ihren Kunden eine breite Palette von Dienstleistungen anbieten, die deren individuellen Bedürfnissen umfassend gerecht wird. Dies bedeutet aber auch, dass sie kompetente Fähigkeiten und breites Fachwissen in zahlreichen Bereichen vorweisen müssen.

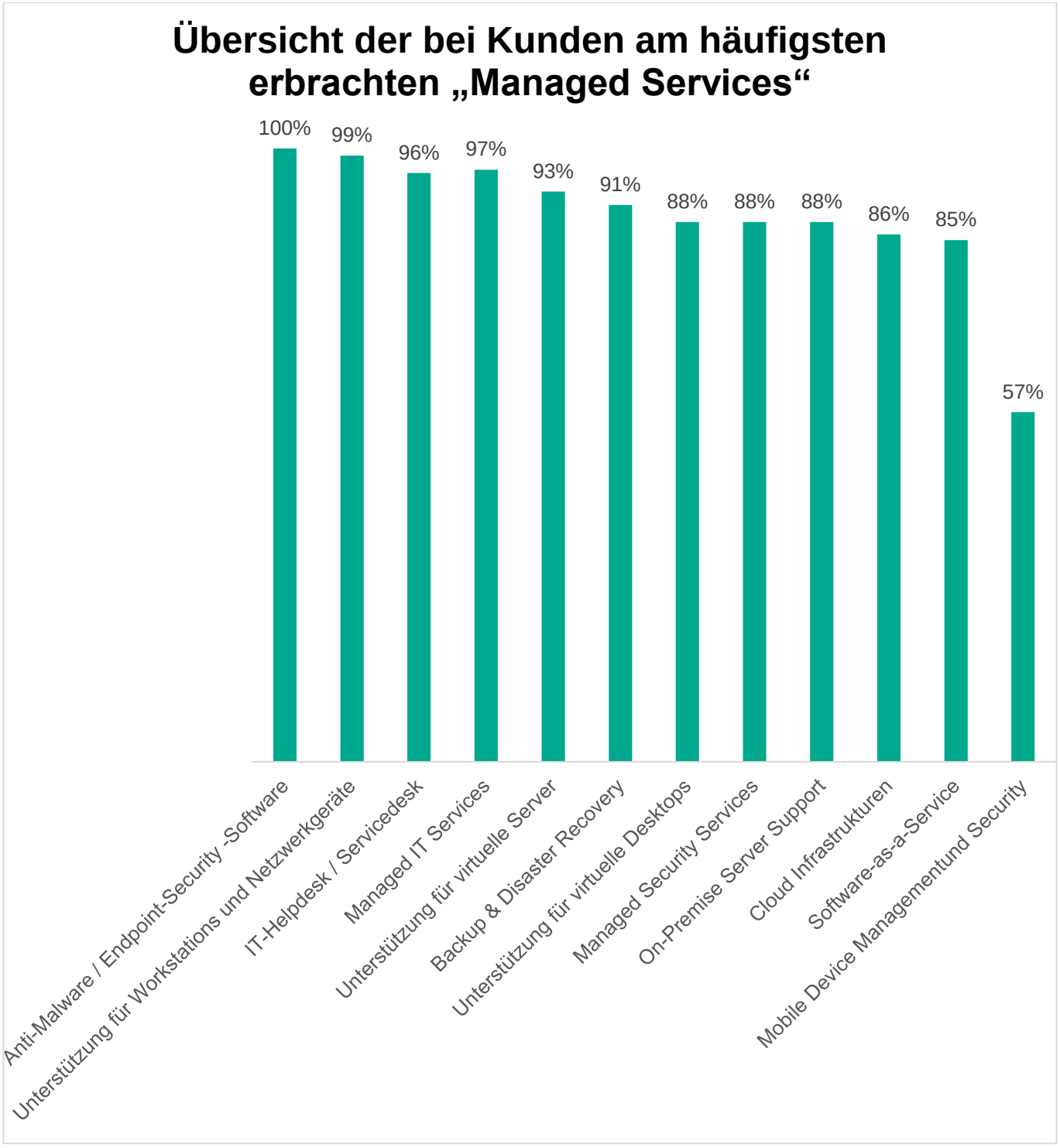


Abbildung 5: Übersicht der bei Kunden am häufigsten erbrachten „Managed Services“

Doch losgelöst von hohen Kundenzahlen, verwaltet etwa ein Viertel (23 Prozent) der MSPs durchschnittlich lediglich zehn bis 25 Geräte pro Auftraggeber. Bei 48 Prozent sind es sogar weniger als zehn Nodes – also Netzwerkknoten – pro Klient.

