SOPHOS
Security made simple.

Erfolgreich zum Next-Gen Managed Security Provider

Wie Sie als IT-Security-MSP im neuen Markt bestehen

Wir erinnern uns noch alle an die alten Zeiten der Managed Service Provider (MSPs). MSPs fungierten als IT-Sicherheitsexperten für Unternehmen, die selbst nicht über entsprechendes Personal verfügten, und verbrachten viel Zeit bei ihren Kunden vor Ort. Sie beurteilten die Anforderungen und Herausforderungen bei der Fehlerbehebung und leisteten den IT-Support, den sich viele Unternehmen nicht leisten oder selbst nicht bewerkstelligen konnten. Auch kam ihnen die wenig beneidenswerte und häufig frustrierende Aufgabe zu, für verschiedene Produktbereiche – Antivirus, E-Mail, Verschlüsselung, Wireless usw. – unterschiedliche Anbieter verwalten zu müssen: Ein zeitraubender Prozess, der für eine komplizierte Abrechnung sorgte und Cashflow-Probleme hervorrief.
Heutige MSPs haben jedoch mit Herausforderungen zu kämpfen, die die alten Zeiten harmlos erscheinen lassen.

Sophos-Whitepaper April 2016

Der Next-Gen MSP

Der Wandel der MSPs hin zum „Next-Gen MSP“ ist nicht zuletzt darauf zurückzuführen, dass sich die Anforderungen auf Kundenseite verändert haben. Die Rolle des MSPs ist in vielen KMUs mittlerweile fest verankert und von zentraler Bedeutung. Bei manchen Kunden übernimmt der MSP sogar die Rolle eines virtuellen CIOs. „Virtuell“ ist beim Thema Next-Gen-MSPs das Schlüsselwort. Besuche vor Ort und normale Geschäftszeiten sind nicht mehr genug – Unternehmen sind darauf angewiesen und erwarten, dass ihr MSP-Support bei Bedarf jederzeit erreichbar ist. Und auch die MSPs selbst müssen von überall mit ihren Kunden in Kontakt treten können. Sowohl Kunde als auch Provider möchten und müssen in der Lage sein, flexibel und mobil zu agieren – ob sie ihre Arbeit nun in einem Büro der herkömmlichen Art oder im heimischen Wohnzimmer erledigen.

Der MSP muss außerdem in der Lage sein, allen Kunden denselben Grad an Service, Sicherheit, Mobilität und Flexibilität bereitzustellen.

Technologische Fortschritte in Hinblick auf Hardware, Software und Benutzeranforderungen haben den Workflow und das Arbeitsumfeld von MSPs komplett verändert. IT-Sicherheit ist komplizierter geworden und MSPs müssen mit immer mehr Fachwissen aufwarten, da Unternehmen zur Verwaltung ihrer Produkte verstärkt auf Cloud-Modelle und webbasierte Ressourcen setzen. Kunden sind nicht mehr an einen Computer, einen Server, einen Standort gebunden und ihre IT-Sicherheitsanforderungen sind demzufolge in die Höhe geschnellt.

Gleichzeitig haben Unternehmenseigner und deren Mitarbeiter ihre Sicherheitsanforderungen drastisch erhöht, weil sie sich vom traditionellen Büro abgekoppelt haben und ihre Arbeit nun mit nach Hause nehmen oder von unterwegs erledigen – und das nicht selten auf mehreren verschiedenen Geräten. MSPs müssen nun in der Lage sein, nicht nur Desktop-Computer zu schützen, sondern auch Laptops, die von einem Standort zum nächsten wandern, Tablets, die sich einfach überall mithinnehmen lassen, und Smartphones, die Datenvolumen verarbeiten können, die früher nur von einem Desktop-PC zu bewältigen waren.

Benutzer haben die Sicherheitsanforderungen komplexer gemacht, indem sie ihren Workflow verändert und ein mobileres Geschäftsumfeld geschaffen haben. Und Cyberkriminelle haben einen noch größeren Entwicklungsschritt vollzogen. Es geht nicht mehr darum, eine Festplatte zu stehlen und kaputtzuschlagen, um an die Daten zu gelangen. Hacker und Diebe bedienen sich immer raffinierterer Methoden und wenden subtilere Taktiken wie Phishingroutinen und Crimeware an, um an wichtige Daten zu gelangen. Oder sie sperren Benutzer mit Ransomware von ihren Dateien aus und erpressen zur Freigabe der Daten ein Lösegeld.

