Der Leitfaden für MSPs: Wie Sie Ihre Managed Security Services mit einem Security-Centric RMM verbessern können

MSP Barracuda

BarracudaMSP.com

Table of Contents

Warum Sie einen Security-First Ansatz fahren sollten

Ihre Managed Services laufen wie eine gut geölte Maschine - jedes verwaltete System ist inventarisiert und auf dem neuesten Stand. Sie sind in der Lage, jedes System aus der Ferne zu unterstützen, und Sie nutzen bereits Automatisierungen, um kleinere Probleme zu beheben. Heisst - im Wesentlichen haben Sie ein vorhersehbares und profitables Managed-Service-Angebot, das funktioniert.

Aber die Zunahme von Cyberangriffen auf kleine und mittelständische Unternehmen (SMB) - die wir als Unternehmen mit weniger als 250 Mitarbeitern definieren - erfordert, dass SMB-Organisationen (und damit auch die MSPs, an die sie ihre IT auslagern) sich proaktiv gegen Cyberangriffe schützen müssen. Die gute Nachricht ist, dass Sie bereits einige Sicherheitskomponenten in Ihr Angebot integriert haben (z. B. Patch-Management), aber lediglich nur einen oder zwei Aspekte der Security zu adressieren, reicht leider nicht aus, um Cyberkriminelle von den Netzwerken Ihrer Kunden fernzuhalten.

MSPs müssen damit beginnen, bei jedem Service, den sie anbieten, einen Security-First-Ansatz zu verfolgen. Dies geht über die Security-Services hinaus, die Sie Ihren Kunden anbieten.

Dieser Ansatz geht über die Sicherheitsservices hinaus, die Sie Ihren Kunden anbieten – und er muss mit Ihrer Remote-Monitoring- und -Management-Lösung (RMM) beginnen. Ein RMM ist unerlässlich für die Bereitstellung von Services für Ihre Kunden, und die richtige Lösung kann sicherstellen, dass Security in Ihre täglichen Aktivitäten eingebettet ist.

Wenn Sie sich dafür entscheiden, ein separates Sicherheitsangebot zu erstellen, gibt es drei Hauptgründe, warum Sie die Security in Ihr RMM einbetten sollten:

1. Cyber-Bedrohungen werden für KMUs immer schlimmer

Sie lesen die Schlagzeilen und hören von hochkarätigen Cyberbedrohungen, bei denen hohe Lösegelder gezahlt, massenhaft Datensätze gestohlen oder Millionen von Euros für die Behebung von Angriffen ausgegeben wurden. Aber es wird immer die Frage gestellt, was ist mit den KMUs?

Im Jahr 2018 berichteten durchschnittlich 34 Prozent der SMB-Organisationen, dass sie das Ziel eines Cybervorfalls waren, und im Jahr 2019 stieg diese Zahl auf 52 Prozent[1].

Und wenn Sie die KMUs selbst nach ihrer Wahrnehmung von Cyberangriffen im Jahr 2019 fragen, wird Ihnen die Mehrheit von ihnen sagen, dass die Angriffe gezielter werden (69 Prozent), ausgefeilter (60 Prozent) und schwerwiegendere Folgen haben (61 Prozent)[2].

Trotz des Eindrucks, dass kleine und mittelständische Unternehmen kein interessantes Ziel für Cyberkriminalität sind, ist es in Wahrheit so, dass Ihre Kunden genauso an vorderster Front kämpfen wie ihre Unternehmenskollegen.

Trotz des Eindrucks, dass KMUs kein interessantes Ziel sind, ist die Wahrheit, dass ihre Kunden genauso an der vordersten Front des **Cyber Security Kampfes stehen wie ihre Kollegen in großen Unternehmen.»**

1 Hiscox, Cyber Readiness Report (2019)

2 Ponemon, State of Cybersecurity in Small and Medium Size Business (2019)

2. SMBs sind bereit, etwas zu tun

Viele MSPs haben die Erfahrung gemacht, dass ihre Kunden ihr Budget nicht für Security-Initiativen ausgeben wollen. Es stimmt zwar, dass KMUs ihr Portemonnaie vielleicht etwas fester halten als größere Unternehmen, aber sie beginnen zu verstehen, dass mit jedem Angriff greifbare Kosten verbunden sind. Cyberattacken stellen nun eine Frage des Zeitpunkts dar, nicht des ob es eine geben wird – **Dies verlagert die Diskussion um Security von einer "Versicherungspolice" zu einer Notwendigkeit**.

Die durchschnittlichen Kosten, die ein KMU für die Behebung eines einzelnen Cybervorfalls zahlt, belaufen sich auf etwas mehr als 11.000 US-Dollar (ca. 9.350 EUR). Das ist zwar eigentlich auf den ersten Blick nicht berichtenswert, aber ein erheblicher Teil des Umsatzes Ihres Kunden, der nicht in Gewinn umgewandelt wird.

Als Reaktion darauf stellen KMUs nun aktiv einen Teil ihres Budgets für die Verbesserung ihrer Security-Position zur Verfügung. Im Durchschnitt geben KMUs 98.000 US-Dollar (8.3150 EUR) ihres Budgets für Cybersicherheit aus. In der Dach Region sehen die Zahlen ähnlich aus. Die Aufschlüsselung der Ausgaben von KMUs nach Mitarbeitergröße sieht wie folgt aus[1]:

[1] Anzahl der Mitarbeiter	[2] durchschnittliche jährliche Ausgaben für Cybersicherheit
[3] 1-19	[4] $7,000/5.940 EUR
[5] 20-49	[6] $37,000/31.401 EUR
[7] 50-99	[8] $115,000/31.401 EUR
[9] 100-249	[10] $436,000/370.000 EUR

Hinzu kommt, dass im Durchschnitt 62 Prozent der KMUs planen, ihre Ausgaben für ihre Cybersicherheitsinitiativen zu erhöhen,

wobei fast ein Drittel von ihnen sowohl Security-Outsourcing (30 Prozent) als auch Sicherheitsberater (31 Prozent) als Top-Prioritäten für das kommende Jahr ansieht. Darüber hinaus gibt fast ein Drittel (32 Prozent) der KMUs an, dass sie bereits einen MSP zur Unterstützung der IT-Sicherheitsoperationen ihres Unternehmens einsetzen[2].

