Der Leitfaden für MSPs zur Stärkung von Managed Security Services mittels sicherheitszentrierter RMM.

MSP Barracuda
Your journey, secured.

BarracudaMSP.com

Table of Contents

Warum Sie einen Security-first-Ansatz verfolgen sollten

Ihr Managed Service läuft wie geschmiert – alle von Ihnen verwalteten Systeme werden erfasst und befinden sich auf dem aktuellsten Stand. Sie können alle Systeme aus der Ferne administrieren und nutzen bereits einige automatisierte Prozesse, um kleinere Probleme zu beheben. Im Grunde genommen verfügen Sie also über ein funktionierendes, berechenbares und rentables Managed Service Angebot.

Allerdings sorgt die steigende Anzahl von Cyber-Angriffen auf Klein- und Mittelunternehmen (KMU) – als solche definieren wir Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern – dafür, dass KMUs proaktiv versuchen (und somit auch die MSPs, zu denen ihre IT ausgelagert wurde) das Thema Cyber-Angriffe zu anzugehen.

Die gute Nachricht ist hier, dass Sie bereits Sicherheitskomponenten in Ihrem Angebot integriert haben (z.B. Patch-Management). Jedoch reicht es nicht aus, nur ein oder zwei Sicherheitskomponenten abzudecken, um Cyberkriminelle davon abzuhalten, in das Netzwerk Ihrer Kunden einzudringen.

1. Cyber-Bedrohungen für KMUs nehmen zu

Sie kennen die Schlagzeilen, hören von hochkarätigen Cyber-Bedrohungen, die zu hohen Lösegeldzahlungen geführt haben, wissen von massivem Datendiebstahl oder den hunderttausenden oder Millionen US-Dollar, die zur Schadensbehebung nach Angriffen aufgebracht wurden. Es stellt sich aber immer folgende Frage: Wie steht es um die KMUs?

Der durchschnittliche Anteil von KMUs, die 2019 in irgendeiner Form von Cyber-Vorfällen betroffen waren, ist im Verlauf des Jahres 2018 um 58% gestiegen; 2018 berichteten durchschnittlich 34 % aller KMUs, Ziel eines Cyber-Vorfalls gewesen zu sein. Diese Zahl stieg 2019 auf 52%[1].

Wenn man sich direkt an die KMUs wendet und sie nach ihrer Wahrnehmung von Cyber-Angriffen im Jahr 2019 fragt, sagt ein Großteil, dass die Angriffe zielgerichteter (69%) und komplexer (60%) geworden sind, sowie schwerwiegendere Konsequenzen haben (61%)[1].

Obwohl es scheint, dass KMUs kein interessantes Ziel für Cyberkriminalität darstellen, ist es Fakt, dass diese Kunden genauso an erster Front stehen wie Großunternehmen.

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

2. KMUs sind bereit, etwas dagegen zu unternehmen

Viele MSPs haben die Erfahrung gemacht, dass ihre Kunden ihr kostbares Budget nicht für Sicherheitsmaßnahmen verwenden möchten. Es stimmt zwar, dass KMUs sparsamer sind als Großunternehmen, jedoch verstehen sie langsam, dass mit jedem Angriff konkrete Kosten auf sie zukommen und das Cyber-Angriffe nun eine Frage des „Wann“ und nicht des „Ob“ sind. Beim Thema Sicherheit geht es jetzt nicht mehr um eine mögliche Risikoabsicherung, sondern um eine Notwendigkeit.

Die durchschnittlichen Kosten, die für Schadensbehebung nach einem einzelnen Cyber-Vorfall auf ein KMU zukommen, belaufen sich bei etwas mehr als 11.000 USD. Das ist zwar nichts Neues, jedoch handelt es sich dabei dennoch um eine beachtliche Summe, die dem Kunden fehlt und aus derer er keinen Profit ziehen kann. KMUs reagieren darauf, indem sie nun aktiv in Cybersicherheit investieren. KMUs investieren mittlerweile durchschnittlich 98.000 USD in Cybersicherheit. Die Ausgaben von KMUs sind abhängig von der Mitarbeiterzahl und sehen wie folgt aus:

Mitarbeiterzahl	Durchschnittliche jährliche Ausgaben für Cybersicherheit
1-19	7.000 USD
20-49	37.000 USD
50-99	115.000 USD
100-249	436.000 USD

Zu diesen guten Neuigkeiten für MSPs kommt hinzu, dass durchschnittlich 62% der KMUs planen, ihre Ausgaben für Cybersicherheitzu steigern. Ein Drittel davon sehen Outsourcing (30%) und Security Consultants (31%) als Prioritäten für das nächste Jahr. Zudem setzt ein Drittel (32%) aller KMUs Berichten zufolge bereits einen MSP ein, um die Cybersicherheit ihres Unternehmens zu gewährleisten1[1].

Ein großer Teil Ihrer Kundenbasis ist demnach also bereit, das Thema Cyber-Angriffe anzugehen; sie wissen nur noch nicht wie. Und hier kommen Sie ins Spiel.

