

WHITEPAPER

Vom MSP zum MSSP

ZUSAMMENFASSUNG

Lohnt es sich, ein Managed Security Service Provider – kurz MSSP – zu werden? Diese Frage treibt derzeit die gesamte IT-Servicebranche um. Doch was genau ist und tut ein MSSP überhaupt? Bringt ein Auftreten unter dieser Bezeichnung Vorteile? Wissen Kunden zwischen „MSP“ und „MSSP“ zu unterscheiden? Über all dies herrscht wenig Klarheit.

Unser Whitepaper beschreibt genauer, was einen echten MSSP-Service ausmacht und welches Geschäftspotenzial er erschließen kann. Es nennt die derzeitigen Defizite vieler Serviceanbieter und erklärt, wie sich diese überwinden lassen.

Im Sommer 2017 fragte SolarWinds MSP über 400 kleine und größere Unternehmen in den USA und Großbritannien zu ihrem Umgang mit Sicherheitsanforderungen und wie sie ihren Serviceanbieter beurteilen.

Das wohl entscheidendste Resultat dieser Umfrage: 80 % der befragten Unternehmen möchten innerhalb der nächsten 12 Monate etwas an ihrem IT-Sicherheitsmanagement verändern, ob es nun ein Wechsel des Serviceanbieters ist, die Rückholung des bisher ausgelagerten Sicherheitsmanagements in den eigenen Betrieb oder umgekehrt seine Auslagerung. Der überraschend hohe Wert von 80 % zeigt, wie stark der Markt für IT-Sicherheit derzeit in Bewegung ist und welche Chancen das Serviceanbietern eröffnet.

Aus der Umfrage ergeben sich insgesamt fünf chancenreiche Kundensegmente:

- i. 60 % der Unternehmen managen die gesamte IT-Sicherheit oder zumindest Teilbereiche davon selbst. Mehr als vier Fünftel (82 %) dieser Gruppe wollen die gesamte Sicherheit in den nächsten 12 Monaten auslagern. Die Hälfte der Wechselwilligen nennt für diese Entscheidung Kostengründe – hier liegt also Geschäftspotenzial für Serviceanbieter mit einer günstigen Kostenstruktur. Diese Unternehmen stellen mit 25 % das größte der hier insgesamt erschließbaren fünf Kundensegmente dar und sind für professionell aufgestellte und entsprechend ausgestattete MSPs mit die attraktivste Zielgruppe.
- ii. Das zweitgrößte Segment umfasst 24 % des Gesamtpotenzials. Diese Unternehmen wollen den Service auslagern, um zu einer insgesamt besseren IT-Sicherheit zu gelangen. Hier können Serviceanbieter mit einer Fach- und Sachkompetenz in der erforderlichen Tiefe und Breite schnell gegenüber der internen IT punkten.
- iii. 10 % der Unternehmen arbeiten beim Sicherheitsmanagement derzeit mit einem externen Anbieter zusammen, möchten die betreffenden Funktionen jedoch wieder ins eigene Unternehmen zurückverlagern. Hier liegt eine Chance für Serviceanbieter, die diesen Unternehmen klarmachen können, dass ihre Unzufriedenheit nicht am Servicemodell der Auslagerung liegt, sondern an ihrem bisherigen Dienstleister, und sie infolgedessen dazu bringen, ihre Pläne zu überdenken.

Unser Whitepaper beschreibt genauer, was einen echten MSSP-Service ausmacht und welches Geschäftspotenzial er erschließen kann. Es nennt die derzeitigen Defizite vieler Serviceanbieter und erklärt, wie sich diese überwinden lassen.

- iv. 9 % der befragten Unternehmen möchten wechseln, weil sie der Meinung sind, der aktuelle Anbieter sei sein Geld nicht wert: Sie möchten also eine bessere Leistung erhalten. Wer mit dieser Zielgruppe ins Geschäft kommen will, muss ein besseres, umfassenderes oder innovativeres Angebot auf den Tisch legen können.
- v. Das letzte Segment sind die 8 % der Unternehmen, die ihre IT-Sicherheit bereits extern betreuen lassen, aber auf der Suche nach einem günstigeren Anbieter sind. Diese Gruppe ist nicht nur die kleinste, sondern auch am wenigsten lukrativ. Wer sie gewinnen möchte, muss den bisherigen Anbieter und andere Konkurrenten unterbieten – unter Umständen bis hin zu einem Punkt, an dem es unrentabel wird. Zwar haben Anbieter mit bereits stark automatisierten Abläufen hier einen Vorteil, da sie preisgünstiger anbieten können, doch Kunden mit Preismotivation bieten kaum Wachstumspotenzial und wandern höchstwahrscheinlich bald wieder ab.

Wie erschließen Sie sich als IT-Serviceanbieter das hier dargestellte Geschäftspotenzial?

Unterm Strich gesagt: indem Sie vom MSP zum MSSP werden. Schließlich geben immerhin 70 % der befragten Unternehmen an, sie würden einen Serviceanbieter, der unter der Bezeichnung „MSSP“ auftritt, positiver beurteilen. Aber wenn „MSSP“ mehr als ein Etikett sein soll, was genau gehört dann dazu?

Von einem echten MSSP-Service kann dann die Rede sein, wenn es eine umfassende und stimmige Palette an Sicherheitsleistungen gibt und der Service zuverlässig, fachlich kompetent und in gut organisierter Weise erbracht wird. SolarWinds MSP unterteilt Sicherheitsleistungen in insgesamt vier Kategorien, die Servicebereitstellung selbst wiederum ruht unserer Meinung nach auf drei Säulen.