Ein erheblicher Prozentsatz Ihrer Kunden ist bereit, sich mit Cyberangriffen auseinanderzusetzen; sie wissen nur nicht, was sie dagegen tun sollen. und genau da können Sie ansetzen.

3. Ihre RMM-Lösung bietet bereits eine gewisse Security

Unabhängig davon, ob Sie Security-Services separat anbieten oder in Ihr Kernangebot integrieren möchten, haben Sie bereits einige Vorteile, da Sie Ihren Kunden bereits Services verkauft haben, die ein RMM nutzen:

- **Sie haben bereits fast jedes System beim Kunden schon gesehen** – Das Vorhandensein eines RMM verschafft Ihnen den notwendigen Einblick in die Vorgänge im Netzwerk Ihres Kunden. Sie haben die Möglichkeit, die Desktops, Laptops, Server und sogar Cloud-basierte Systeme Ihrer Kunden zu überwachen, zu verwalten, zu aktualisieren und zu schützen. In vielerlei Hinsicht ist ein RMM eine notwendige Grundlage für jede Art von Security-Angebot.
- **Security gehört bereits zu Ihrem Wortschatz im Verkauf** Die meisten RMMs verfügen über eine Form des integrierten Patch-Managements oder eines Drittanbieters, das mit einer rudimentären Form des Schwachstellen-Scannens von Systemen und Anwendungen verknüpft ist. Es gibt keinen MSP, der nicht irgendeine Form von Anti-Malware-Lösung einsetzt. Im Wesentlichen haben Sie also die Grundlagen gelegt; Sie müssen nur noch eine Reihe von Security-Lösungen aufbauen, die eine mehrschichtige Sicherheitsstrategie für Ihren Kunden schaffen.
- **Der Kunde vertraut Ihnen schon** – Das ist der Schlüssel; Sie haben eine Kundenbeziehung aufgebaut, in der Sie sie mit Rat, Vision, Richtung und Ausführung für ihre Technologie versorgen. Wer könnte besser als Sie diese Liste um Security erweitern?

Es gibt hier eine offensichtliche Möglichkeit - eine, die Sie irgendwie schon anbieten. Also, was sollten Sie tun?

> Sie haben die Grundlagen geschaffen, Sie müssen nur noch eine Reihe von Security-Lösungen aufbauen, die eine mehrschichtige Sicherheitsstrategie für Ihre Kunden schaffen.»

Zum“Security-First” Ansatz übergehen

Es geht darum, den Sicherheitsgedanken in jeden Service zu integrieren, beginnend mit RMM. Es ist eine Denkweise, die Cyberbedrohungen als ein weiteres betriebliches Risiko identifiziert, das kontinuierlich angegangen werden muss. Wir werden uns drei spezifische Schritte ansehen, die Sie unternehmen können, um Sicherheitsservices in Ihr bestehendes RMM-Angebot zu integrieren.

Die folgenden High-Level-Schritte helfen Ihnen, einen sicherheitszentrierten Ansatz zu etablieren, der von Ihrem RMM unterstützt wird und später zu einem separaten Angebot an Sicherheitsdiensten weiterentwickelt werden kann.

- **Definieren Sie Ihre Managed Security Services** – Hier legen Sie fest, wie Ihr Security-Serviceangebot aussieht, welche Teile der Umgebung Ihres Kunden Sie schützen werden und wie Sie die Automatisierung in Ihrer RMM-Lösung nutzen werden, um die Servicebereitstellung zu vereinfachen.
- **Finden Sie Lösungen, die Ihre Serviceanforderungen erfüllen** – Sie müssen diejenigen Softwarelösungen identifizieren, welche bei der Bereitstellung Ihres Dienstes helfen, die Integrationen, die für die Bereitstellung wichtig sind, und wie die Automatisierung über alle beteiligten Lösungen hinweg genutzt werden kann.
- **Suchen Sie nach Möglichkeiten, die Automatisierung zu nutzen, um die Arbeit zu erledigen** – Viele sicherheitsrelevante Aufgaben erfordern kein regelmäßiges menschliches Eingreifen, es sei denn, es liegt ein Problem vor, das behoben werden muss. Die Nutzung von Automatisierung wird eine Schlüsselkomponente für Ihre Servicebereitstellung sein; eine, die sich stark auf Ihr bestehendes RMM stützen kann, um Folgendes zu liefern.

Die Nutzung der Automatisierung wird eine Schlüsselkomponente für Ihre Servicebereitstellung sein; eine Komponente, die sich stark auf Ihr bestehendes RMM stützen kann, um Folgendes zu liefern:»

Definieren Sie Ihr Managed Security Service Angebot

Das Hinzufügen von Security zu Ihren bestehenden Services oder das Erstellen eines völlig neuen Serviceangebots ist nicht so einfach, wie die Auswahl einer Software und deren Aufbau.

Bei der Bereitstellung von Cybersicherheit für Ihre Kunden müssen MSPs einen mehrschichtigen Ansatz verfolgen - und daher mehrere Lösungen nutzen, die Teil des Services sein müssen. - um sicherzustellen, dass sie etwas liefern können, das tatsächlich Schutz bietet.