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

3. Ihre RMM-Lösung sorgt bereits für Sicherheit

Ob Sie nun darüber nachdenken, eine separate Sicherheitslösung anzubieten oder überlegen, diese direkt in Ihr Core Support Managed Services zu integrieren, da sie bereits Services, die RMM nutzen, an Ihre Kunden verkauft haben - Sie haben einen Vorteil gegenüber einem MSP, der neu in diesem Bereich ist:

- **Sie befassen sich bereits mit allen Systemen** – Da Sie RMM schon verwenden, verfügen Sie über das nötige Wissen darüber, was im Netzwerk Ihres Kunden passiert. Das bedeutet auch, dass Sie administrativ in der Lage sind, die PCs, Laptops, Server und sogar cloud-basierte Systeme Ihrer Kunden zu überwachen, verwalten, aktualisieren und zu schützen. RMM ist in vieler Hinsicht eine notwendige Basis für sämtliche Sicherheitsangebote, deren Ziel es ist, die Umgebung Ihres Kunden weiter zu sichern.
- **Sicherheit ist für Sie kein Fremdwort** – Die meisten RMM Lösungen verfügen über ein integriertes Patch Management oder das eines Drittanbieters, das nur ein rudimentäres Sicherheitslücken-Scanning von Systemen und Anwendungen bietet. MSPs werden immer eine Art von Anti-Malware-Lösung in ihre Systeme integrieren. Sie verfügen also über den Grundstock und müssen nun Ihre Sicherheitslösungen ausbauen, damit sie Ihren Kunden eine mehrstufige Sicherheitsstrategie anbieten können.
- **Ihr Kunde vertraut Ihnen** – Das ist ausschlaggebend; Sie haben bereits eine Beziehung zum Kunden aufgebaut und stehen ihm in technischen Belangen mit Rat und Weitblick richtungsweisend zur Seite und kümmern sich um die Umsetzung. Wer ist also besser als Sie dafür geeignet, den Sicherheitsaspekt zu ergänzen?

Sie stehen also vor einer Chance – eine Chance, die sie ohne Weiteres ergreifen können. Wie können Sie das angehen?

Auf Security-first setzen

Beginnend bei RMM sollte zuerst ein Sicherheitsbewusstsein in alle Servicedienstleistungen integriert werden. Mit dieser Denkweise werden Cyberbedrohungen als Betriebsrisiko wahrgenommen, welches kontinuierlich behandelt werden muss. Wir werden uns drei spezifische Schritte ansehen, die Sie durchgehen können, bevor Sie Sicherheitsdienstleistungen hinzufügen und diese in Ihr bestehendes RMM-Angebot integrieren können.

Die folgenden drei Schritte (welche wir in den nächsten Kapiteln behandeln werden) werden Ihnen dabei helfen, ein sicherheitszentriertes RMM Angebot zu schaffen, aus dem man später ein separates Sicherheitsdienstleistungsangebot erstellen kann.

Allerdings sorgt die steigende Anzahl von Cyber-Angriffen auf Klein- und Mittelunternehmen (KMU) – als solche definieren wir Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern – dafür, dass KMUs proaktiv versuchen (und somit auch die MSPs, zu denen ihre IT ausgelagert wurde) das Thema Cyber-Angriffe zu anzugehen.

Die gute Nachricht ist hier, dass Sie bereits Sicherheitskomponenten in Ihrem Angebot integriert haben (z.B. Patch-Management). Jedoch reicht es nicht aus, nur ein oder zwei Sicherheitskomponenten abzudecken, um Cyberkriminelle davon abzuhalten, in das Netzwerk Ihrer Kunden einzudringen.

- **Schritt 1: Definition der Managed Security Services** – in diesem Schritt halten Sie fest, wie Ihr Sicherheitsdienstleisungsangebot aussieht, welche Komponenten der Kundenumgebung Sie schützen wollen und wie Sie die Automatisierung in Ihrer RMM-Lösung nutzen wollen, um die Bereitstellung der Dienstleistung zu vereinfachen.
- **Schritt 2: Lösungen finden, die Ihre Service-Bedürfnisse abdecken** – Sie müssen Softwarelösungen finden, die Ihnen bei der Erbringung der Dienstleistung helfen, Komponenten erkennen, die ausschlaggebend sind, und herausfinden, wie Automatisierung in allen involvierten Lösungen verwendet werden kann.
- **Schritt 3: Suche nach Möglichkeiten, Automatisierung als Lösung für ein Problem zu nutzen** – Sicherheit gehört zu jenen Servicedienstleistungen, bei denen der Mensch nur bei der Behebung schwerwiegender Probleme eingreifen muss. Die Nutzung von Automatisierung wird eine Schlüsselkomponente bei der Bereitstellung Ihrer Dienstleistungen sein; eine, bei der Sie sich auf ihr bestehendes RMM verlassen können.

Definieren Ihres Managed Security Service Angebots

Das Hinzufügen von Sicherheitslösungen zu einem bestehenden Serviceangebot, sowie die Schaffung eines komplett neuen Serviceangebots ist nicht so einfach wie die Erstellung eines Angebots rund um eine ausgewählte Software. Wenn man seinen Kunden Cybersicherheitslösungen anbietet, muss man als MSP einen mehrstufigen Ansatz verfolgen, – und somit mehrere Lösungen nutzen, die Teil des Serviceangebots sein müssen – um sicherzustellen, dass man eine Lösung liefert, die auch tatsächlichen Schutz bietet.

