Von Stagnation zum Erfolg: Wie Sie als MSP wettbewerbsfähig bleiben

Profitieren Sie von den Vorteilen eines sicherheitszentrierten IT-Service Modells

MSP
Barracuda
Your journey, secured.

Mehr Fokus durch verlagerte Dienstleistungen

In den letzten Jahren wurde der MSP Markt zunehmend gesättigt. Traditioneller IT-Support nach dem Break/Fix Modell ist nicht mehr ausreichend, um die ansteigende Zahl von was sind mündige verbraucher? falsche Übersetzung zu beeindrucken. Aufgrund der hohen Anzahl von Anbietern, die ähnliche Dienstleistungen anbieten, ist es notwendig, sich als MSP zu differenzieren, um wettbewerbsfähig zu bleiben.

Da sich die Bedrohungslandschaft kontinuierlich weiterentwickelt und täglich anspruchsvoller wird, beginnen Nur Enduser Ihre Cybersicherheit zu priorisieren. MSPs sollten ihr Angebot für IT-Sicherheit ausbauen, um der wachsenden Nachfrage entgegenzukommen und sich gleichzeitig aus der Masse von Anbietern hervorzuheben.

In diesem Handbuch erklären wir, wie Ihr MSP von einer sicherheitszentrierten Ausrichtung profitieren kann und legen dar, wie Sie beginnen Ihr Angebotsportfolio zu verstärken und diversifizieren. Wir untersuchen:

- Wie Sie der sinkenden Nachfrage nach technischem Support entgegenwirken
- Wie Sie davon profitieren können, ein MSSP zu werden
- Die drei grundlegenden Elemente eines sicherheitszentrierten Service Modells
- Die Vorteile des Barracuda MSPs' Sicherheitspaketes

Warum erleben wir einen massiven Rückgang in der Nachfrage Nachfragerückgang nach IT-Support?

Das Konzept des IT-Supports bezeichnet die Auslagerung von technischer Unterstützung und IT-Dienstleistungen zu einer fachkundigen Drittpartei. Aber warum sinkt die Nachfrage nach IT-Support, wenn Firmen doch so angewiesen auf ihre IT-Infrastruktur sind?

Die Antwort liegt, wenig überraschend, in der Entwicklung von Technologie. In der Anfangszeit von MSPs waren Firmen wenig souverän in Ihrem Umgang mit IT, was bedeutete, dass sie auf fachliches Wissen von Experten zurückgreifen mussten, um betriebsfähig zu bleiben. Im Laufe der Jahre haben Firmen allerdings ein besseres Verständnis von ihrer Technik erhalten und sind in der Lage, die tagtägliche Verwaltung ihrer IT intern zu übernehmen. Heutzutage ist Technologie massgeblich für den Firmenerfolg für Firmenerfolg, was dazu führt, dass traditionelle Break/Fix Modelle nahezu komplett überholt sind. Auf Probleme zu warten, bevor man sie behebt, ist nicht nur ineffizient, sondern führt auch zu anderen Hindernissen, Ausfallzeiten, Umsatzverlusten und erheblichen Frustrationen.

Traditionelle IT-Support Anbieter bieten außerdem wenig durchgängige Überwachung von Sicherheitswarnungen an und legen keinen Schwerpunkt auf Cybersicherheit. In der wachsenden Bedrohungslandschaft setzt dies Firmen großen Sicherheitsrisiken aus. Daher müssen MSPs ein proaktives, sicherheitszentriertes Service Modell adaptieren, um zu vermeiden, stabile Kundenbeziehungen zu verlieren.

Die Lösung: Managed Cyber Security Services

Als MSP wissen Sie, dass sich die Bedrohungslandschaft konstant entwickelt. Dank der hohen Frequenz von Nachrichten über Cyberangriffe in den Medien können Sie davon ausgehen, dass sich Ihre Kunden dem Bedarf der Cybersicherheit auch bewusst sind. Um als MSP größeren Mehrwert aufzuweisen, können Sie Managed Cyber Security Services zu Ihrem Angebotsportfolio hinzufügen. Dies wird Ihnen helfen, sich von der Konkurrenz abzuheben.