Es ist ein heikles Gleichgewicht. Wenn das Angebot zu wenig Security Bereiche abdeckt, wird Ihr Kunde mit Angriffen überhäuft und ist sehr unzufrieden mit Ihnen. Ein zu komplexes Angebot kann allerdings dazu führen, dass die Kunden aufgrund der Kosten, der Komplexität und der vermeintlichen Unausgewogenheit mit ihren Bedürfnissen ganz darauf verzichten. Aus Ihrer Sicht sollten Sie einen Security-Service anbieten, der einige Dinge erfüllt:

1. **Kosten Effizienz** – trotz des Sicherheitsbedürfnisses Ihrer Kunden haben auch diese einen Preis im Kopf.
2. **Es ist effektiv** – Ihr Serviceangebot muss die Umgebungen Ihrer Kunden erfolgreich sichern.
3. **Es hebt ihr RMM auf eine andere Ebene** – Die meisten Angriffe betreffen auf die eine oder andere Weise den Endpoint. Im Grunde genommen denselben Endpunkt, den Sie mit Ihrem RMM Security Tool bereits überwachen und monitoren. Security Services sollten also die offensichtlichen Vorteile eines RMMs mit einbeziehen, das erleichtert Vieles für Sie und Ihre Kunden.

Dieses Kapitel hilft Ihnen, die Security-Komponenten in Ihrem Service-Angebot aus einem strategischen Blickwinkel zu betrachten und gibt Ihnen Hinweise, welche Services Ihr Angebot umfassen sollte.

Was sollte ein Teil Ihres Angebots sein?

Es gibt ein wichtiges Unterscheidungsmerkmal, das skizziert werden muss, bevor wir auf die Einzelheiten eingehen. Es gibt MSPs, die Sicherheitsdienstleistungen anbieten, und es gibt Managed Security Services Provider (MSSP) - beides ist nicht dasselbe. Ihr Sicherheitsangebot setzt schützende Sicherheitsschichten ein, die helfen, **Cybersecurity-Vorfälle** zu **verhindern**, zu **erkennen** und darauf zu **reagieren**. MSSPs gehen darüber hinaus und bieten erweiterte Dienste wie Intrusion Management, Threat Hunting, Compliance Monitoring und mehr.

Es gibt einige Überschneidungen bei bestimmten Diensten. Wir gehen jedoch davon aus, dass Sie lediglich versuchen, ein grundlegendes - aber effektives - Set von Diensten als Teil Ihres Security-Angebots anzubieten.

Ohne auf die verschiedenen Arten von Security-Software- und -Hardware-Lösungen einzugehen, die Sie einsetzen könnten, lassen Sie uns zunächst Ihr Angebot vom Standpunkt der Dienstleistung aus betrachten. Was sollten Sie als Teil Ihres Dienstes sichern?

Für MSPs, die Security-Services hinzufügen möchten, aber nicht so weit gehen, ein MSSP zu werden, gibt es fünf Servicebereiche, in denen Schwachstellen angegangen werden müssen, um die Umgebung richtig abzusichern, ohne dass man dafür ein enormes Maß an Fachwissen benötigt. Diese Bereiche bilden eine mehrschichtige Security-Strategie für Ihre Kunden und helfen Ihnen, Cyberangriffe zu verhindern.

Die Bereiche des Kundennetzwerks, die MSPs unter dem Gesichtspunkt der Security am einfachsten adressieren können, sind.

- **Perimeter** – Dies sollte als logischer Horizont des Kundennetzwerks betrachtet werden, an dem sich Firewalls und Gateways befinden, um das Internet vom internen Netzwerk zu trennen. In den letzten Jahren hat sich dies auch zu einem dynamischen Perimeter entwickelt, der durch die Interaktion der Benutzer mit der Außenwelt abgegrenzt wird. Remote-Benutzer, persönliche Geräte, öffentliches WLAN, Cloud-basierte Anwendungen und Daten, Web-Browsing und E-Mail haben alle einen Einfluss darauf, wo genau der Rand des Netzwerks liegt. Heutzutage umfasst diese Grenze den Remote-Mitarbeiter der von einem Firmengerät in einem Café am anderen Ende der Welt im Internet surft - und Sie müssen diesen Benutzer, das Gerät und die Verbindung absichern.

- **Netzwerk** – Jedes Gerät im Netzwerk hat das Potenzial, Angriffen ausgesetzt zu sein. MSSPs denken an das Netzwerk mit fortschrittlichen Begriffen wie Penetrationstests und Packet Sniffing, aber es gibt immer noch Dinge, die der MSP tun kann, um sicherzustellen, dass die Geräte im Netzwerk sicher sind.
- **Endpoint** – Angreifer müssen im Netzwerk Ihres Kunden Fuß fassen, und Malware braucht eine Umgebung, in der sie sich aufhalten kann. Aus diesem Grund ist der Endpunkt ein primäres Ziel; er bietet Angreifern einen unentdeckten Zugang, von dem aus sie den Rest ihres Angriffs starten können. Im Durchschnitt bleiben Angreifer 146 Tage in einem Netzwerk, bevor sie entdeckt werden[3].
- **User** – Phishing und Social Engineering sind die Angriffsvektoren Nummer eins bei KMUs[2]. Der Erfolg dieser Angriffe hängt fast immer von einer Benutzerinteraktion ab. Einfach ausgedrückt, ein Benutzer muss auf einen Link klicken oder einen Anhang öffnen, damit ein Angriff funktioniert. Als Teil Ihrer Sicherheitsstrategie sollten Sie den Benutzer jedoch sowohl als weitere Schwachstelle als auch als Chance betrachten, die Sicherheit der Umgebung Ihres Kunden zu verbessern.
- **Data** – Als Teil der meisten Cyberangriffe gibt es eine Reihe von Möglichkeiten, Daten zu nutzen, um den Angreifer zu unterstützen. bei Ransomware-Angriffen werden Daten verschlüsselt. Angriffe mit lateraler Bewegung oder Inselhüpfen beinhalten einen Verzeichniszugriff, bei dem häufig Benutzerkonten erstellt, geändert und mit Berechtigungen versehen werden- all das in dem Bestreben, dauerhaften Zugriff auf das Netzwerk und die Ressourcen Ihres Kunden zu erhalten.