Es ist schwierig, hier die richtige Balance zu finden. Ist das Angebot nicht umfangreich genug, sieht sich der Kunde mit Angriffen konfrontiert und wird sehr unzufrieden sein; ist das Angebot zu umfangreich, steigt der Kunde meist aufgrund der Kosten, der Komplexität und der scheinbaren Nichtberücksichtigung seiner Bedürfnisse zur Gänze aus. Bei der Gestaltung Ihres Sicherheitsdienstleistungsangebots sollten Sie folgende Punkte berücksichtigen:

1. **Es soll kosteneffizient sein** – KMUs brauchen Sicherheit, haben aber auch einen Preis dafür im Kopf.
2. **Es soll wirksam sein** – Was auch immer Sie anbieten, soll die Umgebung Ihres Kunden sichern und zwar gut sichern.
3. **Es soll RMM nutzen** – Wie Sie sehen werden, ist bei den meisten Angriffen (in irgendeiner Weise) der Endpoint involviert; jener Endpoint, den Ihr RMM bereits überwacht und verwaltet. Das Anbieten einer Sicherheitslösung, welche die Vorteile von RMM nicht nutzt, ist ein schlechter Dienst an Ihnen und an Ihrem Kunden.

In diesem Kapitel wird Ihr Sicherheitsdienstleistungsangebot aus einem strategischen Gesichtspunkt heraus beleuchtet und Sie erhalten Ratschläge, wie Sie festlegen können, welche Dienstleistungen Ihr Angebot umfassen sollte.

Was sollte Teil Ihres Angebots sein?

Ein wichtiger Punkt muss noch erläutert werden, bevor auf die Einzelheiten des Serviceangebots eingegangen werden kann. Es gibt MSPs, die Sicherheitslösungen anbieten, und es gibt Managed Security Services Provider (MSSP) – das ist aber nicht dasselbe. Ihr Sicherheitsangebot schafft Sicherheitsstufen, die dabei helfen, Zwischenfällen vorzubeugen, sie zu erkennen und auf sie zu reagieren. MSSPs gehen weit darüber hinaus; sie bieten Servicedienstleistungen wie Intrusion Management, Thread Hunting, Compliance Monitoring und noch viele mehr an.

Bei bestimmten Serviceangeboten gibt es Überschneidungen, die wir in diesem Kapitel behandeln werden. Wir nehmen jedoch an, dass Sie ein grundlegendes – aber effektives – Servicepaket als Teil Ihres Sicherheitsangebots anbieten möchten.

Ohne direkt auf unterschiedliche Arten von Sicherheits- Soft- und Hardware einzugehen, lassen Sie uns zuerst aus der Serviceperspektive einen Blick auf Ihr Angebot sowie auf die Frage werfen, welche Sicherheitskomponenten ihr Serviceangebot enthalten sollte.

Für jene MSPs, die Sicherheitsdienstleistungen anbieten wollen, jedoch nicht in die Rolle eines MSSPs schlüpfen möchten, gibt es fünf Servicebereiche, wo Schwachstellen behoben werden müssen. So können sie die Umgebung ausreichend sichern, ohne dass dafür viel Expertise benötigt wird. Diese Bereiche bilden eine mehrstufige Sicherheitsstrategie für Ihre Kunden, die dabei hilft, Cyber-Angriffen vorzubeugen.

Jene Bereiche des Kundennetzwerks, die MSPs von einem Sicherheitsstandpunkt aus am einfachsten angehen können, sind:

- **Perimeter** – Das Perimeter sollte als der Horizont des Kundennetzwerks betrachtet werden, wo Firewalls und Gateways die Grenze zwischen Internet und dem internen Netzwerk bilden. In den letzten Jahren ist daraus ein dynamisches Perimeter geworden, das durch die Benutzerinteraktion mit der Außenwelt definiert wird. Remotebenutzer, persönliche Geräte, öffentliches WLAN, cloud-basierte Anwendungen und Daten, Websurfen und Email haben allesamt Auswirkungen auf die genaue Definition, wo sich die Grenzen des Netzwerks befinden. Heutzutage umfasst das Perimeter auch jene Remotebenutzer, die von einem Firmengerät aus in einem Kaffeehaus irgendwo auf der Welt im Internet surfen – auch dieser Benutzer, das Gerät und die Verbindung müssen geschützt werden.
- **Netzwerk** – Jedes Gerät im Netzwerk kann zum Ziel von Angriffen werden. MSSPs denken bei Netzwerken an komplexe Methoden, wie Penetrationstests und Packet-Sniffing. Es gibt aber immer noch Dinge, die der MSP tun kann, um sicherzustellen, dass die Geräte, die sich im Netzwerk befinden, geschützt sind.

- **Endpoint** – Angreifer müssen innerhalb des Kundennetzwerks Fuß fassen und Malware benötigt eine Umgebung, in der sie sich ausbreiten kann. Deshalb ist der Endpoint ein Hauptangriffspunkt; er ermöglicht Angreifern unentdeckten Zugriff, von dem aus sie den Rest des Angriffs durchführen können. Angreifer halten sich im Durchschnitt 146 Tage innerhalb eines Netzwerks auf, bevor sie entdeckt werden.
- **Benutzer** – Phishing und Social Engineering liegen gemeinsam an erster Stelle der Angriffs-Vektoren auf KMUs[1]. Der Erfolg dieser Angriffe hängt fast immer von der Benutzerinteraktion ab. Kurzum muss ein Benutzer auf einen Link klicken oder einen Anhang öffnen, damit ein Angriff starten kann. Bei der Erstellung Ihrer Sicherheitsstrategie sollten Sie den Benutzer als Schwachstelle, aber auch als Chance zur Förderung der Sicherheit in der Kundenumgebung sehen.
- **Daten** – Im Zuge der meisten Cyber-Angriffe gibt es zahlreiche Möglichkeiten, wie Angreifer Daten zu ihren Gunsten nutzen können. Bei Ransomware-Angriffen werden Daten verschlüsselt. Bei Angriffen, bei denen Lateral Movement oder Island Hopping zum Einsatz kommen, verschaffen sich die Angreifer Zugriff auf Verzeichnisse, um Benutzerkonten zu erstellen, bearbeiten und Berechtigungen erteilen zu können. All das geschieht mit dem Ziel, einen stetigen Zugriff auf das Kundennetzwerk und die Ressourcen des Kunden zu erhalten.