Beziehungshöhen und -tiefen

Ein wachsender Kundenstamm kann ein zweischneidiges Schwert für MSPs sein. Obwohl Unternehmen ihre Dienstleistungen dringend benötigen, verschärft dies den Wettbewerb auf dem Markt und lässt die Ansprüche der Kunden an Dienstleister größer als jemals zuvor werden. Drei Viertel (75 Prozent) der MSPs geben an, dass anspruchsvolle Kunden und Anwender eine zentrale Herausforderung darstellen; 78 Prozent sprechen gar von einem vermehrten Kampf um neue Kunden und zwei Drittel (68 Prozent) ringen darum, ihre Rentabilität aufrecht zu erhalten.

Das Problem fehlender Einnahmen ist häufig dem Missverhältnis zwischen einem sehr breiten Dienstleistungsportfolio, das von MSPs erwartet wird, aufgrund der geringen Anzahl tatsächlich pro Kunde verwalteter Nodes geschuldet. Um ihren Wert gegenüber Kunden zu steigern und gleichzeitig mehr Umsatzmöglichkeiten zu generieren, könnten MSPs Sicherheitssoftware zu günstigeren Konditionen anbieten, um das Auslagerungsmodell für ihre Kunden kosteneffizienter zu gestalten und sie damit langfristig an sich zu binden.

Da die Zufriedenheit der Auftraggeber bei vielen MSPs im Vordergrund steht, ist es nicht verwunderlich, dass die Kundenbindungswerte für 43 Prozent der MSPs das wichtigste Erfolgskriterium sind, während 41 Prozent sich auf Zufriedenheitsumfragen verlassen, um zu beurteilen, wie gut ihr Geschäft funktioniert. Auf der anderen Seite sind die Messwerte, die auf dem Mehrwert basieren, den MSPs ihren Kunden in Bezug auf Rentabilität (33 Prozent) und Effizienz (20 Prozent) bieten, gering.

Geht es um Strategien zur Kundengewinnung, ist die Mehrheit (83 Prozent) der MSPs zur Vergrößerung ihres Kundenstamms auf Mundpropaganda oder persönliche Empfehlungen angewiesen. Daher ist das Reputationsmanagement in der Akquise für MSPs ein Schlüsselfaktor.

Trotz dieser Herausforderungen prognostizieren MSPs in den kommenden zwei Jahren ein signifikantes Geschäftswachstum, wobei 63 Prozent einen starken Anstieg (bis zu 20 Prozent) erwarten. Diese Prognose spiegelt die aktuelle weltweite Marktentwicklung wider, die eine jährliche Wachstumsrate von 9,3 Prozent [3] voraussagt.