Der Aufbau einer Verteidigung unter Verwendung dieser Teile des Netzwerks Ihres Kunden schafft eine mehrschichtige Security-Strategie - eine, bei der jede Schicht zur Stärkung der Security-Position beiträgt, indem sie Cyberattacken mit einer anderen Methode begegnet.

3 Microsoft, Advanced Threat Analytics (2019)

Automatisieren Sie Ihr Angebot mit RMM

Wenn Sie Ihr neues Security-Service-Angebot planen, sollten Sie verschiedene Möglichkeiten in Betracht ziehen, wie Sie die Automatisierung in Ihrer RMM-Lösung nutzen können, um Ihre Kunden auf drei Arten zu schützen:

1. **Verschaffen** Sie sich einen **Überblick** über den aktuellen Stand der Security Ihres Kunden
2. Stellen Sie **proaktiv** sicher, dass die Kundenumgebung **so sicher wie möglich ist**.
3. Richten Sie ein **automatisches Beheben von Problemen**, die den Kunden gefährden, ein.

Je nach der spezifischen Funktionalität Ihrer aktuellen Lösung gibt es eine Reihe von Möglichkeiten, wie die Automatisierung Ihr mehrschichtiges Security-Angebot unterstützen kann. Diese Tabelle zeigt nur einige der Möglichkeiten, wie RMM-Automatisierung helfen kann.

Nutzen Sie die Automatisierung, die Sie in Ihrem RMM finden, um Kunden zu sichern.»

Security Layer	Wege zur Nutzung der RMM Automatisierung
Perimeter	• Anwendung und Durchsetzung von Firewall-Einstellungen zum Schutz von Laptops im offentlichen Wi-Fi
Netzwerk	• Uberwachen Sie neue Geräte und informieren Sie die IT-Abteilung über potenziell bösartige Geräte im Netzwerk • Behebung bekannter OS-Schwachstellen, die als Teil vieler netzwerkbasierter Angriffe auf Internet-zugangliche Server und Endgeräte gilt • Anwenden und Durchsetzen sanktionierter IP Konfigurationen
Endpoint	• Identifizieren Sie potenziell unerwunschte Anwendungen (PUA) mithilfe des Software-Inventars • Behebung bekannter Betriebssystem - und Anwengdunsschwachstellen, die zur Infektion von Endgeraten mit Malware genutzt werden • Uberprufung der Geratekonfigurationen anhand von Sicherheitsempfehlungen • Erzwingen sicherer OS-Konffigurationseinstellungen
User	• Anwengdunseinstellungen anwenden, um Benutzer davor zu schutzen, Opfer von Phishing-Angriffen zu werden
Data	• Uberwachen Sie Log-Ins auf laterale Bewegungen als Teil von Ransomware und Data Breach-Angriffen

Definieren der automatischen Sicherheit

Das Ziel ist es, ein Serviceangebot zu entwickeln, das Sie vorhersehbar liefern können. Wenn Sie also formulieren, wie Ihr Angebot aussehen soll, ist es wichtig, die Automatisierung in den Vordergrund zu rücken, um ein Maß an Vorhersagbarkeit zu erreichen, das die Rentabilität erhöht. Ein RMM ist die Grundlage für Ihr Serviceangebot, und Sie können andere Sicherheitslösungen darauf aufbauen, die wir im nächsten Kapitel behandeln werden: Die Auswahl von Sicherheitslösungen über Ihr RMM hinaus.

Auswahl von Sicherheitslösungen über Ihr RMM hinaus

Im letzten Kapitel haben wir über Ihr neues Angebot als eine mehrschichtige Strategie gesprochen, die fünf Bereiche umfasst: Perimeter, Netzwerk, Endpunkt, Benutzer und Daten. Für jede dieser Schichten gibt es eine Reihe von Möglichkeiten, wie Sie Ihre bestehende RMM-Lösung nutzen können, um jede zu adressieren.

Aber ein RMM bringt Sie bei der Absicherung der Umgebung Ihrer Kunden nur so weit, weil sein Fokus weiter gefasst ist, als nur die Sicherheit. Aus diesem Grund benötigt Ihr RMM Unterstützung durch andere Lösungen.

In diesem Kapitel werden wir verschiedene Lösungen besprechen, die Sie in Betracht ziehen sollten, um ein robustes und effektives Security Angebot zu erstellen und bereitzustellen.

Welche anderen Lösungen benötigen Sie?

Ein RMM-Tool kann zwar einige Funktionen bieten, die bei der Absicherung der Kundenumgebung helfen können, aber Security

ist nicht gerade ein Kernthema der meisten Tools. Sie benötigen einige zusätzliche Security Lösungen, um das Angebot abzurunden. Die offensichtliche Frage dreht sich darum, welche Art von Lösungen benötigt werden.

Es gibt viele Lösungen, aus denen man wählen kann - so viele, dass es verwirrend werden kann, welche Arten von Lösungen notwendig sind. Um dies aufzuschlüsseln, werden wir weiterhin ein mehrschichtiges Security Modell verwenden, um Ihnen zu helfen, eine Strategie zu entwickeln, welche Lösungstypen Sie benötigen.