Neben ihrer entscheidenden Rolle bei Cyber-Angriffen, sollte man diese Komponenten aus dem Kundennetzwerk nutzen, um eine Abwehr basierend auf einer mehrstufige Sicherheitsstrategie aufzubauen – eine Abwehr in der jede Ebene zur Erhöhung der Sicherheit beiträgt, indem sie Cyber-Angriffe mit verschiedenen Methoden angehen.

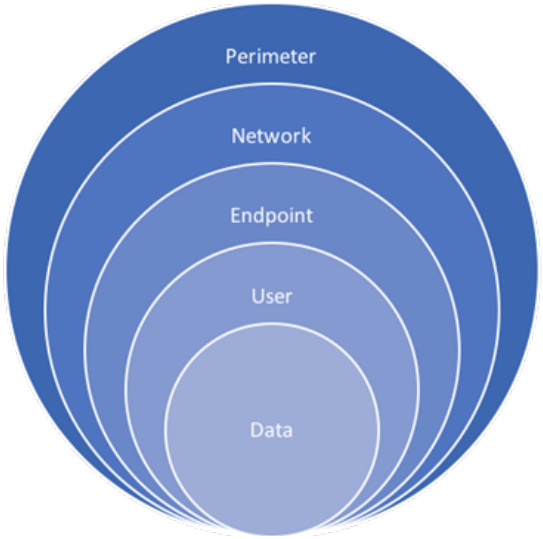
Automatisierung Ihres Angebots mit RMM

Während Sie ihr neues Sicherheitsdienstleistungsangebot planen, sollten Sie auch die Nutzung der Automatisierung, die Ihnen Ihre RMM-Lösung bietet, in Betracht ziehen. Damit können Sie Ihre Kunden auf drei Arten schützen:

1. Sie können Einsicht in den aktuellen Sicherheitsstatus des Kunden geben,
2. Sie stellen proaktiv sicher, dass die Umgebung so sicher wie nur möglich ist,
3. Probleme, die zum Risiko für den Kunden werden könnten, können Sie automatisch beheben.

Abhängig von den spezifischen Funktionalitäten Ihrer aktuellen Lösung gibt es mehrere Möglichkeiten, wie Automatisierung Ihnen mit Ihrem mehrstufigen Sicherheitsangebot helfen kann. Die nachfolgende Tabelle zeigt, wie RMM Automatisierung unterstützen kann.

Sicherheitsstufe	Nutzungsmöglichkeiten von RMM Automatisierung
Perimeter	• Vornehmen und Durchsetzen von Firewall Einstellungen zum Schutz von Laptops in öffentlichen WLAN Netzen
Netzwerk	• Überwachung von neuen Geräten, Benachrichtigung der IT bei potenziell schädlichen Systemen im Netzwerk • Bewertung und Behebung von bekannten OS Schwachstellen, die für netzwerkbasierte Angriffe auf Server mit Internetzugriff und Endpoints mit Patch Management genutzt werden • Anwenden und Durchsetzen von sanktionierten IP- Konfigurationen
Endpoint	• Identifizierung von potentiell unerwünschten Anwendungen (PUA) durch bestehende Software • Bewertung und Behebung bekannter Schwachstellen bei OS und Anwendungen, die im Zuge von Versuchen zur Infizierung von Endpoints mit Malware mittels Patch Management genutzt wurden • Abgleichen der Geräteeinstellungen mit Sicherheitsempfehlungen • Vornehmen und Durchsetzen von sicheren OS Konfigurationseinstellungen
Benutzer	• Vornehmen von Geräteeinstellungen (z.B. Deaktivieren von Macros in Office-Dokumenten), um den Benutzer vor Phishing-Angriffen zu schützen
Daten	• Überwachung von Anmeldungen auf Lateral Movement als Teil von Ransomware und Datendiebstahl



Definition von automatisierten Sicherheitslösungen

Das Ziel ist es, ein Serviceangebot zu entwickeln, das auch erbracht werden kann. In der Entwicklungsphase Ihres Angebots ist es wichtig, dass die Automatisierung an erster Stelle steht, um eine gewisse Berechenbarkeit zu erreichen und so die Rentabilität zu steigern. Da Sie bereits ein RMM besitzen, wird diese zur Basis für das Serviceangebot. Sie bauen sie dann durch weitere Sicherheitsstufen aus, die wir im nächsten Kapitel besprechen.

Auswahl von zusätzlichen Sicherheitslösungen neben RMM

Im letzten Kapitel ging es um Ihre neue mehrstufige Strategie, welche fünf Bereiche umfasst: Perimeter, Netzwerk, Endpoint, Benutzer und Daten. Für diese fünf Bereiche wurden im letzten Kapitel unterschiedliche Möglichkeiten zur Nutzung Ihrer bestehenden RMM-Lösung angeführt.

RMM verhilft jedoch nur teilweise zu einer sicheren Kundenumgebung, da der Fokus breiter ist und mehr als nur Sicherheit umfasst. Ihre RMM-Lösung sollte daher durch andere Lösungen ergänzt werden.