Cybersicherheit ist nicht mehr nur für große Unternehmen relevant. Die letzten Jahre haben verdeutlicht, dass Firmen jeder Größe Cyberattacken ausgesetzt sind. Die nachfolgenden Statistiken heben die steigende Nachfrage nach Cyber Security Services unter kleineren und mittelständischen Unternehmen vor.

43% der Cyberangriffen zielen ab auf KMUs.

Source: Ponemon Institute

66% der Kleinunternehmen haben in den letzten 12 Monaten einen Cyberangriff erlebt.

Source: Ponemon Institute

40% der Kleinunternehmen, die eine Cyberattacke erlebt haben, hatten Ausfallzeiten von mindestens 8 Stunden.

Source: Cybersecurity Magazine

83% der kleinen und mittelständischen Unternehmen sind nicht finanziell vorbereitet, um sich von einer Cyberattacke zu erholen.

Source: Cybersecurity Magazine

9 von 10 Kleinunternehmen würde erwägen, ihren IT-Dienstleister zu wechseln, falls Sie einen neuen Anbieter mit besseren Cyber Security Services finden.

Source: Connectwise

Aufgrund der sich ständig entwickelnden Bedrohungslandschaft werden Ihre Kunden immer auf neue Cyber Security Lösungen oder Modernisierung Ihrer existierenden Lösungen angewiesen sein. Wenn Sie Managed Cyber Security Services zu Ihrem Angebotsportfolio hinzufügen, werden Sie immer Cross oder Upsell Möglichkeiten für zusätzliche Security Lösungen haben, was Ihre Rentabilität und Skalierbarkeit steigert.

Die Einführung des MSSPs

Falls Sie ernsthaft überlegen, auf ein sicherheitszentriertes Service Modell umzustellen, sollten Sie erwägen ein Managed Security Service Provider (MSSP) zu werden.

Ein MSSP ist ein ausgelagerter Anbieter, der Unternehmen mit einem kompletten Cyber Security Services Paket ausstattet. Im Gegensatz zu traditionellen MSPs ist das Herzstück eines MSSPs die Sicherheitszentrierung. In Zusammenarbeit mit zuverlässigen Partnern, um Zugang zu marktführenden Programmen und Lösungen zu erlangen, bieten MSSPs die durchgängige Überwachung und Verwaltung der Sicherheitssysteme und Geräte eines Unternehmens an. Ein MSSP zielt darauf ab, Risiken abzuschwächen, Schwachstellen zu eliminieren, Bedrohungen zu minimieren und gleichzeitig zu berücksichtigen, den Geschäftsbetrieb ihrer Kunden nicht zu beeinträchtigen.

Die geläufigsten Dienstleistungen, die MSSPs anbieten, umfassen unter anderem:

- **Remote Monitoring und Management (RMM)**
- **Email Security**
- **Expanded Threat Detection und Response (XDR)**
- **Netzwerk und Cloud Sicherheit**
- **Datenschutz**
- **Managed Firewall**
- **Intrusion Detection**
- **Identifizierung von Schwachstellen**
- **Antivirus Dienstleistungen**

Falls Ihr MSP bereits sicherheitsbewusst ist und Sie nach einem bedeutungsvollen Unterscheidungsmerkmal suchen, ist es der nächste logische Schritt, ein MSSP zu werden. Einen sicherheitszentrierten Ausblick zu entwickeln wird Ihnen nicht nur dabei helfen, neue Geschäftsperspektiven zu entwickeln, sondern gleichzeitig im Angesicht einer schwankenden Nachfrage auch wichtige Kunden zu halten.

Die drei grundlegenden Elemente eines sicherheitszentrierten Service Modells

Um ein MSSP zu werden, müssen Sie andere Schriftart nicht fett Sicherheitsstrategie entwickeln, die definiert, welchen Schutz Sie Ihren Kunden bieten. Jedes Unternehmen, das Sie beauftragt, wird viele verschiedene Bedrohungsstellen haben. Um erfolgreich die Daten und Anlagen eines Unternehmens zu schützen, müssen Sie deshalb einen vielschichtigen, optimal integrierten Sicherheitsansatz implementieren.