Jede der fünf folgenden Schichten steht für eine bestimmte Stelle, an der die Möglichkeit besteht, einen Angriff zu verhindern - dies sollte die Grundlage für Ihre Auswahl sein.

Perimeter

Angriffe können in Form von automatischen Scans Ihrer mit dem Internet verbundenen Systeme und Anwendungen erfolgen. Die Einrichtung einer Next-Gen-Firewall, einer Web Application Firewall und einer Intrusion Detection/Prevention kann bösartige Scans und Zugriffe blockieren und einen Angriff stoppen, bevor er beginnt.

Angriffe, die erfolgreich in ein Kundennetzwerk eindringen, müssen fast immer zu einem Command-and-Control-Server (c2) gelangen. Jede Art von bösartigem ausgehendem Datenverkehr kann oft durch die Implementierung von domainbasierter Nachrichtenauthentifizierung, -berichterstattung und -konformität (besser bekannt als DMARC) und DNS/URL-Filterung vereitelt werden, um den Zugriff auf bösartige Domains und Systeme im Internet zu identifizieren und zu blockieren.

Netzwerk

Es gibt einige Möglichkeiten, wie Sie das Netzwerk des Kunden für eine bessere Sicherheit optimieren können. Die Beschränkung des Zugriffs auf kritische Systeme und Anwendungen mithilfe der Netzwerksegmentierung kann das potenzielle Risiko eines Angriffs auf kritische Ressourcen deutlich senken. Sie können das das Patch-Management hervorragend ergänzen, indem Sie Schwachstellen-mit speziellen Scans im Netzwerk erkennen und so proaktiv Systeme und Anwendungen identifizieren, die für Angriffe anfällig sind.

Die Fähigkeit, den Netzwerkverkehr auf anomale und bekanntermaßen bösartige Traffic Muster zu überwachen, kann dabei helfen, Angreifer von weiteren bösartigen Aktionen abzuhalten.

Endpoint

Wenn es ein Angriff durch alle vorherigen Schichten geschafft hat, benötigen Sie Endpunkt-basierte Anti-Malware- und Endpunkt-Erkennungs- und Reaktionslösungen, um das Verhalten potenziell bösartiger Betriebssysteme und Anwendungen zu überwachen und zu blockieren.

User

In vielerlei Hinsicht ist der Benutzer Ihr schwächstes Glied; er ist es, der bösartige E-Mail-Anhänge öffnet und auf bösartige Links klickt, ohne darüber nachzudenken.

Wenn Sie also Web- und E-Mail-Scan-Lösungen einsetzen, die proaktiv nach bösartigen Inhalten suchen, bevor der Benutzer damit interagieren kann, schützen Sie den Benutzer vor sich selbst. Aber auch die Benutzer können ein Teil Ihrer Sicherheitsstrategie sein, indem sie kontinuierlich an Schulungen zum Thema Sicherheit teilnehmen. Dies schult ihre Wachsamkeit bei der Arbeit und zeigt ihnen, welche Taktiken und Angriffsmethoden bei Angriffen üblicherweise verwendet werden.

Daten

Die vorangegangenen Schichten sind alle darauf ausgelegt, Angreifer davon abzuhalten, an Ihre Daten zu gelangen. Sollte es ihnen gelingen, sich Zugang zu verschaffen, führen Ransomware-Angriffe potenziell zu verschlüsselten Daten und Datenverletzungen, die die Manipulation von Benutzer- und Gruppenkonten im Active Directory beinhalten können, um den Zugriff zu erleichtern. Daher sollten Backups Teil Ihres Sicherheitsangebots sein, um die Umgebung in einen als gut und sicher bekannten Zustand zurückversetzen zu können. Es ist auch wichtig zu beachten, dass einige Ransomware speziell nach Backup-Dateien auf lokalen Systemen sucht. Daher sollte ein Cloud-basiertes Backup eine Priorität für Ihren MSP sein.

In der Tabelle sind empfohlene Lösungstypen aufgeführt, die speziell für die Abwehr von Angriffsmaßnahmen in jeder Phase eines Cyberangriffs konzipiert sind.

Protection layer	Solution type
Perimeter	• Next-Gen/Cloud-Gen Firewall • Web Application Firewall • Intrusion Detection/Prevention • DMARC • DNS/URL Filtering
Netzwerk	• Netzwerk Segmentierung • Vulnerability Scanning • Netzwerk Monitoring/Packet Inspection
Endpoint	• Anti-Malware • Endpoint Detection und Response
User	• Email Scanner • Web Scanner • Security Awareness Training
Daten	• Cloud-based Backup/Recovery

Eine weitere, nicht aufgeführte Schicht, die Sie berücksichtigen sollten, ist die Identität. Der Schutz von Benutzeranmeldeinformationen mit Multi-Faktor-Authentifizierung ist ein einfaches und effektives Mittel, um festzustellen, dass ein Benutzer derjenige ist, für den er sich ausgibt. Zusätzlich kann der Schutz privilegierter Identitäten durch die Verwendung einer Art Passwort-Tresor für privilegierte Konten (allgemein als Privileged Access Management bezeichnet) ebenfalls von Nutzen sein.

All dies kann für einen MSP, der nur wenig Erfahrung mit dem Anbieten von Security hat, etwas entmutigend klingen. Lassen Sie sich von der Liste nicht abschrecken.

Softwareanbieter, die sich auf MSPs spezialisiert haben, haben bereits Wege gefunden, die Implementierung und Integration dieser Art von Lösungen zu vereinfachen, so dass Sie nicht das Gefühl haben, am ersten Tag unterzugehen.