So ergeben sich aus vier Kategorien mal drei Säulen insgesamt 12 Leistungsmerkmale, die einen MSSP ausmachen. Mit diesen 12 Merkmalen können Sie potenzielle Kunden davon überzeugen, die Sicherheit ihrer IT in Ihre kompetenten Hände zu legen, anstelle sie selbst zu managen oder bei ihrem bisherigen Anbieter zu bleiben.

70 % der befragten Unternehmen haben bestätigt, sie würden einen Serviceanbieter, der unter der Bezeichnung „MSSP“ auftritt, positiver beurteilen.

Vier Kategorien für Sicherheitsleistungen	Die drei Säulen der Servicebereitstellung
Infrastruktur	Wissen
Identitäts- und Zugriffsmanagement (IAM)	Gute Organisation
Datensicherheit	Technik, Tools und Ressourcen
Risiko- und Schwachstellenmanagement	

Ergo: Der Sprung zum MSSP verschafft Ihnen einen maßgeblichen Wettbewerbsvorteil. Bezeichnenderweise sind es nur 66 % der befragten Unternehmen, die ihrem aktuellen Anbieter ausreichend vertrauen, was die Sicherheit der IT-Infrastruktur angeht – und das, obwohl „Infrastruktur“ in der Umfrage als die kritischste der vier Kategorien eingestuft wird.

Zwischen Leistungsumfang und -qualität der aktuellen Serviceanbieter und den Ansprüchen der Kunden gibt es also eine Diskrepanz. An der lässt sich ablesen, worin genau die Anforderungen für künftige MSSPs bestehen.

Wer also sein Know-how und seine Fertigkeiten und Ressourcen zügig so erweitern kann, dass er sich mit Fug und Recht „MSSP“ nennen kann, wird die Konkurrenz schon bald ausstechen.

WAS IST EIN MANAGED SECURITY SERVICES PROVIDER?

Viele sind der Meinung, „MSSP“ sollte nicht nur ein schönes Etikett für ein bestimmtes IT-Serviceangebot, sondern ein echtes Qualitätsmerkmal sein, das genau definierte Sicherheitsleistungen und ihre Erbringung in einer Zuverlässigkeit und Qualität garantiert, die über dem Niveau eines durchschnittlichen Anbieters liegen.

Leider nennen sich etliche Serviceanbieter „MSSP“, ohne darüber nachzudenken, was das heißt und ob sie die Anforderungen erfüllen – wenn sie sie überhaupt kennen.

Umgekehrt gibt es genügend Anbieter, die das Leistungsspektrum eines MSSP sehr wohl abdecken, ohne sich als solcher zu bezeichnen. Damit verschenken sie den Imagevorteil, der damit einhergeht.

Vielfach ist einfach unklar, welche Merkmale und Services einen IT-Serviceanbieter als MSSP qualifizieren, auch wenn insgesamt durchaus Konsens herrscht, dass hierfür bestimmte Qualifikationen, Prozesse, technische Möglichkeiten und Ressourcen benötigt werden. Nur welche sind es? Hier mangelt es an Klarheit.

Tatsächlich sind es ganz bestimmte Leistungen und Kompetenzen, die ein IT-Serviceanbieter unter der Bezeichnung „MSSP“ erbringen können sollte.

Die oben erwähnten vier Kategorien lassen sich in jeweils drei bis fünf Bausteine untergliedern:

1. Infrastruktur

- Absicherung von Endgeräten
- NOC/SOC-Services
- Firewalls
- Gefahrenerkennung und -analyse
- Absicherung der Netzwerkaußengrenzen

Leider nennen sich etliche Serviceanbieter „MSSP“, ohne darüber nachzudenken, was das heißt und ob sie die Anforderungen erfüllen – wenn sie sie überhaupt kennen.

2. Datensicherheit

- Malware-Abwehr
- Business Continuity/Disaster Recovery
- Forensik
- Whitelisting von Anwendungen, Verhinderung von Datenverlusten
- E-Mail-Sicherheit

3. Risiko- und Schwachstellenmanagement

- Schwachstellen-Scans und Patching
- Penetrationstests
- Überprüfung von Sicherheitsrichtlinien
- Einbruchserkennung

4. Identitäts- und Zugriffsmanagement

- Benutzerzugriff und Verwaltungsrechte
- Daten-Governance
- Authentifizierung und Berechtigung

Für die gute Bereitstellung jeder Servicekategorie sind drei Faktoren ausschlaggebend, die „drei Säulen der Servicebereitstellung“:

1. Wissen

Voraussetzung für ein exzellentes Leistungsniveau ist hier, dass alle Technik- und Beraterteams gleichermaßen solide Kenntnisse und Erfahrungen haben. Wenn Wissen nicht durchgängig verfügbar ist, hemmt das die geschäftliche Expansion und kann beim Weggang bestimmter Mitarbeiter empfindliche Lücken reißen. Wichtige Bereiche sind Bestandsaufnahme, Management, Überwachung, Risikominimierung, Fehlerermittlung und Wiederherstellung.

2. Gute Organisation

Sie basiert auf zuverlässigen Abläufen für die Berichterstattung, Ereignisverfolgung und Verwaltung. Gute Organisation ist nicht nur eine Voraussetzung für die wirksame Servicebereitstellung und die Zufriedenheit von Kunden, sondern legt auch das Fundament für eine ISO- oder ITIL-Zertifizierung.