In diesem Kapitel werden wir über die verschiedenen Lösungsmöglichkeiten sprechen, die Sie in Betracht ziehen sollten, um ein stabiles und effektives Gesamtsicherheitsangebot zu erstellen.

Welche zusätzlichen Lösungen benötigen Sie?

RMM wurde nicht als Sicherheitslösung geschaffen; es bietet zwar Funktionen, die dabei helfen, die Kundenumgebung zu sichern, jedoch liegt der Kernfokus nicht auf Sicherheit. Um Ihr Angebot abzurunden, benötigen Sie also zusätzliche Sicherheitslösungen. Hier stellt sich die Frage, welche Arten von Sicherheitslösungen benötigt werden.

Es gibt viele Lösungen, aus denen man wählen kann – so viele, dass es schnell verwirrend wird, wenn man herausfinden will, welche Arten von Lösungen notwendig sind. Um dies aufzuschlüsseln, werden wir weiterhin ein mehrstufiges Sicherheitsmodell nutzen. Damit helfen wir Ihnen herauszufinden, welche Arten von Lösungen Sie benötigen.

Alle der fünf nachfolgenden Stufen stehen jeweils für einen bestimmten Moment während eines Angriffs, wo sich eine Möglichkeit bietet, den Angriff zu stoppen – diese sollten die Basis für die Wahl Ihrer Sicherheitslösung zum Stoppen eines Angriffs sein.

Perimeter

Angriffe können in der Form von automatisierten Scans Ihrer mit dem Internet verbundenen Systeme und Anwendungen erfolgen. Das Einsetzen einer Next-Gen Firewall, einer Web Application Firewall und eines Intrusion Detection und Prevention-Systems kann bösartige Scans und Zugriffe abwehren und somit einen Angriff rechtzeitig stoppen. Angriffe, die es schaffen, erfolgreich in ein Kundennetzwerk einzudringen, müssen sich anschließend über einen „call home“ mit einem Command and Control (C2) Server verbinden. Sämtlicher ausgehender, bösartiger Datenverkehr kann oftmals durch das Einsetzen von Domain-based Message Authentication, Reporting & Conformance (auch DMARC genannt) und DNS/URL Filter verhindert werden. Diese identifizieren und blockieren den Zugang zu bösartigen Domains und Systemen im Web.

Netzwerk

Es gibt mehrere Möglichkeiten, wie man das Kundennetzwerk für mehr Sicherheit nutzen kann. Die Einschränkung des Zugriffs auf kritische Systeme und Anwendungen (basierend auf dem Bedarf) durch Netzwerksegmentierung kann das potentielle Risiko eines Angriffs auf wichtige Ressourcen senken. Schwachstellen-Scans des Netzwerks können Patch Management Bemühungen steigern und proaktiv dabei helfen, jene Systeme und Anwendungen zu bestimmen, die anfällig für Angriffe sein könnten. Abschließend kann die Möglichkeit, den Netzwerkverkehr auf ungewöhnliche und bekannte bösartige Verkehrsmuster zu überwachen, dabei helfen, Angreifer vom Weiterführen schädlicher Eingriffe abzuhalten.

Endpoint

Wenn es ein Angriff durch alle vorherigen Ebenen geschafft hat, sollten Sie Endpoint-basierte Anti-Malware und Endpoint Detection and Response-Lösungen installiert haben, um potenziell bösartige OS und Anwendungen zu überwachen und zu blockieren.

Benutzer

Die Benutzer sind in vieler Hinsicht das schwächste Glied in der Kette; sie sind diejenigen, die unüberlegt bösartige Email-Anhänge öffnen und auf schädliche Links klicken. Das Verwenden von Web und Email Scanning Lösungen, die proaktiv nach bösartigen Inhalten suchen, bevor der Benutzer agiert, hilft dabei, den Benutzer vor sich selbst zu schützen. Benutzer können aber auch eine andere Rolle in Ihrer Sicherheitsstrategie einnehmen. Regelmäßige Schulungen des Sicherheitsbewusstseins helfen, den Benutzern die Bedeutung ihrer Rolle für die Sicherheit des Unternehmens vor Augen zu führen. Zudem lernen die Benutzer während der Arbeit wachsam zu sein und welche Angriffstaktiken und Methoden häufig verwendet werden.

Daten

Die vorherigen Ebenen dienen dazu, die Angreifer davon abzuhalten, an Daten zu gelangen. Sollte es ihnen jedoch gelingen, Zugriff auf die Daten zu erhalten, führen Ransomware-Angriffe zu Datenverschlüsselung, potentiell im gesamten Unternehmen. Zudem kommt es zu Datendiebstahl, bei dem möglicherweise die Benutzer- und Gruppenaccounts aus dem Active Directory genutzt werden, um den Zugriff zu erleichtern. Backups sollten daher Teil Ihres Sicherheitsangebots werden, um sicherzustellen, dass die Umgebung in einem guten und sicheren Zustand wiederhergestellt werden kann. Zudem ist es wichtig festzuhalten, dass einige Ransomware-Arten speziell nach lokalen Backup Dateien suchen. Daher sollte das Erstellen cloud-basierten Backups Priorität haben.

Die untenstehende Tabelle führt die empfohlenen Lösungsansätze nach Sicherheitsebene aus. Dabei handelt es sich jedoch nicht um eine vollständige Auflistung möglicher Lösungsansätze, sondern um wertvolle Lösungen, die speziell für Abwehrmaßnahmen in allen einzelnen Abschnitten eines Cyber-Angriffs entwickelt wurden.