Solche geschickteren Angriffe in Kombination mit steigender Online-Präsenz und der ewig währenden menschlichen Fehleranfälligkeit führen dazu, dass heutige MPSs mehr Einsatz zeigen müssen denn je, um die Anforderungen ihrer Kunden zu erfüllen. Die Endbenutzer ihrer Kunden werden nicht nur von Phishingroutinen heimgesucht, die hinterlistig genug sind, um selbst aufgeklärte Benutzer hinters Licht zu führen. Sie nutzen auch zwei, drei oder noch mehr Geräte oder Tools, um auf Unternehmensdaten zuzugreifen, und bieten damit eine größere Angriffsfläche als früher.

In dieser neuen und weit komplexeren Umgebung erfolgreich bestehen zu können, wird für MSPs immer schwieriger. Die Vielzahl der Anbieter und Produkte, die MSPs benötigen, um die gesamte Palette erforderlicher Service-Leistungen abzudecken, war schon immer eine Belastung. Aber in der schnelllebigen Umgebung von heute hat sich die Verwaltung dieser Anbieter zum kostspieligen Zeitfresser entwickelt. MSPs arbeiten mit einem begrenzten Budget und müssen entscheiden, wo ihr Budget am besten angelegt ist.

Außerdem geht der Trend bei MSP-Services von Langzeitverträgen (waren bislang die Norm) hin zu Subscription-Modellen – ein Wandel, dem sich MSPs in der Next-Gen-Ära anpassen müssen. Dieser Trend wirkt sich auch auf den Anbieter aus, da die meisten Anbieter-Services als unbefristete und nicht monatliche Lizenzen angeboten werden und demzufolge verhindern, dass MSPs ihre Abrechnung einheitlich gestalten können. Dies hat Folgen für den Cashflow – sowohl beim MSP als auch beim Anbieter.

MSPs haben jedoch Möglichkeiten, Kosten zu sparen: Sie können Lizenzen z. B. in großen Mengen über einen Aggregator beziehen, was für eine gewisse finanzielle Entlastung sorgt.

Wie werde ich ein erfolgreicher MSP in der Next-Gen-Ära?

Was also muss ein MSP tun, um im aktuellen Markt erfolgreich bestehen zu können? Der Trick besteht darin, sich mit seinem Angebot von der Konkurrenz abzusetzen.

Werden Sie zum virtuellen CIO

Kunden vertrauen ihrem MSP ihr wichtigstes Unternehmensgut an - nämlich ihre Daten. Ein erfolgreicher MSP sollte in der Lage sein, den Kunden sowohl auf hoch fachlicher Ebene als auch auf Benutzerebene zu beraten und als Ansprechpartner für Fragen bezüglich Hardware, Software usw. zur Verfügung stehen.

Bieten Sie besseren Service als die Konkurrenz

Erfüllen Sie die Anforderungen moderner Kunden, indem Sie jederzeit und überall erreichbar sind —über eine SaaS-basierte Management-Konsole. Die geeigneten Tools verschaffen Ihnen die Flexibilität, um mit der Mobilität Ihrer Kunden Schritt zu halten.

Next-Gen MSPs müssen ihre Sicherheitsstrategie auf die Anbieter ausrichten. Gleichzeitig müssen die Anbieter sich stärker in das MSP-Anbieter-Ökosystem integrieren und Tools entwickeln und bereitstellen, die MSPs nutzen können, um ihren Geschäftsbetrieb am Laufen zu halten (PSA) und Remote-Monitoring und -Management (RMM) für ihre Kunden zu leisten.

Heben Sie sich mit bewährter Sicherheit von der Konkurrenz ab

Stellen Sie sicher, dass Ihre Tools branchenführende Sicherheit und erstklassigen Schutz bieten. Wenn Sie Ihre Kunden zuverlässig vor Bedrohungen von außen abschirmen, können diese ihren Benutzern einen sicheren, unterbrechungsfreien Service bereitstellen. MSPs, die den richtigen Anbieter für eine Zusammenarbeit finden und von diesem entsprechend geschult werden, damit sie die Tools den Anbieters optimal nutzen und vermarkten können, sind in der Lage, ihre Kunden umfassend vor Cyberbedrohungen zu schützen.

Arbeiten Sie effizienter und reichen Sie diese Effizienz an Ihre Kunden weiter

Konzentrieren Sie sich auf das Wesentliche. Sie können z. B. die Anzahl Ihrer Anbieter-Partnerschaften reduzieren, um Ihr Anbieter-Management zu optimieren, und Ihre eigene Effizienz steigern, indem Sie so wenig verschiedene Tools wie möglich verwenden, um die Anforderungen Ihrer Kunden zu erfüllen. Wenn Sie einen geeigneten Aggregationspartner finden – oder noch besser einen Anbieter, der die Technologien, die Sie über ihn lizenzieren, selbst entwickelt (kann eine weitaus effizientere Option sein als ein „Marktplatz" oder Aggregator) – können Sie ein breites Spektrum optimal integrierter und aufeinander abgestimmter Services anbieten und viele manuelle Arbeitsschritte zur Aktualisierung und Verwaltung von Sicherheitsservices entfallen.