3. Technik, Tools und Ressourcen

Zu guter Letzt steht und fällt eine gute Servicebereitstellung mit der Wahl der richtigen Tools und ihrem optimalen Einsatz. Ein kluger Personaleinsatz ist hier ebenso wichtig wie Schulungs- und Zertifizierungsmaßnahmen zu allen Tools, Programmen und Ressourcen, die genutzt werden sollen. Viele dieser Zertifizierungen lassen sich direkt bei den Anbietern des jeweiligen Bausteins absolvieren (zum Beispiel RMM oder SIEM).

Aus der Kombination der drei Säulen und vier Kategorien entstehen 12 Leistungsmerkmale, die einen echten MSSP-Service ausmachen:

Die 12 Merkmale eines echten MSSP-Service

			Vier Kategorien für Sicherheitsleistungen			
			Infrastruktur	Datensicherheit	Risiko- und Schwachstellenmanagement	Identitäts- und Zugriffsmanagement
			Absicherung der Endgeräte, NOC/SOC-Services, Firewalls, Gefahrenerkennung und -analyse, Absicherung der Netzwerkaußengrenzen	Malware-Abwehr, Business Continuity/ Disaster Recovery, Forensik, Whitelisting und Verhinderung von Datenverlusten, E-Mail-Sicherheit	Schwachstellen-Scans und Patching, Penetrationstests, Überprüfung von Sicherheitsrichtlinien, Einbruchserkennung	Benutzerzugriff und Verwaltungsrechte, Daten-Governance, Authentifizierung und Berechtigung
Drei Säulen der Servicebereitstellung	Wissen	Solide und umfassende Kenntnisse von Technikern und Beratern	✓	✓	✓	✓
	Gute Organisation	Zuverlässige interne Prozesse und effiziente Servicebereitstellung	✓	✓	✓	✓
	Technik, Tools und Ressourcen	Umfassende technische Ausstattung und erfahrenes Personal	✓	✓	✓	✓

VOM MSP ZUM MSSP: LOHNT SICH DER SCHRITT?

Wie wir gesehen haben, müssen Anbieter für einen seriösen Marktauftritt als MSSP einiges leisten. Welche Geschäftschancen eröffnen sich ihnen damit? Anders gefragt: Lohnt sich der ganze Aufwand am Ende?

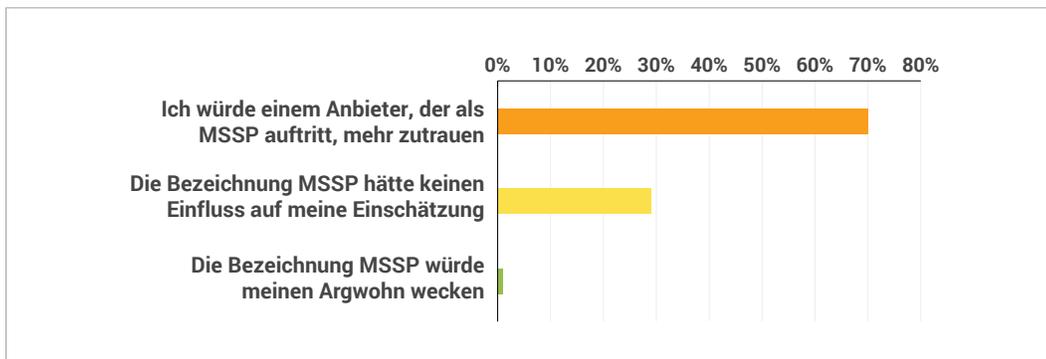
In diesem Zusammenhang hat SolarWinds MSP eine Umfrage durchgeführt. 400 kleine und größere Unternehmen in den USA und Großbritannien sollten sagen, auf welchem Wege sie im Laufe der nächsten 12 Monate für ihre IT-Sicherheit sorgen wollten. Die Analyse der Ergebnisse legt unter anderem offen, welche Anbieter hierfür am besten aufgestellt sind: durchschnittliche MSPs oder echte MSSPs.

Der Markt für IT-Sicherheitsleistungen ist aktuell stark in Bewegung, wie die Umfrage zeigt: Zum einen streben viele Unternehmen Veränderungen in puncto IT-Sicherheit an, zum anderen klaffen zwischen den Erwartungen der Kunden und dem Leistungsspektrum der Anbieter Lücken. In jedem Wandel stecken Chancen. In der IT-Sicherheit scheint diese Binsenweisheit jedoch nur für die „echten“ MSSPs zu gelten.

WIE WICHTIG IST DIE BEZEICHNUNG „MSSP“?

Manche Serviceanbieter halten den Titel „Managed Security Services Provider“ für ein schönes Etikett ohne praktischen Mehrwert. Die Kunden dagegen legen unerwartet großen Wert darauf, wie ein Anbieter sich nennt.

Frage: Hat die Bezeichnung „Managed Security Services Provider“ Einfluss darauf, wie sehr Sie einem Serviceanbieter vertrauen?



Ein überwältigend großer Teil (70 %) der Unternehmen findet einen Anbieter seriöser, wenn dieser ein MSSP ist. Das kann nur eines heißen: MSPs sollten sich darauf konzentrieren, die 12 bereits genannten Leistungsmerkmale zu erfüllen.

Dennoch treibt viele Serviceanbieter die Frage um, ob sie den Weg zum MSSP überhaupt gehen möchten, schließlich eröffnet ein solcher Umbau nicht nur Umsatzchancen in einem Wachstumsmarkt, sondern birgt auch Risiken. Das Zögern ist also durchaus verständlich.