Perimeter	• Next-Gen/Cloud-Gen Firewall • Web Application Firewall • Intrusion Detection und Prevention • DMARC • DNS/URL Filter
Netzwerk	• Netzwerksegmentierung • Schwachstellen-Scan • Netzwerk Überwachung/ Packet Inspektion
Endpoint	• Anti-Malware • Endpoint Detection and Response
Benutzer	• Email Scanner • Web Scanner • Schulungen des Sicherheitsbewusstseins
Daten	• Cloud-basiertes Backup/Wiederherstellung

Eine weitere Ebene, die in der Tabelle nicht erwähnt wurde, aber trotzdem erwähnenswert ist, ist die Identitäts-Ebene. Der Schutz der Anmeldeinformationen durch eine mehrstufige Authentifizierung ist eine einfache und effektive Methode zur Sicherstellung, dass es sich um einen echten Benutzer handelt. Zudem kann es auch von Nutzen sein, wichtige Benutzer mittels einer Art Passworttresor (auch Privileged Access Management genannt) zu schützen.

Für einen MSP, dessen Erfahrung im Anbieten von Sicherheitslösungen nicht über das Installieren eines Antivirusprogramms hinausgeht, wirkt diese Liste vielleicht etwas einschüchternd. Lassen Sie sich aber von der Tabelle nicht verunsichern; Softwarelieferanten mit Fokus auf MSP haben bereits Wege gefunden, die Implementierung und Integration dieser Lösungen zu vereinfachen, damit Sie nicht schon am ersten Tag das Gefühl haben, in einer Flut von Lösungen zu ertrinken.

Zusammenführen aller Lösungen

Sofern möglich, sollten Sie nach Wegen suchen, die Automatisierung und Integration nutzen, um die Erbringung der Servicedienstleistung zu verbessern. Im letzten Kapitel haben wir bereits über die Nutzungsmöglichkeiten von RMM gesprochen. Während Sie nach den richtigen Lösungen suchen, bestimmen Sie ähnliche Komponenten, die mehr Informationen liefern, um die Sicherheit zu erhöhen bei gleichzeitigem Senken von Risiken.

Im nächsten, und zugleich letzten Kapitel, werden wir uns mit dem Nutzen von Automatisierung für Ihre Sicherheitsdienstleistungen auseinandersetzen und Ihnen praktische Anwendungsbeispiele zeigen.

Der Nutzen von Automatisierung im Security-Bereich

MSPs haben sich von reinen IT-Profis, die alles selbst machen, weiterentwickelt. Die Herausforderung für MSPs ist es, neue Methoden, Hilfsmittel und Prozesse zu finden, die ihnen beim Wachsen helfen. Bei den meisten Dienstleistungen kann man Probleme noch manuell beheben. Auch wenn eine RMM-Lösung im Einsatz ist, die Automatisierung durch Scripting ermöglicht, entscheiden sich viele MSPs dafür, Probleme anderweitig zu beheben. Bei manchen Dienstleistungen – wie RMM und Backups – ist es (bis zu einem bestimmten Grad) möglich, die Dienstleistung manuell durchzuführen. Beim Thema Sicherheit ist das aber einfach nicht möglich.

Es gibt zahlreiche Aspekte rund um das Thema Sicherheitsdienstleistungen, die es schwierig bis geradezu unmöglich machen, den Kunden effektiv zu schützen. Zu diesen gehören:

- **Die wachsende Komplexität von Angriffen** – Im Bereich Cyberkriminalität wird stark in Methoden investiert, die einen erfolgreichen Angriff sicherstellen. Phishing-Angriffe nutzen mittlerweile hoch entwickelte Social Engineering Methoden – sie wählen sorgfältig ein bestimmtes Ziel aus, erstellen gefälschte Webseiten, die aussehen als wären sie echt, um Anmeldedaten zu stehlen und nutzen Verschleierungstechniken, die Malware davor schützen, von Sicherheitslösungen entdeckt zu werden.

- **Die Verfügbarkeit von Crimeware als Service** – Heutzutage kann so gut wie jeder, der will, ins „Geschäft“ mit Cyber-Angriffen einsteigen. Entwickler von Ransomware bieten
  z.B. ihre Software einem „Möchtegern Cyberkriminellen“ (das macht den Einstieg in die Cyberkriminalität einfach) als „Service“ ohne Vorauskosten an und werden mit einem Teil des erwirtschafteten Geldes bezahlt.
- **Der ständige Taktikwechsel** – Cyberkriminelle testen ihre Methoden kontinuierlich. Das tun sie nicht nur in Bezug auf Sicherheitslösungen, sondern auch in der Praxis, indem sie ausprobieren, was funktioniert und was nicht. Sie ändern ihre Angriffsmethoden, um zu vermeiden erkannt zu werden, steigern den Infizierungsgrad und verbessern die Erfolgsrate ihrer Angriffe.
- **Die Unvorhersehbarkeit von Angriffen** – MSPs können, wie auch jedes andere IT Unternehmen, nicht wissen, wann, wo, wie und wie groß der Umfang des nächsten Angriffs sein wird. Das macht die Problemlösung enorm schwierig.