Zusammenstellung der Lösungen

Wenn es geht, suchen Sie nach Möglichkeiten, sowohl die Automatisierung als auch die Integration zu nutzen, um die Servicebereitstellung zu verbessern.

Bei der Auswahl der zu verwendenden Lösungen sollten Sie auf ähnliche Funktionen achten, die die Intelligenz erhöhen, die Sicherheit verbessern und das Risiko reduzieren.

In unserem nächsten Kapitel werden wir den Wert der Automatisierung erörtern und praktische Möglichkeiten aufzeigen, wie sie eingesetzt werden kann.

Der Schutz von nutzeranmeldeinformationen mit **Multi-Faktor-Authentifizierung** ist ein einfaches und effektives Mittel, um festzustellen, dass ein Benutzer derjenige ist, der er vorgibt zu sein. »

Der Wert von Automatisierung im Security Umfeld

Im Laufe der Jahre sind viele Managed-Service-Unternehmen von einem einzigen IT-Profi, der alle Arbeiten selbst erledigte, zu größeren Unternehmen gewachsen, die ihren Kunden mehrere Dienstleistungen anbieten.

Die Herausforderung für MSPs besteht nun darin, neue Methoden, Tools und Prozesse zu finden, die es ihnen ermöglichen, zu wachsen. Aber bei den meisten Diensten gibt es immer noch die Möglichkeit, Probleme manuell zu lösen. Selbst mit einer RMM-Lösung, die über Skripte automatisiert werden kann, ziehen es viele MSPs immer noch vor, ihre Techniker die Arbeit machen zu lassen. für einige Dienste- nämlich RMM und Backups - ist es (bis zu einem gewissen Grad) möglich, Services manuell zu erbringen. wenn es um Sicherheit geht, ist das einfach nicht möglich.

Es gibt eine Reihe von Dingen, die es schwierig machen, Sicherheitsdienste manuell bereitzustellen. Dazu gehören:

- **Die zunehmende Raffinesse der Angriffe** – Cyberkriminelle investieren massiv in Methoden, um einen erfolgreichen Angriff zu gewährleisten. Phishing-Angriffe verwenden jetzt fortschrittliche Social-Engineering-Methoden - und gehen sogar so weit, dass sie ein bestimmtes individuelles Ziel ausforschen und gefälschte Websites erstellen, die wie ihr. legitimes Gegenstück aussehen, um Anmeldeinformationen zu stehlen, und nutzen ausweichende Infektionstechniken, um zu verhindern, dass die Malware von Sicherheitslösungen erkannt wird.
- **Die Verfügbarkeit von Crimeware-as-a-Service** – Heute kann jeder, der in das “Geschäft” mit Cyberangriffen einsteigen möchte, dies tun. So bieten die Entwickler von Ransomware diese “as-a-Service” an, ohne dass dem Cyberkriminellen Vorlaufkosten entstehen (was den Einstieg in die Cyberkriminalität erleichtert), und werden über einen Prozentsatz des eingenommenen Lösegelds entschädigt.
- **Der ständige Wechsel der Taktik** – Cyberkriminelle testen kontinuierlich ihre Methoden, sowohl gegen Sicherheitslösungen als auch im praktischen Einsatz. Sie schauen, was funktioniert und was nicht, und ändern ihre Angriffsmethoden, um eine Entdeckung zu vermeiden, die Infektion zu erhöhen und den Erfolg der Angriffe zu verbessern.

- **Die Unvorhersehbarkeit von Angriffen** – MSPs haben nicht die Möglichkeit zu wissen, wann, wo, wie und in welchem Umfang ein Angriff erfolgt. Das macht die Abhilfe im besten Fall schwierig.

Im Grunde genommen ist die Einrichtung und Aufrechterhaltung der Sicherheit eines KMUs ein sich ständig bewegendes Ziel. Die Bedrohungslandschaft ändert sich in rasantem Tempo, sodass es für einen MSP sehr schwierig ist, mit jedem neuen Angriff, jeder Sicherheitskonfiguration eines Systems usw. Schritt zu halten.

Um ein Angebot zu schaffen, das sich wirklich um die Sicherheit des Kunden bemüht, wird Automatisierung zu einer Notwendigkeit - vom Einsatz zum Schutz der Kundenumgebung, zur Verhinderung von Angriffen über Schwachstellen, zur Erkennung von Angriffen, wenn sie auftreten, bis hin zu Abhilfemaßnahmen. kurz gesagt: Sicherheitsdienste brauchen Automatisierung, um erfolgreich zu sein.

Die Vorteile des Einsatzes von Automatisierung

Automatisierung bietet Ihnen mehr als nur den Vorteil, dass etwas ohne manuelles Eingreifen erledigt wird. Es gibt eine Reihe von Möglichkeiten, wie die Automatisierung dem MSP bei der Bereitstellung eines Sicherheitsdienstleistungsangebots zugute kommt. Dazu gehören::

- **Konsistenz** – Konsistenz ist wichtig, um zu wissen, dass die gesamte Umgebung auf die exakt gleiche Weise verwaltet wird. Wenn Sie sich entschieden haben, eine bestimmte Sicherheitskonfiguration zu implementieren oder einige Patches aufzuspielen, können Sie nicht einige Systeme nur teilweise konfiguriert haben. Die Automatisierung stellt sicher, dass jedes System und jede Anwendung, die verwaltet werden muss, dies auch tut.
- **Genauigkeit** – Während es bei der Konsistenz darum geht, sicherzustellen, dass alle Systeme gleich konfiguriert sind, geht es bei der Genauigkeit darum, sicherzustellen, dass die spezifische Konfiguration pro System oder pro Anwendung korrekt ist. Die Automatisierung ermöglicht die Bereitstellung, Konfiguration und Aktualisierung ohne Abweichungen im Design Ihrer Sicherheitsrichtlinie.