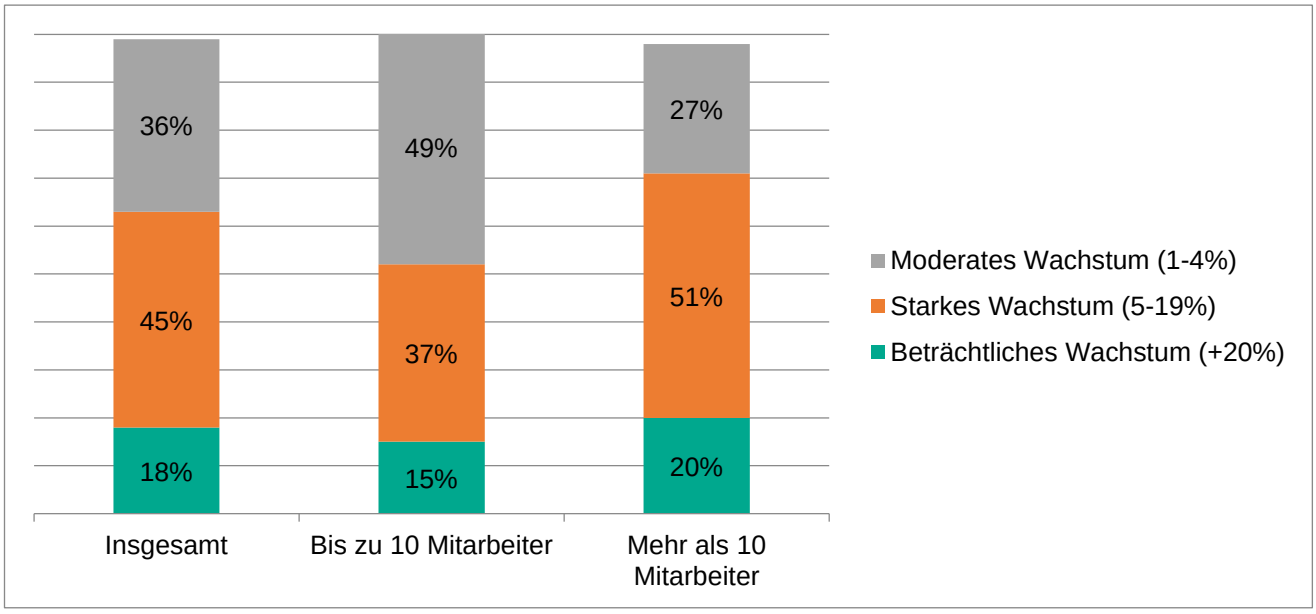


Abbildung 6: Erwartetes Wachstum des MSP-Geschäfts

Der perfekte Sicherheitspartner

Bei vielen Unternehmen steht die Auslagerung des IT-Sicherheitsmanagements ganz oben auf der Geschäftsagenda. Doch wie können MSPs diesen Bedarf kontinuierlich erfüllen und sicherstellen, dass die Lösungen und Dienstleistungen, die sie anbieten, allen gestellten Anforderungen gerecht werden? Bei der Suche nach Partnerschaften mit IT-Sicherheitsanbietern richten sich 92 Prozent der Anbieter von Managed Services nach den Kriterien Reputation und Preisgestaltung. Knapp dahinter folgen die einfache Verwaltung, Integration und der Lizenzeinkauf (88 Prozent).

Die Art und Weise, wie MSPs Lizenzen erwerben, hat auch Auswirkungen auf deren geschäftliches Risiko und ihre potenzielle Vergütung – trägt jedoch dazu bei, dass Dienstleistungen für Kunden schneller und einfacher erbracht werden können. Managed Service Provider bevorzugen insgesamt Flexibilität bei der Lizenzierung, wobei fast die Hälfte (47 Prozent) der Befragten angibt, individuelle Lizenzerwerbsmodelle für jeden Kunden zu präferieren. Wobei sich laut der Kaspersky-Befragung inzwischen 44 Prozent für ein monatliches Abonnementmodell im Bereich IT-Sicherheitssoftware und Dienstleistungen entschieden haben. Beide Optionen bieten MSPs eine gewisse Flexibilität für den Fall, dass ein Kunde wegbricht, so dass Lizenzen insgesamt effizienter verwaltet werden können.

Bei der Entscheidung von MSPs für oder gegen eine Sicherheitslösung beziehungsweise einen Anbieter, sind ein unkomplizierter Erwerb von Lizenzen und die einfache Verwaltung entscheidend. Tatsächlich gab mehr als die Hälfte (56 Prozent) der befragten MSPs an, dass sie ein Anbieter-Lizenzmanagement-Portal verwendet, um Lizenzen zu beziehen. MSPs profitieren darüber hinaus von einer Remote Monitoring and Management (RMM)-Plattform und Professional Service Automation (PSA)-Tools, da sie für die zentrale Überwachung und Verwaltung sowie die Automatisierung alltäglicher Routineaufgaben in andere Softwarelösungen integriert werden können.