In einer von SolarWinds MSP durchgeführten Umfrage sollten 400 kleine und größere Unternehmen in den USA und Großbritannien sagen, auf welchem Wege sie im Laufe der nächsten 12 Monate für ihre IT-Sicherheit sorgen wollten.

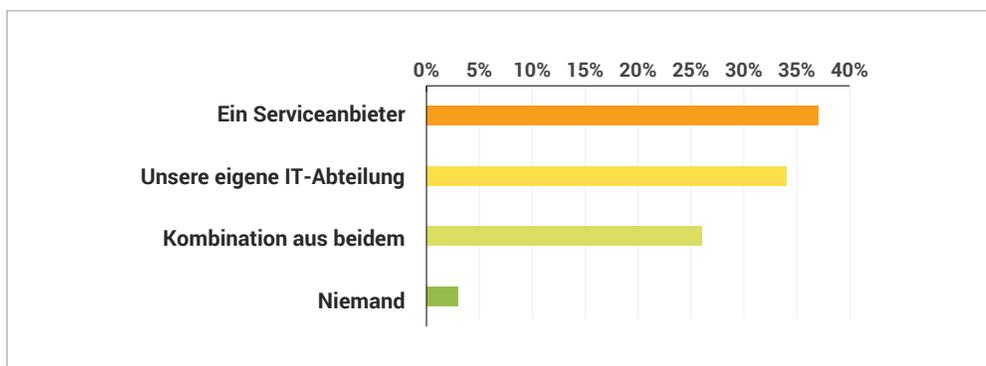
Genau aus diesem Grunde kommt es auf die 12 Leistungsmerkmale an. Alleine das MSSP-Etikett im Namen zu führen, wird auf Dauer nicht tragen: Schnell werden die Kunden feststellen, dass der Anbieter weder das geforderte Servicespektrum aufbringt noch hinreichend kompetente Leistung zeigt – von einer rentablen Ausführung einmal ganz abgesehen.

Wer sein Angebot jedoch auf die 12 Leistungsmerkmale gründet, legt das richtige Fundament dafür, einen Großteil seiner Risiken abzufedern.

MARKTCHANCEN FÜR MSSPS

Gibt es für ein echtes MSSP-Angebot einen Markt? Und ist er groß genug, um den Geschäftsumbau zu rechtfertigen? Wo genau liegen Potenziale, die sich MSSPs erschließen können?

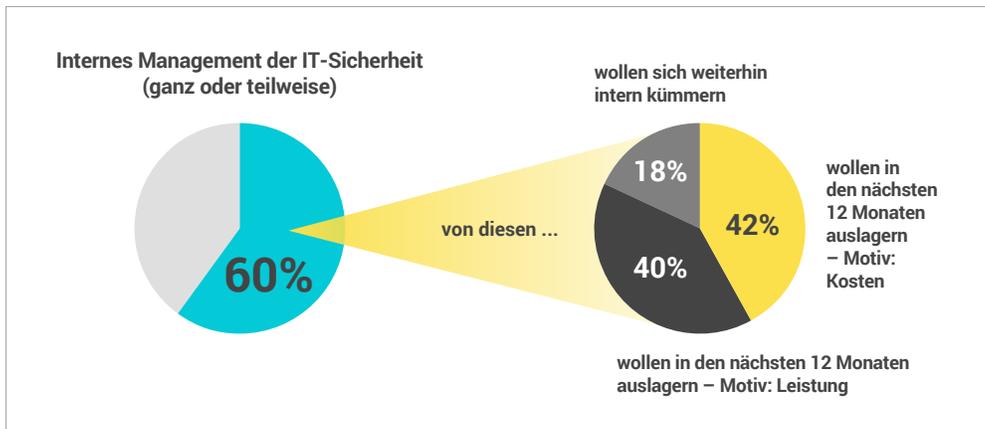
Frage: Wer kümmert sich bei Ihnen aktuell um die IT-Sicherheit?



Die Grafik zeigt nur einen Aspekt der Wirklichkeit, nämlich wie Unternehmen aktuell für ihre IT-Sicherheit sorgen. Hinzu kommt aber ein zweiter Punkt: Ganze 80 % möchten die Serviceerbringung in den nächsten 12 Monaten ändern. In anderen Worten: Für professionelle und gut ausgestattete MSSPs liegt hier ein großes Geschäftspotenzial.

GESCHÄFTSCHANCE 1 – INTERNE IT IST ÜBERFORDERT

Viele Serviceanbieter mag es überraschen: 60 % der Unternehmen managen die gesamte IT-Sicherheit oder zumindest Teilbereiche davon zwar selbst, doch mehr als vier Fünftel (82 %) dieser Gruppe haben die Absicht, die Sicherheit in den nächsten 12 Monaten auszulagern – 42 % aus Kostengründen, 40 % der Leistung wegen.



Unternehmen, die ohne externen Anbieter arbeiten, bilden nicht nur das größte, sondern auch das für MSSPs am einfachsten erschließbare Segment dieses Marktes.

Diese 82 % stellen beachtliche 49 % aller befragten Unternehmen dar. Somit bilden diejenigen, die derzeit ohne externen Anbieter arbeiten, nicht nur das größte Segment dieses Marktes, sondern auch das für MSSPs am einfachsten erschließbare.