Wir von Barracuda MSP empfehlen, Ihren Ansatz in drei grundlegende Elemente der Sicherheit aufzuteilen, um so zu gewährleisten, dass Sie die wichtigsten potentiellen Schwachstellen eines Unternehmens adressieren.

1. Schutz von Benutzern, Informationen, Anwendungen und Geräten

Da sich die Technologie kontinuierlich entwickelt, Unternehmen nun in der Lage, zunehmend mobile Vorgehensweisen für den Arbeitsalltag einzusetzen. Die Einführung der Cloud hat extrem flexible Betriebsmöglichkeiten eröffnet und hybrides und Fernarbeiten begünstigt den Aufschwung von Maßnahmen wie Bring Your Own Device (BYOD). Während diese neuen Betriebsmodelle und technologischen Fortschritte zu offensichtlichen Produktivitätssteigerungen führen, werfen sie allerdings auch signifikante Sicherheitsbedenken auf.

Als MSSP ist es nicht mehr ausreichend, die Geräte und Anwendungen lediglich mit Lösungen wie Antivirus Software und Multi-Faktor Authentifizierung (MFA) zu schützen. Obwohl diese Lösungen natürlich noch äußerst wichtig sind, müssen Sie Ihre Prozesse der sich entwickelnden technischen Umgebung anpassen. Unternehmensdaten werden heutzutage in Netzwerken, Clouds und auf Geräten gespeichert. Dies bedarf ausreichendem Datenschutz und Verschlüsselung auf allen Ebenen, sowie im Transfer als auch im Ruhezustand.

Da menschliches Versagen die Ursache von 95% der Cyberattacken ist, müssen Sie auch Benutzer vor sich selbst schützen. Neben Mitarbeiterschulungen ist es außerdem notwendig, Sicherheitslösungen einzusetzen, die verhindern, dass Benutzer auf Malware zugreifen können, ohne aber ihren tagtäglichen Betrieb oder Prozesse einzuschränken.

2. Bereitstellung von sicherem Zugang zu Public Cloud Plattformen

In den letzten Jahren ist die Adaption der Cloud in Unternehmen sprunghaft angestiegen. Allerdings verwendet die Mehrzahl von Unternehmen die Public Cloud: Im Besitz und betrieben von Drittparteien. Um daher sicherzustellen, dass Ihre Kunden sicher in ihrer Cloud Umgebung agieren können, sollten Sie Sicherheitsregelungen der Plattform prüfen und Ihren Kunden potentielle Schwachstellen oder Veränderungen melden. Sie müssen außerdem sicher gehen, dass End-zu-End Verschlüsselung vorhanden ist, um Kundendaten in der Cloud zu schützen.

3. Kontinuierlicher Fortschritt von Sicherheitsfähigkeiten

Dank der sich kontinuierlich weiterentwickelnden Cyber-Bedrohungen müssen Sie gewährleisten, dass Ihre Sicherheitslösungen in der Lage sind, dem dynamischen Umfeld standzuhalten. Das bedeutet, sicherzustellen dass Sie Ihre Lösungen laufend modernisieren und dass Sie Zero-Day Fähigkeiten einführen, um neue Bedrohungen identifizieren und beheben zu können. Sie können Ihre Kunden außerdem unterstützten, indem Sie regelmäßige Sicherheitsbewertungen durchführen, die gewährleisten, dass ihr Sicherheitsniveau neuen Bedrohungen standhalten kann.

Das Barracuda MSP Sicherheitspaket

Um als MSSP die effektivsten Dienstleistungen bieten zu können, sollten Sie ergänzende, integrierte Sicherheitslösungen verwenden. Barracuda MSP bietet ein branchenführendes Komplettpaket an, das Ihre Bereitstellung von innovativen, robusten Sicherheitsleistungen unterstützt. Mit den unterstehenden Leistungen können Sie einfach und effizient umfassenden Schutz bieten.