Abbildung 7: Haupteinsatzgebiete von RMM-Plattformen bei MSPs

Qualitäten versus Herausforderungen

Wie bei jeder Art von Beziehung, hoffen beide Seiten vom gemeinsamen Miteinander maximal zu profitieren, doch gibt es hierbei natürlich auch unvermeidliche Herausforderungen und Hürden, die es zu überwinden gilt. Geht es um die Erwartungshaltung gegenüber heutigen MSPs, setzen Kunden in erster Linie eine hohe Expertise (84 Prozent) voraus, egal ob für On-Premise- oder Cloud-Infrastrukturlösungen. Sie sollten darüber hinaus in der Lage

sein, bei der Einhaltung von Compliance-Richtlinien und Regulationsbestimmungen zu helfen (82 Prozent), schnell zu reagieren und hohe Service-Level-Agreements einzuhalten (80 Prozent).

Interessanterweise wurde insbesondere die Kompetenz bezüglich Cybersicherheit von 74 Prozent der Kunden, die IT-Managementsupport suchten, als ein Schlüsselmerkmal für MSPs hervorgehoben. Dass diese Anforderung in der Erwartungsliste der Kunden so weit oben steht, zeigt, dass die Fähigkeit, mit der sich rasant entwickelnden Cybersicherheitslandschaft Schritt halten zu können, ein Punkt ist, bei dem Unternehmen zusätzliche Unterstützung benötigen.