Um ein Angebot zu schaffen, das den Kunden wirklich absichert, wird die Automatisierung zur Notwendigkeit.»

- **Aktuelle Sicherheit** – Bei der Automatisierung geht es nicht nur darum, Skripte auszuführen, um Aufgaben zu erfüllen. Es sollte ein gut durchdachter Prozess sein, der es Ihnen ermöglicht, alle Ihre Lösungen auf dem neuesten Stand zu halten, wenn sich die Bedrohungslandschaft ändert. Wenn beispielsweise neue Malware oder bösartige Domains entdeckt werden, ist die automatische Aktualisierung der entsprechenden Lösungen, um diese Angriffsmöglichkeiten zu blockieren, ein enormer Mehrwert für Ihr Angebot, um den Sie sich nie kümmern müssen.
- **Schnelleres Ansprechen** – Das Ziel eines Managed Security Service-Angebots ist es, dass Sie eine sichere Umgebung aufrechterhalten, die den Kunden schützt. Es können jedoch Probleme auftreten, wie z. B. die Identifizierung eines ungepatchten Systems. Mithilfe von Automatisierung können solche Probleme ohne menschliches Eingreifen gescannt, identifiziert und behoben werden, was Ihre Bereitstellungskosten senkt.
- **Skalierbarkeit** – Wenn Ihr Unternehmen mehr Geräte übernehmen muss, können Sie den Service durch Automatisierung ausbauen, ohne mehr Personal einstellen zu müssen.
- **Vorhersagbarkeit** – Die Automatisierung liefert dies in zweierlei Form. Erstens wird die Auslieferung Ihres Angebots aufgrund der Konsistenz und Genauigkeit der Auslieferung wesentlich vorhersehbarer. Zweitens addieren sich die bisherigen Vorteile der Automatisierung bis hin zu einer vorhersehbar sicheren Umgebung, in der Ihr Vertrauen in die Sicherheit der Umgebung hoch ist.
- **Rentabilität** – Vorhersagbarkeit führt zu Rentabilität. Durch die Automatisierung den Aufwand für die Kundenakquise zu automatisieren, ist es viel einfacher, Ihr Angebot in einen profitablen Zustand zu bringen.

Bessere Sicherheit durch Automatisierung

Schauen wir uns anhand einiger Beispiele an, wie Automatisierung (ob als Teil Ihres RMM oder anderer Sicherheitslösungen) zur Verbesserung der Servicebereitstellung eingesetzt werden kann. Die Tabelle auf der folgenden Seite hebt einige Methoden hervor, wie Automatisierung innerhalb der drei verschiedenen Phasen der Sicherheit praktisch genutzt werden kann: Prävention, Schutz und Erkennung sowie Reaktion.

Service stage	Automation example	Solution
Prevention **Herausforderung:** Verhindern Sie die Ausführung eines Angriffs, indem Sie eine sichere Umgebung schaffen	Überwachung des Netzwerks auf neue Geräte	RMM
	Überwachungssysteme für potentiell unerwünschte Anwendungen	RMM
	Zweck: Einen Angriff abwehren Aktualisierte Definitionen und maschinelle Lernalgorithmen durch Schaffung einer eine sichere Umgebung	Eindringen/Detection/Prevention DNS/URL Filtering Web Scanning Email
	Überprüfung, Aktualisierung und Durchsetzung von Sicherheitskonfigurationen auf Netzwerkgeräten, Betriebssystemen und Anwendungen	Firewalls RMM (OS, Applications)
	Schwachstellen, Scanning und Patching	RMM (OS, Applications)
	Sicherstellung ordnungsgemäßer Backups durch Job-Überwachung und -Wiederherstellung	Backup/Recovery
Protection/Detection **Herausforderung:** Überwachung und Identifizierung von Hinweisen auf potenziell bösartige Aktivitäteny	Aktualisierte Definitionen und Algorithmen für maschinelles Lernen	Anti-Malware EDR
	Test and verify attachments	Email Scanning
	Überwachung auf verdächtiges OS-Verhalten	EDR
	Überwachung auf verdächtige oder unangemessene Konfigurationsänderungen	RMM
Response **Herausforderung:** Reagieren Sie auf führende oder aktive Indikatoren für einen Angriff	Quarantäne von bösartigen Dateien und Codeausführung	Email Scanning Anti-Malware EDR
	Ausführen von Abhilfeskripten zur Behebung erkannter Probleme	RMM

Erreichen von Sicherheit durch Automatisierung

MSPs sind per Definition bestrebt, Services zu liefern, die von Natur aus vorhersehbar sind. Aber die Art der Cyberangriffe macht es schwierig, dies zu erreichen. Automatisierung macht Sicherheit weitaus erreichbarer; von der Einrichtung und Aufrechterhaltung einer sicheren Konfiguration über die Erkennung von Angriffsversuchen bis hin zur schnellen Ergreifung von Maßnahmen zur Behebung erfolgreicher Angriffe.

MSPs, die bereits RMM-Tools verwenden, haben einen guten Start mit einer Plattform, die eine benutzerdefinierte Automatisierung bieten kann. Durch das Hinzufügen anderer Lösungen, die relative Maßnahmen nutzen, um ihren Teil einer mehrschichtigen Sicherheitsstrategie zu adressieren, können MSPs schnell ein Servicebereitstellungsmodell erstellen, das effektiv, reaktionsschnell, skalierbar und vorhersehbar ist.