Extended Detection and Response (XDR)

Garantieren Sie, dass die Endpunkte Ihrer Kunden vollständig gesichert sind dank unseres KI-angetriebenen Managed Detection und Response Systems, welches von einem 24x7 Security Operations Center (SOC) unterstützt wird. Sie und Ihre Kunden finden ein Stück Seelenfrieden durch:

- **Kompletten Endpunkt Schutz**
- **Verwaltung durch zentralen Knotenpunkt**
- **In Zusammenhang gesetzte Bedrohungserkennung**
- **24/7 Bedrohungserkennung und Reaktion**
- **Behebung durch einen Klick**

Tel: +44 (0) 1256 833400 | BarracudaMSP.com

Email Security

91% aller Cyberangriffe beginnen mit einer Phishing-Mail, was sie zu einer der stärksten und gefährlichsten Bedrohungen macht. Mit einem vielschichtigen Email Security Ansatz erlaubt Barracuda Total E-Mail Protection für MSPs Ihnen, die Posteingänge Ihrer Kunden gegen alle Formen von E-Mail-Bedrohungen zu schützen, einschließlich Phishing, Spam, Malware und Ransomware.

- **Cloud E-Mail Gateway Defense**
- **Schutz vor Phishing und Identitätstäuschung**
- **Automatische Bedrohungserkennung und Incident Response**
- **Kostenloser E-Mail Threat Scanner**
- **Globales Netzwerk zur Bedrohungserkennung**

Sicherheitszentriertes RMM

Führen Sie Sicherheitsbewertung und Verwaltung für die Netzwerke Ihrer Kunden mit Barracuda MSP's zentralisierter Plattform durch. Hier können Sie Routineaufgaben planen und automatisieren und Probleme dank 200+ Pre-Skripts erkennen und beseitigen. Barracuda RMM erlaubt Ihnen, Dienstleistungen mit einem vielschichtigen Sicherheitsansatz nahtlos umzusetzen.

- **Eingebauter Sicherheitsaudit**
- **Microsoft Patch Management**
- **Benutzerdefiniertes Monitoring und Benachrichtigungen**
- **Detaillierte Berichterstattung**
- **PSA Ticket System**

Netzwerk & Cloud Sicherheit

Durch Barracuda MSP's Netzwerksicherheits-Lösungen können Sie Ihren Kunden Schutz für Ihre SaaS-Umgebungen, Fernzugriff, Web-Aktivitäten, mobiles Internet und Netzwerkumgebungen gewährleisten.

Wir bieten Ihnen Hardware, Cloud und virtuelle Bereitstellungsoptionen mit voller Flexibilität an, ohne Ihr Schutzniveau zu beeinträchtigen.

- **Cloud-basierende Firewall**
- **Sicherer CloudGen Zugriff für Anwendungen und Arbeitsaufkommen**
- **Filter und Schutz für Web-Inhalte**
- **Schutz für Internetanwendungen**

Datenschutz

Barracuda MSP's Datenschutzlösung ermächtigt Sie, die unternehmenskritischen Daten Ihrer Kunden zu sichern. Egal ob Sie auf On Premise, Appliance-based Lösungen angewiesen sind oder einen hardwareunabhängigen Ansatz bevorzugen, wir bieten Ihnen volle Flexibilität.

- **Barracuda Backup – für physische, virtuelle und SaaS-Umgebungen, entweder On-Premise oder in der Cloud; einsetzbar in unter einer Stunde**
- **Intronis Backup – zur Gänze rebranding-fähig, auf reiner Softwarebasis**
- **Cloud-to-Cloud Backup für Office 365 – skalierbare Backup und Wiederherstellungs-Lösung für Microsoft 365 Daten**

Ihre Weiterentwicklung zu einem sicherheitszentrierten MSP beginnt heute

Möchten Sie mit Ihrem MSP wettbewerbsfähiger und relevanter werden? Als Marktführer kann Barracuda MSP Ihnen helfen, Ihr Sicherheitsportfolio zu erweitern und Sie unterstützen, Ihre Dienstleistungen mit einer innovativen Produktauswahl zu erweitern.

Wagen Sie den Schritt zum sicherheitszentrierten MSSP und kontaktieren Sie Barracuda MSP noch heute.