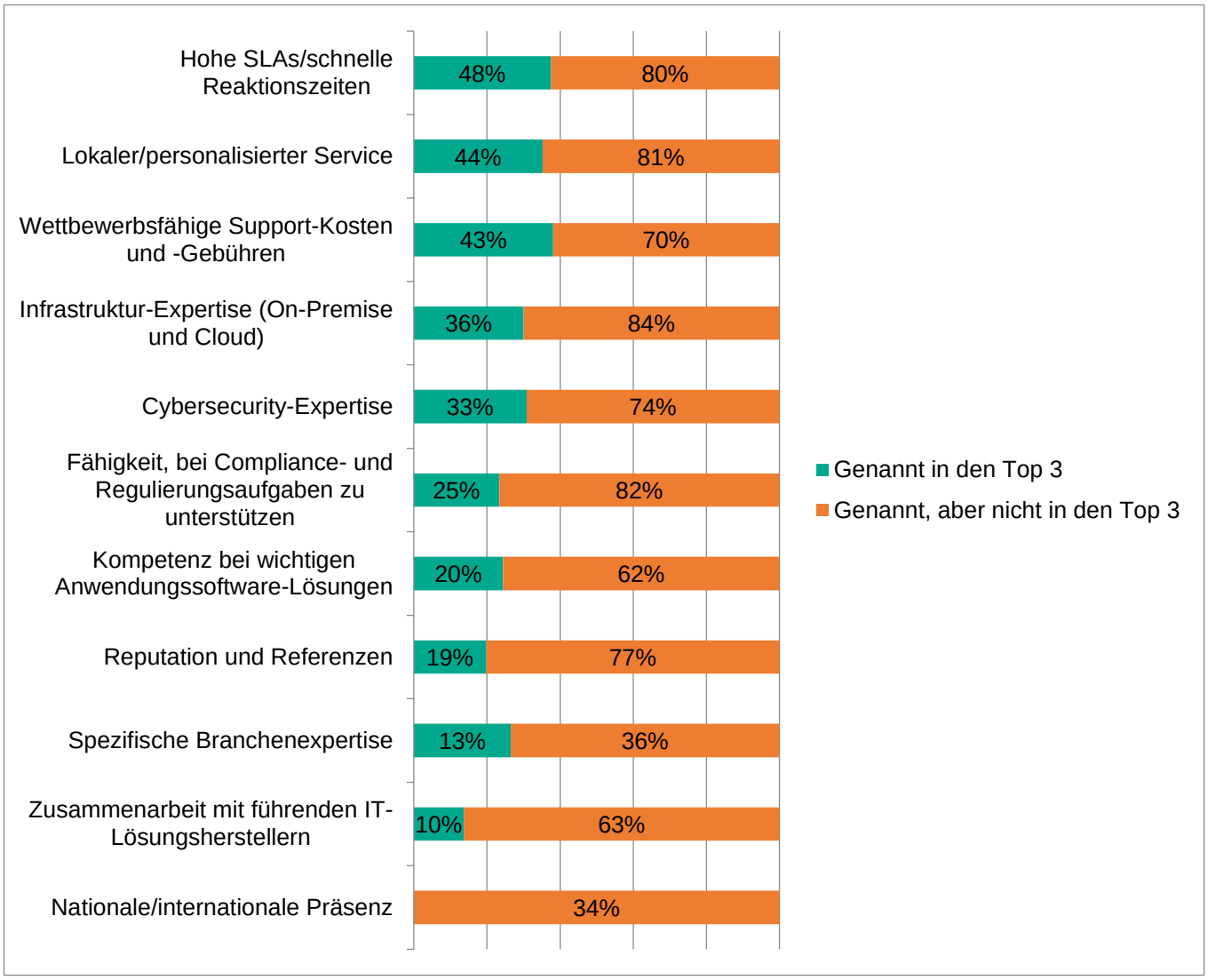


Abbildung 8. Fertigkeiten, die Kunden von MSPs zunehmend erwarten

Zusätzlich zu diesen genannten Anforderungen wird von MSPs erwartet, auch mit unerwarteten Vorfällen und Entwicklungen umgehen zu können – eine weitere Herausforderung, die eigene Vertrauenswürdigkeit und Kompetenz unter Beweis zu stellen. Drei Viertel (78 Prozent) der Kunden erwarten, dass sich MSPs auch mit Themen befassen, die nicht vertraglich vereinbart wurden. Für andere MSPs sind es durch Nutzer entstandene Probleme (65 Prozent) oder die Unfähigkeit, Helpdesk-Prozessen zu folgen (59 Prozent), die Mehraufwand erfordern und Mehrarbeit verursachen.