Im Wesentlichen ist die Schaffung und Erhaltung eines Sicherheitssystems für ein KMU wie ein Ziel, dass ständig in Bewegung ist; die Bedrohungslandschaft unterliegt einem kontinuierlichen Wandel. Somit ist es für einen MSP schier unmöglich, jedem neuen Angriff oder der Sicherheitskonfigurationen jedes Systems etc. Rechnung zu tragen.

Bei der Erstellung eines Angebots, mit dem Ziel, den Kunden bestmöglich zu schützen, sollte man somit auf Automatisierung setzen: zum Schutz der Kundenumgebung, zum Vorbeugen von Angriffen durch Schwachstellen, zum rechtzeitigen Erkennen von Angriffen und für Korrekturmaßnahmen. Kurzum müssen Sicherheitslösungen Automatisierung einsetzen, um erfolgreich sein zu können.

Die Vorteile der Automatisierung

Automatisierung bietet weit mehr Vorteile als nur das Erledigen von Aufgaben ohne manuellen Eingriff; es gibt unterschiedliche Wege, wie Automatisierung den MSP bei der Ausführung einer Sicherheitsdienstleistung unterstützen kann. Diese umfassen:

- **Einheitlichkeit** – Einheitlichkeit ist unerlässlich, weil man dadurch weiß, dass die Umgebung immer gleich verwaltet wird. Wenn Sie sich entschlossen haben, eine bestehende Sicherheitskonfiguration zu verwenden oder Patches anwenden möchten, können Sie beispielsweise nicht einfach nur ein System richtig konfigurieren und alle anderen nur teilweise. Automatisierung sorgt hier dafür, dass jedes System und jede Anwendung, die verwaltet werden soll, auch wirklich verwaltet und nach den erforderlichen Vorgaben gleich konfiguriert wird.
- **Genauigkeit** – Wenn es um Bereitstellung, Verwaltung, Meldung und Schadensbehebung geht, kann es im Security-Bereich bei manuellen Tätigkeiten zu zahlreichen menschlichen Fehlern kommen. Während es beim Thema Einheitlichkeit darum geht, dass alle Systeme gleich konfiguriert sind, geht es beim Thema Genauigkeit darum, dass die spezifische Konfiguration pro System oder pro Anwendung korrekt ist. Automatisierung gibt uns die Möglichkeit, Anwendungen bereitzustellen, zu konfigurieren und zu aktualisieren, ohne sich um mögliche Abweichungen im Sicherheitssystem sorgen zu müssen.
- **Sicherheit auf dem neuesten Stand** – bei Automatisierung geht es nicht nur um das Ausführen von Skripts zur Erfüllung von Aufgaben; Automatisierung sorgt auch dafür, dass all Ihre Lösungen auf dem neuesten Stand sind, während sich die Bedrohungslandschaft verändert. Wenn z.B. neue Malware oder bösartige Domains entdeckt werden, hilft die automatische Aktualisierung der jeweiligen Lösung dabei, diese Angriffe abzublocken und verleiht Ihrem Sicherheitsangebot so einen enormen Nutzen, um den Sie sich keine Gedanken mehr machen müssen.

- **Schnellere Response** – Managed Security Services ermöglichen die Aufrechterhaltung einer sicheren Umgebung, die den Kunden schützt. Es können jedoch Probleme auftreten, z.B. wenn ein nicht gepatchtes System erkannt wird. Automatisierung kann zur Suche, Erkennung und Behebung dieser Probleme ohne menschliches Eingreifen genutzt werden und somit die Bereitstellungskosten senken.
- **Skalierbarkeit** – Wenn Sie mehrere Kunden oder mehrere Standorte eines Kunden verwalten, können Sie nur mittels Automatisierung Ihre Servicedienstleistungen ausbauen, ohne dafür mehr Mitarbeiter einstellen zu müssen, die nicht denselben Grad an Einheitlichkeit, Genauigkeit und Response gewährleisten können.
- **Berechenbarkeit** – Wird durch Automatisierung in zweierlei Form geboten. Erstens: die Bereitstellung Ihres Angebots ist aufgrund Ihrer Einheitlichkeit und Genauigkeit berechenbarer. Zweitens: die Vorteile der Automatisierung sorgen für eine berechenbarere, sichere Umgebung, von deren hohem Sicherheitsgrad Sie überzeugt sein können.
- **Rentabilität** – Berechenbarkeit sorgt für Rentabilität. Durch Automatisierung wird ein Großteil des Arbeitsaufwands direkt für den Schutz des Kunden aufgebracht. Somit ist es viel einfacher, die Dienstleistung rentabel zu machen.

Verbesserte Sicherheit durch Automatisierung

Nehmen wir nun die wichtigsten Punkte aus den anderen Kapiteln und sehen wir uns an, wie Automatisierung in der Praxis Ihr Leben erleichtern kann.

Lassen Sie uns ein paar Beispiele aus diesem eBook anschauen und prüfen, inwiefern Automatisierung (ob als Teil ihres RMM oder anderer Sicherheitslösungen) genutzt werden könnte, um Ihre Dienstleistungserbringung zu verbessern. Die nachfolgende Tabelle zeigt ein paar Methoden, wie Automatisierung in drei verschiedenen Sicherheitsphasen genutzt werden kann: Prävention, Schutz & Erkennung und Response.