All diese Unternehmen haben nämlich ein klares Motiv für die Auslagerung der Sicherheit: Kosten oder Leistungsspektrum. Darauf müssen Sie Ihre Verkaufsbotschaft ausrichten.

» **Kosten**

Anbieter, die ihre Prozesse bereits stark automatisiert haben, sind hier am besten aufgestellt.

» **Leistung**

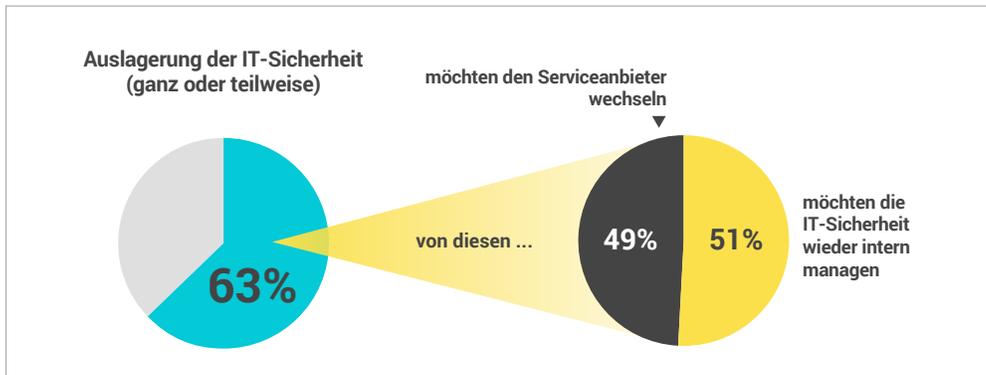
Hier wird überzeugen, wer die vier Kategorien der Sicherheitservices zuverlässig abdecken kann und seine Servicebereitstellung eng an den drei besagten Säulen orientiert.

- **Wissen:** Der Anbieter ist imstande, kompetent zu beraten, und kann Branchenqualifikationen vorweisen.
- **Gute Organisation:** Der Anbieter geht im gesamten Betrieb nach definierten Prozessen und Strukturen vor.
- **Technik, Tools und Ressourcen:** Der Anbieter setzt Spitzentools ein und hat die entsprechenden Zertifizierungen dafür.

GESCHÄFTSCHANCE TYP 2 – MIT DEM AKTUELLEN ANBIETER UNZUFRIEDEN

Nun zum schwierigeren Part: den eigenen Wettbewerbern einen Teil ihres Geschäfts abzufragen.

63 % der Unternehmen haben ihre Sicherheitsfunktionen teilweise oder vollständig ausgelagert. Entscheidend daran ist, dass mehr als die Hälfte (59 %) dieser Gruppe in den nächsten 12 Monaten etwas ändern möchte.



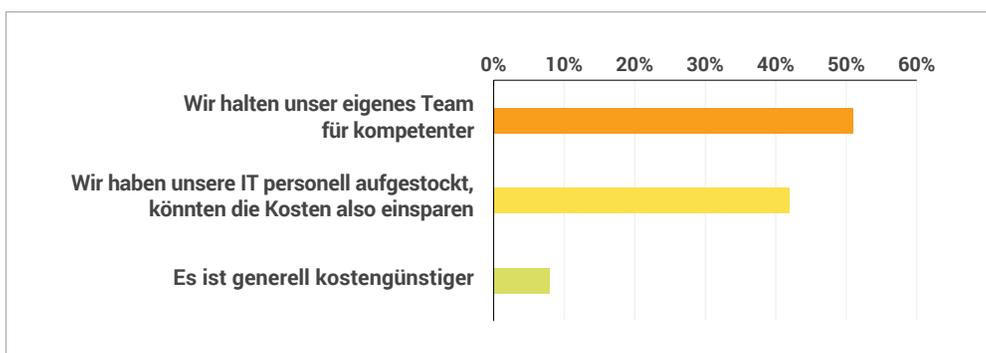
51 % der Unternehmen, die ihre Sicherheit teilweise oder vollständig ausgelagert haben, glauben, die fragliche Leistung selbst besser zu erbringen, oder sind mit dem bisher geleisteten Service insgesamt zu unzufrieden.

An diesem Punkt trennt sich die Zielgruppe in exakt zwei gleiche Hälften: Die eine möchte die IT-Sicherheit wieder ins eigene Haus zurückverlagern, die andere möchte ihren Anbieter wechseln.

Unternehmen, die sich wieder selbst um die IT-Sicherheit kümmern wollen

Diese Zielgruppe birgt durchaus Chancen für MSSPs – so überraschend das auf den ersten Blick klingen mag. Immerhin sagen 51 % in dieser Gruppe, dass sie den externen Anbieter verlassen möchten, weil sie der Meinung sind, die fragliche Leistung selbst besser zu erbringen oder die Unzufriedenheit zu groß geworden ist.

Frage: Aus welchem Grund möchten Sie sich künftig wieder intern um Ihre IT-Sicherheit kümmern?



Der nächste Schritt für Sie als professionellen MSSP ist einfach: Sie müssen diese Zielgruppe überzeugen, dass ihre Unzufriedenheit nicht am Servicemodell der Auslagerung liegt, sondern an den Mängeln ihres bisherigen Dienstleisters. Dass Sie selbst das sehr wohl besser könnten, lässt sich anhand der 12 Leistungsmerkmale mühelos und nachvollziehbar belegen.