Eine weitere Methode zur Effizienzsteigerung: Optimieren Sie Ihre Lizenzverwaltung. Wenn Sie sich für ein Abrechnungs- und Lizenzmodell entscheiden, bei dem Sie Lizenzen flexibler auf verschiedene Kunden verteilen können – wie ein Modell zur aggregierten monatliche Abrechnung – können Sie die von Ihnen angebotenen Services beschleunigen und besser auf wechselnde Kundenanforderungen reagieren.

Gestalten Sie Ihre Abrechnung effizienter

Das alte Paradigma jährlicher Verträge für Anbieter-Services erweist sich in der von ständigen Änderungen geprägten Welt der Next-Gen MSPs als nicht mehr effizient. Wenn Sie Ihren Kunden monatliche Rechnungen schicken, sollte Sie in der Lage sein, auch Ihre eigenen Rechnungen monatlich zu begleichen.

Ein Hinweis zu Aggregationsservices: MSPs, die mit verschiedenen Anbietern zusammenarbeiten, zahlen für Lizenzen meist pro Gerät und Service – für einen Benutzer fallen also jeweils separate Lizenzgebühren für Smartphone, Laptop, Tablet usw. an. Mit dem richtigen Anbieter, der das MSP-Modell versteht, kann der MSP auf Benutzerbasis für die Gesamtzahl der Services zahlen und ist damit in der Lage, weit flexibler auf die Anforderungen des Kunden einzugehen – unabhängig davon, wie viele Geräte ein Benutzer besitzt.

Jetzt neu: Sophos MSP Connect

Mit dem umfangreichen Service-Portfolio von Sophos können Sie im Rahmen unseres MSP-Security-Programms Endpoint-, Email-, Web-, Mobile-, Wireless-, Netzwerk-/Firewall- und Server-Lösungen über einen einzigen Anbieter-Partner beziehen. Sie müssen also nicht mehr verschiedene Anbieter-Beziehungen pflegen oder eine Vielzahl von Verträgen im Auge behalten. Weil alle Produkte von Sophos stammen, sind sie für eine optimale Schutzleistung vollständig integriert, sodass Sie Sicherheitslösungen mit maximaler Leistungsstärke anbieten können.

Das Sophos MSP Connect Programm vereint 30 Jahre Branchenerfahrung mit bewährten Sicherheitsfunktionen zum Schutz vor opportunistischen und gezielten Sicherheitsrisiken.

Die Endpoint- und Netzwerklösungen, die Sie Ihren Kunden anbieten, sind nicht nur in eine zentrale Plattform integriert. Ihnen werden auch alle Sicherheitslizenzen und Kundeninformationen in einem zentralen Verwaltungs-Dashboard angezeigt. Ein Jonglieren zwischen verschiedenen Tools und Verwaltungsressourcen ist nicht mehr notwendig. Über einen einzigen, kompletten Mechanismus und ein zentrales Tool behalten Sie den Status Ihrer Kunden und alle Risiken im Blick und können schnell auf Bedrohungen reagieren.

Sophos ist zu 100 % dem Channel verpflichtet. MSPs erwerben partnereigene Lizenzen und müssen diese Lizenzen demzufolge nur einmal kaufen. Sie können die Lizenzen dann auf verschiedene Kunden verteilen und müssen nicht mehr eine Vielzahl von Transaktionen abwickeln, um die Anforderungen Ihrer Kunden zu erfüllen.

Mit Sophos MSP Connect erhalten Sie zudem eine monatliche Rechnung, also genau wie Sie auch Ihre eigenen Kunden Services in Rechnung stellen.

Sophos ist bereits marktführend bei Next-Gen-Sicherheit. Mit Sophos MSP Connect können MSPs dieses Know-how nun nutzen, um ihren Benutzern erstklassige Sicherheit, niedrigere Betriebskosten und höhere operative Effizienz zu bieten. Ein erfolgreicher Next-Gen MSP dient Unternehmen als virtuelle leitende Hand, die ihnen besten Service, beste Sicherheit und maximale Effizienz zum lukrativen Preis bietet. Mit Sophos MSP kein Problem!

Weitere Infos zum Sophos-MSP-Programm unter www.sophos.de/MSP

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

04.05.2016 WP-DE (MP)

SOPHOS