Durch den Einsatz von Automatisierung können MSPs ein Servicebereitstellungsmodell schaffen, das effektiv, reaktionsschnell, skalierbar und vorhersehbar ist.»

Sicherheitsdienste beginnen mit einem sicherheitszentrierten RMM

Es ist offensichtlich, dass selbst die kleinsten Organisationen immer noch anfällig für - und sogar handverlesene Ziele von - Cyberangriffen sind. Daher ist es zwingend erforderlich, dass MSPs beginnen, formell Managed Security Services zum Schutz, zur Vorbeugung, zur Erkennung und zur Reaktion auf Cyberangriffe anbieten.

Wenn Sie einen Sicherheitsservice entwickeln, definieren und schließlich anbieten, ist es wichtig, die Sicherheitsfunktionen, die bereits in Ihrer RMM-Lösung enthalten sind, in das Serviceangebot zu integrieren. in einigen Fällen können RMM-Funktionen die Grundlage eines Aspekts des neuen Sicherheitsservices sein (z. B. Patch-Management) oder verwendet werden In einigen Fällen können RMM-Funktionen die Grundlage eines Aspekts des neuen Sicherheitsdienstes sein (z. B. Patch-Management) oder sie können verwendet werden, um sowohl proaktive als auch reaktive Sicherheitsmaßnahmen durch Automatisierung zu ergänzen (z. B. Überwachung und Behebung von nicht genehmigten Konfigurationsänderungen an Endpunkten).

RMM stellt eine leistungsstarke Grundlage für ein Sicherheitsangebot dar. MSPs, die bereits Managed Services anbieten, die RMM-Lösungen nutzen, haben das Potenzial, einfach einen Basis-Service anzubieten, der mit der Zeit erweitert werden kann, vorausgesetzt, Ihre RMM-Lösung hat sicherheitsrelevante Funktionen und Automatisierung bereits integriert. Als MSP führt der Weg zum Angebot von Sicherheitsdienstleistungen.

Ihre Kunden werden sich des Bedarfs zunehmend bewusst und werden sich entweder an Sie wenden, um ihre Sicherheitsbedürfnisse zu befriedigen, oder an einen MSP, der dies tut. Beginnen Sie also damit, herauszufinden, welche Funktionalitäten genutzt werden können, definieren Sie den Umfang Ihres neuen Services, wählen Sie eventuell benötigte zusätzliche Sicherheitslösungen aus und nutzen Sie die Automatisierung Ihres RMM als Grundlage für eine neue Möglichkeit zur Generierung von Serviceeinnahmen.

Key takeaways

Ein RMM Tool sollte Folgendes mitbringen:

- ein nahezu obligatorisches Minimum an Security, das MSP-Kunden nutzen, um ihr Unternehmen und ihre Endbenutzer zu schützen,
- welches klar kommuniziert und als Teil des Dienstleistungsangebots des MSP an Kunden hervorgehoben werden kann.

Ein sicherheitszentrierte Bild, das ein RMM-Tool für einen MSP projiziert signalisiert, wie

- wichtig Cybersecurity als Kern der Dienstleistungen des MSP-Unternehmens ist,
- die Ernsthaftigkeit, mit der der MSP die Sicherheit seiner Kunden behandelt.

Andere Sicherheitslösungen und -dienste können hinzugefügt oder auf ein RMM-Tool aufgesetzt werden:

- damit das RMM-Tool als solider Ausgangspunkt eines Portfolios von Sicherheitsdiensten dienen kann,
- dass der Gesamtwert des Portfolios an Sicherheitsdienstleistungen eines MSP gestärkt wird,
- und um mehr Kunden anziehen.

Sicherheitsangebote zu automatisieren, hat den Vorteil:

- Aufgaben werden vereinfacht und steigern somit die Effizienz
- Sie reduzieren den Aufwand, sparen Personalkosten und machen das Leben sowohl für den MSP als auch für seine Kunden einfacher.

Über Barracuda MSP

Barracuda MSP ist der MSP-Geschäftsbereich von Barracuda Networks. Unsere Mission ist es, den Erfolg unserer IT-Service-Provider-Partner voranzutreiben, indem wir branchenführende Sicherheit und Datenschutz über eine speziell entwickelte MSP-Plattform, ein konstantes Engagement für den Erfolg unserer Partner und eine Fülle von Channel-Know-how bieten.

Wir glauben an das Managed Service Provider Modell. wir verstehen ihre Herausforderungen. und wir sind Champions für ihren Erfolg.

Dank eines einzigartigen Geschäftsmodells und einer MSP-freundlichen Preisstruktur sind unsere Partner in der Lage, ihre wiederkehrenden Umsätze und Margen zu steigern und ihr Geschäft profitabel zu skalieren.

Über Barracuda RMM

Barracuda RMM ist ein leistungsfähiges, sicherheitsorientiertes Remote-Monitoring- und Management-Tool für MSPs, das mehrere Funktionen zur Stärkung der Sicherheitslage eines MSPs bietet, darunter ein umfassendes Reporting zur Weitergabe an SMB-Kunden, ein zentrales Dashboard, Aufgabenautomatisierung, PSA-Ticketing und Unterstützung für die Integration von Drittanbieter-Apps, um nur einige zu nennen.

Barracuda RMM wurde entwickelt, um MSPs zu unterstützen:

- Vergrößern Sie Ihr Geschäft.
- Automatisieren Sie Ihre Servicebereitstellung.
- Senken Sie Ihre Betriebskosten.

Besuchen Sie unsere Website, um zu erfahren, wie Barracuda RMM Ihren MSP mit den Werkzeugen und Einblicken ausstattet, die Sie benötigen, um Ihren Kunden hochwertige Remote-Sicherheits- und Support-Services zu bieten.