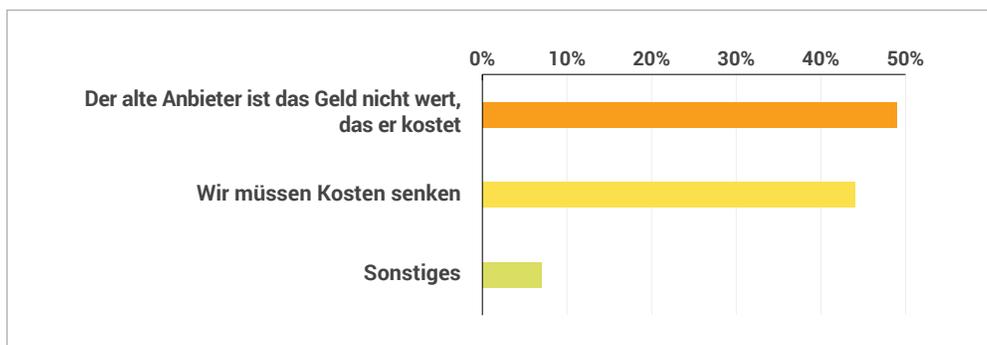
Als weiteres Argument lassen sich bei dieser Gruppe die Zahlen zu Geschäftschance 1 anführen, die belegen, dass sehr viele, die sich intern um die Sicherheit kümmern, früher oder später bei einem externen Anbieter landen, sobald offenbar wird, dass woanders mehr Leistung für weniger Geld zu haben ist.

Der Aufwand, diese Zielgruppe zu erreichen, ist zwar größer, kann sich jedoch lohnen: Unternehmen, die im Begriff sind, ihre Sicherheit wieder ins eigene Haus zu verlegen, machen immerhin 10 % des gesamten Marktpotenzials aus.

Unternehmen, die den Serviceanbieter wechseln möchten

Der zweite Teil der Unternehmen, die mit dem aktuellen Anbieter unzufrieden sind, wird sich nach einem neuen umsehen (49 %). Und wieder gibt es zwei Motive: Kosten und Leistung.

Frage: Aus welchem Grund möchten Sie Ihren bisherigen Serviceanbieter wechseln?



Genau die Hälfte der Unternehmen auf der Suche nach einem neuen Anbieter sagt, der alte sei das Geld nicht wert, das er kostet. Zwar klingt das, als seien Kosten das Motiv, doch eigentlich geht es hier um die Leistung. Die Betroffenen erhalten für die Mittel, die sie aufwenden, nicht den Service, den sie erwartet haben. Wenn Sie hier rein vom Preis her argumentieren, verfehlen Sie den eigentlichen Punkt. Vielmehr sollten Sie Ihr Expertentum in Sachen Sicherheit belegen – anhand der 12 Leistungsmerkmale. Damit präsentieren Sie sich als kompetenter und leistungsfähiger als der bisherige Anbieter. Das ist die beste Voraussetzung, um diese Zielgruppe zu gewinnen.

Die andere Hälfte der Zielgruppe sucht tatsächlich aus rein finanziellen Gründen einen neuen Anbieter, da sie sich den alten nicht mehr leisten können. Mit 8 % des gesamten Marktpotenzials ist dieses Segment das kleinste und das am wenigsten lukrative. Diese Kunden können Sie nur gewinnen, wenn Sie den bisherigen Anbieter sowie andere Konkurrenten so weit unterbieten, dass es für Sie am Ende unrentabel wird. Es liegt auf der Hand, dass die MSSPs mit bereits stark automatisierten Abläufen hier kostengünstiger anbieten können und infolgedessen in der bestmöglichen Position bei dieser Zielgruppe sind. Doch die Erfahrung in der Branche lehrt: Wer Sie nur aufgrund Ihrer günstigen Tarife gewählt hat, bietet Ihnen wenig Wachstumspotenzial und wird den Wert Ihrer Leistung wahrscheinlich bald erneut anzweifeln.

Genau die Hälfte der Unternehmen auf der Suche nach einem neuen Anbieter sagt, der alte sei das Geld nicht wert, das er kostet. Zwar klingt das, als seien Kosten das Motiv, doch eigentlich geht es hier um die Leistung.

Geschäftschancen 1 und 2 Alle Aspekte im Überblick

	Kundengruppe	Situation	Motiv für Änderung	% von Gesamtpotenzial	Lukrativität	So überzeugen Sie
Geschäftschance 1	Interne IT ist überfordert	Der Baustein Sicherheit – derzeit intern abgedeckt – soll innerhalb der nächsten 12 Monate ausgelagert werden.	Kosten	25 %	am höchsten	Heben Sie auf Ihre gute Organisation ab, die Ihnen das Anbieten besonders günstiger Tarife ermöglicht.
			Leistung	24 %	am höchsten	Zeigen Sie (vier Kategorien für Sicherheitservices/ drei Säulen der Servicebereitstellung), dass Umfang und Qualität Ihres Angebots die bisherige Leistung des internen Teams übertrifft.
Geschäftschance 2	Mit dem aktuellen Anbieter unzufrieden	Gruppe 1: Arbeit des externen Anbieters soll in den nächsten 12 Monaten von der internen IT übernommen werden.	Leistung	10 %	gut	Zeigen Sie, dass die Enttäuschung nicht an der Auslagerung an sich liegt, sondern am bisherigen Anbieter, und belegen Sie anhand der 12 Leistungsmerkmale, dass Sie es besser könnten.
			Gruppe 2: Externer Anbieter soll in den nächsten 12 Monaten durch einen neuen ersetzt werden.	Leistung	9 %	durchschnittlich
		Kosten		8 %	am niedrigsten	Überzeugen Sie den Kunden anhand der 12 Leistungsmerkmale, aber machen Sie sich darauf gefasst, dass Sie Ihre Preise senken müssen, um den aktuellen Anbieter zu unterbieten.
	Kundengruppe	Situation	Motiv für Änderung	% von Gesamtpotenzial	Lukrativität	So überzeugen Sie

KÖNNEN AKTUELLE SERVICEANBIETER DIESE GESCHÄFTSCHANCEN FÜR SICH NUTZEN?