Service Ebene	Automatisierungsbeispiel	Lösung
Prävention **Ziel:** Einen Angriff zur Gänze abwehren, indem man eine Umgebung schafft, die so sicher wie nur möglich ist	Überwachung des Netzwerks auf neue Geräte	RMM
	Systeme zur Überwachung von PUAs	RMM
	Aktualisierte Definitionen und Maschinenlernalgorithmen	Intrusion Detection/ Prevention DNS/URL Filter Web Scanning Email Scanning
	Prüfen, Aktualisieren und Durchsetzen von Sicherheitskonfigurationen bei Netzwerkgeräten, Betriebssystemen und Anwendungen	Firewalls RMM (Betriebssystem, Anwendungen)
	Schwachstellen-Scan, Patching	RMM (Betriebssystem, Anwendungen)
	Sicherstellung ordnungsgemäßer Backups durch Aufgabenüberwachung und Korrektur	Backup/ Wiederherstellung
Schutz/Erkennung **Ziel:** Überwachen und Erkennen von Indikatoren möglicher bösartiger Aktivitäten	Aktualisierung von Definitionen und Maschinenlernalgorithmen	Anti-Malware Endpoint Detection and Response (EDR)
	Testen und Prüfen von Anhängen	Email Scanning
	Überwachung auf verdächtiges OS Verhalten	Endpoint Detection and Response (EDR)
	Überwachung auf verdächtige oder zweckwidrige Konfigurationsänderungen	RMM
Response **Ziel:** Reaktion auf Leit- oder aktive Indikatoren eines Angriffs	Bösartige Dateien und Code-Ausführung unter Quarantäne setzen	Anti-Malware Endpoint Detection and Response (EDR)
	Ausführen von Korrektur-Scripts zur Behebung eines gefundenen Fehlers	RMM

Sicherheit durch Automatisierung

Das erklärte Ziel von MSPs ist es, Dienstleistungen anzubieten, die von Natur aus berechenbar sind. Doch Cyber-Angriffe machen es naturgemäß schwierig, dies zu erreichen. Automatisierung hilft MSPs dabei, Kundenschutz weitaus greifbarer zu machen und in Zahlen abzubilden. Dies geht von der Erstellung und Aufrechterhaltung einer sicheren Konfiguration über das Erkennen von Angriffsversuchen bis hin zum schnellen Handeln, um Schäden nach erfolgreichen Angriffen zu beheben.

Jene MSPs, die bereits RMM Servicedienstleistungen anbieten, verfügen über eine gute Ausgangsplattform, die eine erweiterbare und benutzerdefinierte Automatisierung ermöglicht. Wenn man weitere Lösungen mit einem hohen Maß an Automatisierungsmöglichkeit nutzt, tragen diese ihren Teil zu einer mehrstufigen Sicherheitsstrategie bei. So können MSPs schnell ein effizientes, reaktionsschnelles, skalierbares und planbares Modell zur Servicebereitstellung schaffen.

Sicherheitsdienstleistungen beginnen mit einem sicherheitszentriertem RMM

Es ist bereits klar, dass auch Unternehmen, die so klein wie Ihre Kunden sind, immer noch – und teilweise sogar ausgewählte – Ziele von Cyber-Angriffen sind. Es ist also zwingend notwendig, dass MSPs damit beginnen, ihren Kunden Managed Security Services anzubieten, die vor Cyber-Angriffen schützen, diesen vorbeugen, sie erkennen und auf diese reagieren.

Während Sie darauf hinarbeiten, Sicherheitsdienstleistungen zu entwickeln, zu definieren und schlussendlich auch anzubieten, ist es wichtig, jene bereits in Ihrer RMM-Lösung enthaltenen Sicherheitskomponenten in ihr Angebot zu integrieren.

In manchen Fällen können RMM Komponenten die Basis für einzelne Aspekte der neuen Dienstleistung sein (z.B. Patch Management). RMM kann aber auch mittels Automatisierung zur Steigerung der proaktiven und reaktiven Sicherheitsmaßnahmen (z.B. Überwachung und Schadensbehebung bei unbestätigten Endpoint Konfigurationsänderungen) verwendet werden. Während Sie eine mehrstufige Sicherheitsstrategie aufbauen, sollten Sie überlegen, wie jeder Teil Ihrer Strategie das RMM nutzen kann, das ja bereits Zugriff auf die Endpoints und Server innerhalb der Kundenumgebung hat.

RMM bildet eine leistungsstarke Grundlage für ein Sicherheitsdienstleistungsangebot. MSPs, die in ihren Managed Services bereits RMM-Lösungen nutzen, haben die Möglichkeit, mit einem Basisangebot zu beginnen, das im Laufe der Zeit ausgebaut werden kann. Das funktioniert jedoch nur, wenn die RMM Lösung über integrierte sicherheitszentrierte Komponenten und Automatisierungsfunktionen verfügt.

Als MSP führt kein Weg an Sicherheitsdienstleistungen vorbei; das Sicherheitsbewusstsein der Kunden wächst und sie werden sich mit ihren Sicherheitsbedenken an Sie wenden, oder einen anderen MSP suchen, der sich darum kümmert. Nutzen Sie jetzt die Chance: Beginnen Sie damit, zu prüfen, welche Komponenten Ihrer RMM-Lösung Sie nutzen können. Definieren Sie den Umfang Ihres neuen Service-Angebots, wählen Sie notwendige zusätzliche Sicherheitslösungen aus und nutzen sie die Komponenten Ihrer RMM-Lösung gemeinsam mit Automatisierung als Basis für eine neue lukrative Einnahmequelle.

MSP Barracuda®
Your journey, secured.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.
@BarracudaMSP | LinkedIn: BarracudaMSP | blog.barracudamsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com