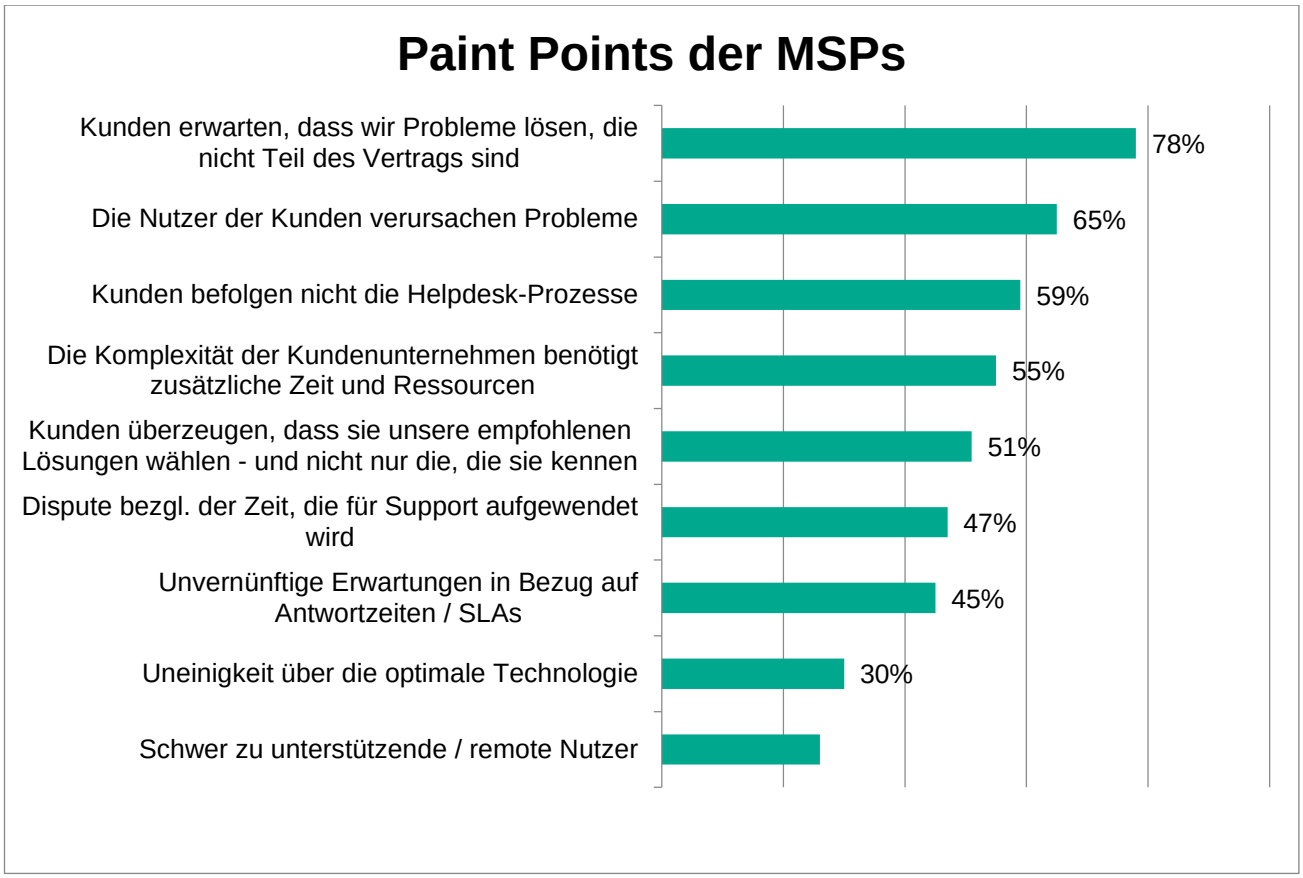


Abbildung 9. Paint Points, denen MSPs ihren Kunden begegnen

Die größte Herausforderung für MSPs stellt jedoch zweifellos die Menge an Cyberangriffen und Malware-Infektionen dar, die zu Ausfallzeiten beim Kunden (72 Prozent) führen, dicht gefolgt von Ransomware-Attacken (65 Prozent). Aber es sind nicht nur externe Bedrohungen, die zu Schwierigkeiten führen können: Auch der Faktor „Mensch“ verursacht weiterhin Probleme. Hierbei erachten 69 Prozent der MSPs Anwenderfehler und das Nichtbefolgen von Sicherheitsrichtlinien als größte Bedrohungen für den Schutz ihrer Kunden.

Was bedeutet das für Managed Service Provider?

Die Auswirkungen eines Sicherheitsvorfalles können – nicht nur für den Kunden, sondern auch für den MSP – weitreichende Folgen haben. So war etwa die jüngste Datenschutzverletzung von Capital One [4], mit über 16 Millionen Betroffenen, auf eine falsch konfigurierte Web-Anwendungs-Firewall von Amazon Web Services (AWS) zurückzuführen. Dennoch wurde diese Schwachstelle nicht gehackt und AWS zugeschrieben, sondern einem Kunden angelastet, der die Cloud-Firewall nicht richtig konfiguriert hatte [5].

Dies ist nur ein Beispiel dafür, wie Dritte im Falle einer – durch Kunden verursachten – Datenpanne in die Schusslinie geraten können. Mit Sicherheit nicht zum letzten Mal. Tatsächlich gaben 43 Prozent der Befragten, die eine Datenschutzverletzung erlitten haben, ihrem MSP die Schuld. Nur 41 Prozent akzeptierten die Verantwortlichkeit eigener Mitarbeiter für einen solchen Vorfall. Noch überraschender ist jedoch die Tatsache, dass ein Viertel (27 Prozent) der Geschädigten den erlittenen Schaden auf mangelndes IT-Sicherheits-Know-how ihres Dienstleisters zurückführten.

Sicherheitsfehler des Kunden können sich jedoch auch auf den zeitlichen Aufwand des MSPs für Problemlösungsaktivitäten auswirken. Dies bestätigen 67 Prozent der Befragten, wobei ein Drittel (38 Prozent) durch den vermehrten Aufwand sogar Geld verloren hat, ohne dass dies auf eigene Fahrlässigkeit oder mangelnde Sachkenntnis zurückzuführen war.

Schlussfolgerungen und Empfehlungen

Offensichtlich sind die Faktoren Kostenreduzierung und optimale Nutzung verfügbarer IT-Budgets die Hauptgründe für Unternehmen, ihr IT-Management auszulagern. Deren Mangel an internen Ressourcen und Fähigkeiten in der IT-Sicherheit eröffnet für MSPs klare Chancen, sich als Cyber-Security-Experten zu profilieren und die Lücke im Sicherheitsmanagement von Unternehmen in ganz Europa zu schließen.