Der Überblick auf der vorherigen Seite zeigt: Bei der Erschließung aller fünf Segmente kommt es vorrangig auf die 12 Leistungsmerkmale (4 Kategorien für Sicherheitsservices mal 3 Säulen der Servicebereitstellung) an.

MSSPs, die ihr Geschäft ohnehin entsprechend strukturieren, haben die besten Chancen im Wettbewerb um diese potenziellen Kunden.

Das führt zu der Frage: Auf wie viele Serviceanbieter trifft das aktuell zu? Anders formuliert: Wie groß ist Ihr Wettbewerbsvorteil, wenn Sie Ihren Betrieb zu einem MSSP weiterentwickeln?

Zur Beantwortung dieser Frage hat SolarWinds MSP die Umfrageteilnehmer um Einschätzung der Qualifikation ihrer Anbieter gebeten und insbesondere gefragt, wie viele der 12 Leistungsmerkmale sie erfüllen.

Zu jeder der 4 Kategorien wurde gefragt, ob die Serviceanbieter der Unternehmen

- » ausreichend Sach- und Fachkenntnis besitzen,
- » geeignete organisatorische Abläufe pflegen,
- » für einen ausgezeichneten Service die notwendige Technik, Tools und Ressourcen haben.

(Es ging also darum, ob ihre Servicebereitstellung auf den drei Säulen ruhte.)

Um die potenzielle Auswirkung von Leistungsmängeln zu ermitteln, wurden die Unternehmen gebeten, die vier Kategorien nach Wichtigkeit zu ordnen.

Das Ergebnis ist zwar alarmierend, eröffnet jedoch Anbietern, deren Geschäft auf den 12 Leistungsmerkmalen fußt – echten MSSPs also – gute Geschäftschancen.

LEISTUNGSMÄNGEL

Mit großem Abstand zu den drei folgenden Kategorien wurde „Infrastruktur“ als wichtigste der 4 Kategorien eingestuft. Das erscheint nicht sonderlich überraschend, schließlich sind hier einige der Grundbausteine der IT-Sicherheit – Firewalls, Endpunktsicherheit und NOC/SOC-Services beispielsweise – angesiedelt.

		Wie stark vertrauen Sie Ihrem Serviceanbieter in folgenden Punkten?			
		Fach- und Sachkenntnis <small>% der Befragten, die Kenntnisse ihres Anbieters als „ausgezeichnet“ oder „meinem Anspruch genügend“ einstufen</small>	Gute Organisation <small>% der Befragten, die ihren Anbieter als „ausgezeichnet“ oder „angemessen“ einstufen</small>	Technik und Tools <small>% der Befragten, die ihr Vertrauen als „hoch“ oder „ausreichend“ einstufen</small>	Vertrauen durchschnittlich insgesamt
Priorität aus Unternehmenssicht	Infrastruktur	40 %	76 %	81 %	66 %
	Identitäts- und Zugriffsmanagement (IAM)	49 %	89 %	93 %	77 %
	Datensicherheit	43 %	86 %	87 %	72 %
	Risiko- und Schwachstellenmanagement	46 %	87 %	89 %	74 %

Bei der Frage, welche Kompetenz Unternehmen ihrem Serviceanbieter in den einzelnen Kategorien attestierten, rangierte Infrastruktur durchgängig ganz hinten – gleichfalls mit großem Abstand zu den anderen drei Kategorien. In den „weniger wichtigen“ Bereichen trauten die Befragten ihren Anbietern mehr zu.

In anderen Worten: Serviceanbieter werden als kompetent in den weniger kritischen Bereichen wahrgenommen und als weniger kompetent im kritischsten Bereich.

Dieser Befund könnte seine Ursache darin haben, dass der Bereich Infrastruktur nun einmal sehr umfassend und damit entsprechend schwer abzudecken ist. Vielleicht ist es auch einfach nur so, dass selbst geringfügige Vorfälle und Fehler besser im Gedächtnis bleiben, wenn sie einen derart grundlegenden Bereich betreffen. Nicht auszuschließen ist auch, dass der (falsche) Eindruck der Befragten von ihrem Anbieter auf einer schlichten Fehleinschätzung seiner Kompetenz beruht.

All dies ändert nichts an der folgenden Aussage:

Serviceanbieter, die sich als MSSP aufstellen möchten, um von dem geschilderten Marktpotenzial in den nächsten 12 Monaten zu profitieren, müssen ihre Kompetenzen vorrangig in der Infrastruktursicherheit ausbauen, da Leistungsmängel in diesem Bereich besonders stark abgestraft werden. Ob dies wirklich so ist oder nur der Wahrnehmung der Kunden entspringt, ist dabei unerheblich: In der Servicebranche ist Wahrnehmung gleich Wirklichkeit.

BESSERE SICHERHEITSSERVICES LEISTEN – WIE?

Der Schlüssel für eine verbesserte Bereitstellung von Sicherheitsservices ist eine gute Orientierung an den drei Säulen. Aber wo fangen Sie an? Am schnellsten beheben lassen sich faktische oder wahrgenommene Mängel bei „Wissen“. In der obigen Matrix hat diese Säule die niedrigsten Werte – möglicherweise deshalb, weil sich „Wissen“ nie zweifelsfrei belegen lässt und seine Beurteilung meist stark subjektiv ist.

Wissen entfaltet auch die insgesamt größte Hebelwirkung. Es hat Einfluss auf die Klugheit technischer, personalwirtschaftlicher und organisatorischer Entscheidungen und die Verbesserung von Vertrieb, Marketing und Kundenservice.

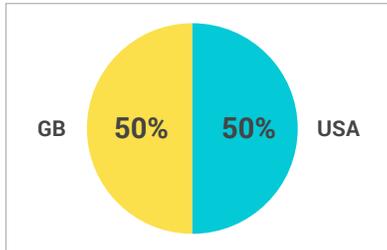
Natürlich ist Wissen ein Ziel, das sich nie endgültig erreichen lässt. Aber wenn Sie als Serviceanbieter stets über die neuesten Bedrohungen und technischen Maßnahmen informiert sind, Ihre Kunden entsprechend beraten und anweisen können und dafür sorgen, dass Ihr Team regelmäßig Zertifizierungen ablegt, dann haben Sie den ersten Schritt hin zum MSSP bereits getan.

Und führen Sie den Titel verdientermaßen, so werden sich Ihnen all die oben genannten Geschäftschancen eröffnen.

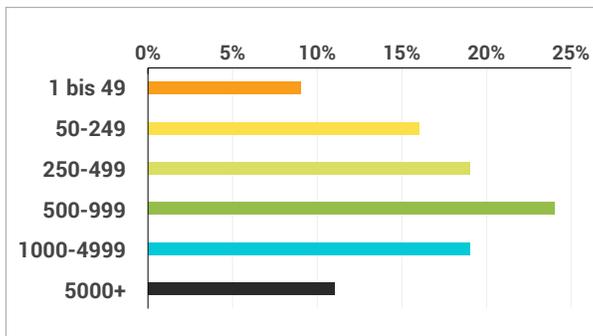
ZUR UMFRAGEMETHODE

Im Sommer 2017 befragte SolarWinds MSP über 400 IT-Entscheider und -Entscheiderinnen in Unternehmen. 50 % der befragten Unternehmen waren KMU, 50 % größere Unternehmen. Eine Hälfte der Unternehmen hatte ihren Sitz in Großbritannien, die andere in den USA.

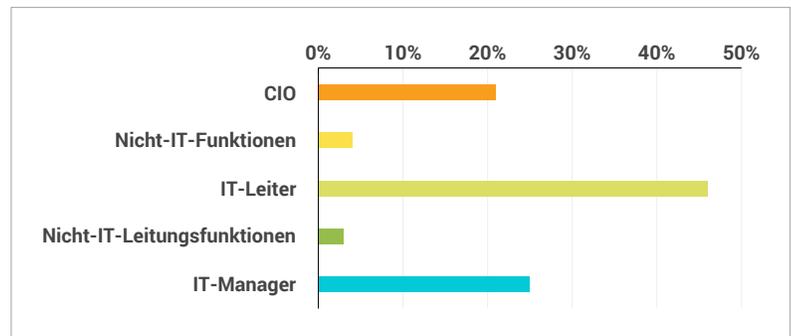
Geografische Verteilung



Verteilung der Unternehmensgrößen (Mitarbeiterzahl)



Verteilung nach Funktionen



MEHRSCICHTIGE SICHERHEIT

KOLLEKTIVE INTELLIGENZ

INTELLIGENTE AUTOMATISIERUNG



SolarWinds MSP unterstützt IT-Serviceanbieter mit Technik für die Erbringung eines professionellen und rentablen Service. Lokal installiert und in der Cloud bieten unsere Lösungen mehrschichtige Sicherheit, kollektive Intelligenz sowie intelligente Automatisierung und schaffen datenbasierte Einblicke, dank derer Provider ihre Arbeit schneller und einfacher erledigen. SolarWinds MSP hilft IT-Anbietern, sich auf das Wesentliche zu konzentrieren: die Erfüllung ihrer SLAs und den Aufbau eines gewinnbringenden Geschäftsmodells.

© 2017 SolarWinds MSP Canada ULC und SolarWinds MSP UK Ltd. Alle Rechte vorbehalten.

Die Marken SolarWinds und SolarWinds MSP sind ausschließlich Eigentum von SolarWinds MSP Canada ULC, SolarWinds MSP UK Ltd. oder seiner verbundenen Unternehmen. Alle anderen hier genannten Marken sind Marken der entsprechenden Eigentümer.

Dieses Dokument enthält generelle Hinweise und dient nur zu Informationszwecken. Es stellt keine Rechtsberatung dar. Die hier dargestellten Informationen und Sichtweisen können sich ändern und/oder treffen nicht notwendigerweise auf Ihre Situation zu. SolarWinds MSP übernimmt weder ausdrücklich noch stillschweigend Gewähr noch Haftung oder Verantwortung für Korrektheit, Vollständigkeit oder Nutzen der in diesem Dokument enthaltenen Informationen. Zur Klärung etwaiger Fragen im Zusammenhang mit Gesetzen und Verordnungen, die in diesem Dokument angesprochen werden, empfehlen wir, den Rat eines Rechtsexperten einzuholen.