Es ist daher von entscheidender Bedeutung, dass MSPs – um ihren Kunden ein hohes Serviceniveau zu bieten und der wachsenden Nachfrage nach ausgelagerten Sicherheitsdienstleistungen gerecht zu werden – über ein komplettes Set an Know-how und technologischer Ausstattung verfügen. Um neue Kunden zu gewinnen und den Umsatz zu steigern, müssen sie das Repertoire angebotener Dienstleistungen erweitern und sich auf Marktpositionierung und Reputationsmanagement konzentrieren. Nur so sind sie in der Lage, sich gegenüber ihren Mitbewerbern durchzusetzen.

Kunden erwarten von ihrem Managed Service Provider umfassenden Schutz vor Bedrohungen, aber auch Kompetenz in Sachen Informationssicherheit. Mangelnde Sachkenntnis auf diesem Gebiet kann zum Verlust von Kunden führen und die eigene Vertrauenswürdigkeit als Berater und Partner gefährden. Für MSPs ist es unerlässlich, Vertrauen und Kundentreue aufzubauen, was nur mit einer Kombination aus professionellen Tools und dem nötigen Know-how möglich ist – ein essenzieller Baustein, um Kunden bei jedem Schritt innerhalb ihres Business unterstützen zu können.

Die eigene Reputation ist hierbei entscheidend. Nur ein einziger Fehler hat langfristige Auswirkungen auf die Gewinnung und Bindung von Kunden. Für MSPs ist es daher von großem Vorteil, die komplette Bandbreite an Sicherheitsdienstleistungen – unterstützt durch einen starken und zuverlässigen Cybersecurity-Partner – abzudecken. Nur so lassen sich das prognostizierte Marktwachstum realisieren, die Gewinne steigern und die langfristige Stabilität des eigenen Unternehmens gewährleisten.

Cybersicherheitsanbietern kommt bei der Unterstützung von MSPs eine wichtige Rolle zu. Es ist kein Geheimnis, dass MSPs ihre Sicherheitsdienste in den nächsten Jahren erweitern wollen. Anbieter von Sicherheitsaudits, Vorfallreaktionslösungen und E-Mail- oder Web-Gateways werden von den steigenden Anforderungen profitieren.

Sie können hier wichtiges Wissen weitergeben, um beim MSP Fähigkeiten zu verbessern sowie Unterstützung bei Marketing und Vertrieb zu bieten. Das Managed-Service -Provider-Partnerprogramm von Kaspersky [6] bietet beispielsweise spezielle Cybersicherheitsprodukte für MSPs sowie Trainings, Schulungsmaterialien und Veranstaltungen an, die sich an Managed Service Provider richten. Kaspersky verfügt über ein breites Lösungs- und Support-Portfolio für MSPs, das sowohl On-Premise- als auch Cloud-basierte Lösungen bereitstellt – angefangen vom Endpoint-Schutz über die hybride Cloud-Sicherheit bis hin zu E-Mail- und Web-Security. Allesamt in Remote Monitoring and Management (RMM)- sowie Professional Services Automation (PSA)-Plattformen integrierbar, um Service Providern bei der Automatisierung von Routineaufgaben zu helfen. Das Programm umfasst zudem Marketingunterstützung und bietet darüber hinaus finanzielle Vorteile für alle Kaspersky-Partner.

Weitere Informationen zur Kaspersky-Managed-Service Provider-Partnerschaft finden sich unter https://www.kaspersky.de/partners/managed-service-provider .

[1] https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

[2] https://www.marketsandmarkets.com/PressReleases/managed-services.asp

[3] https://www.marketsandmarkets.com/Market-Reports/managed-services-market-1141.html

[4] https://www.tagesschau.de/wirtschaft/capital-one-hacker-101.htm I

[5] https://www.msspalert.com/cybersecurity-news/aws-cloud-cybersecurity-configuration-errors/

[6] https://www.kaspersky.de/partners/managed-service-provider