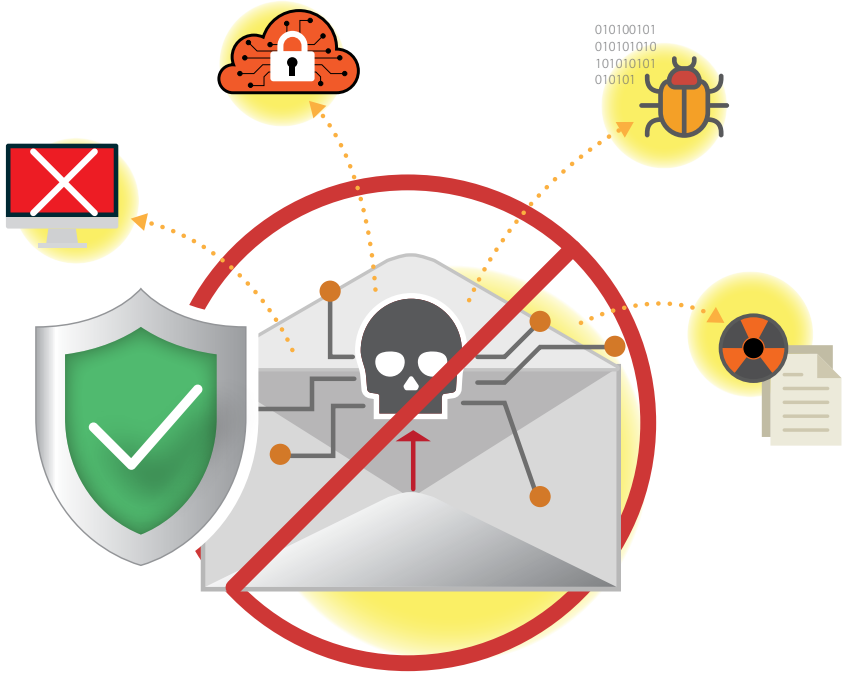
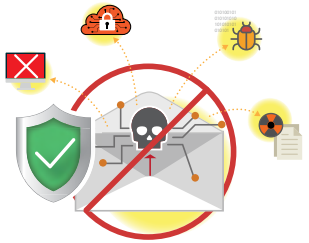
Barracuda®
MSP

Das neue "Must-Have" für MSPs:



Managed Email Security Services

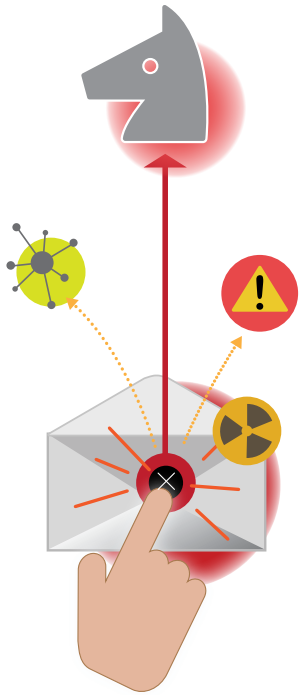


Einführung

Im Bereich der Cyber Sicherheit gibt es einen einfachen Grund dafür, dass Emails die Nummer eins Bedrohung darstellen – und es ist wahrscheinlich, dass dies sich in naher Zukunft nicht ändern wird. Menschen öffnen Emails.

Es braucht lediglich nur eine Person in der Organisation ein Attachment herunterladen oder einen Link klicken, der auf eine Webseite führt, die mit Schadprogrammen infiziert ist, um die ganze Organisation zu gefährden.

Es gibt momentan unzählige Vorfälle, bei denen Organisationen mit Erpressungstrojanern (= Ransomware) aufgeordert werden, entweder mittels einer Zahlung an Cyber Kriminelle den Zugang zu verschlüsselten Daten wiederzuerlangen oder Fälle, bei denen erhebliche Kosten bei der Datenwiederherstellung verursacht werden.



Größtenteils wurde die Malware durch einen Email Anhang verbreitet, der mit Hilfe von Social Engineering Techniken, genau dafür hergestellt wurde. Diese sind oft so gutgemacht, das auch der IT erfahrenste Endverbraucher dazu verleitet wird, den Anhang herunterzuladen.

Verwaltete Email Sicherheitsservices sind Schlüsselfaktoren für Managed Service Provider (im Folgenden MSP genannt). Ein vollständiger Kundenschutz ohne die

> “Man kann keinen rein statischen Email Security Service anbieten — genausowenig wie die Hersteller. Dazu ist die Bedrohungsvielfat zu groß und selbst zu dynamsich.”
>
> — Brian Babineau

Email-Attacken verstehen lernen.

Email Attacken verstehen lernen. Gezielte Email Attacken, die über einen gefährdeten Email Account gesteuert werden, waren in den letzten 12 Monaten der erfolgreichsten Email Attacken Überträger. Täglich werden Millionen Emails versendet, die möglicherweise versteckte Malware enthalten. Einige Branchenberichte veranschaulichen, dass die kombinierte Bedrohung von Phishing und Malicious Email Anhängen ein Drittel (34%) aller Vorfälle ausmacht.

Die meisten dieser Attacken kann man auf Social Engineering und das Vertrauen auf externe Programme, die eine Sicherheitslücke ausnutzen, zurückführen. Die Angriffe haben grundsätzlich zwei Hauptziele. Das erste ist Schadsoftware bei einem End User zu installieren, von dem aus sie sich (quer) ausbreiten kann. Das zweite ist ein weitaus hinterlistigeres Ziel. Wenn es Cyber Kriminellen gelingt, Endbenutzer dazu zu bewegen, Ihre Nutzerinformationen preiszugeben, wird es möglich, Emails die mit Schadsoftware infiziert sind, von einem seriösen Endbenutzer Email Account zu versenden. Laut einer Umfrage, die unter 140 Organisationen mit einem Durchschnitt von 16,821 Emailbenutzern, die von Osterman Forschung (2)durchgeführt wurde, kann man schätzen, **dass in den letzten 12 Monaten bereits 44 Prozent an Unternehmen Opfer von Email Angriffen durch einen gehackten End Nutzer Account waren.** Die Umfrage bestätigt auch, dass gezielte Email Angriffe durch einen gehackten Email Account die erfolgreichste Art der Email Angriffen in den letzten zwölf Monaten war. Erpressungstrojaner sind natürlich die lähmendste Form an Schadsoftware, die per Email geteilt werden kann.

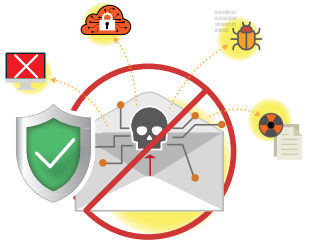
Ein Report, der durch Malwarebytes (3) durchgeführt wurde, zeigt, dass 20 Prozent der kleinen bis mittelgroßen Unternehmen, die von Erpressungstrojanern betroffen waren, alle Geschäftsvorgänge beenden mussten, um sich sofort mit dem Problem auseinanderzusetzen. Das Lösegeld, das gefordert wird, ist meist minimal, kann aber auch erheblich sein. Die direkten Kosten für das Unternehmen ist die Nicht produktive Zeit, die anfällt, ungeachtet der Tatsache ob das Lösegeld bezahlt wird, oder nicht. Der Malwarebytes Bericht zeigt zudem, dass 20% der betroffenen Unternehmen die Geschäftsprozesse einstellen mussten, eine Erpressungstrojanerinfektion **verursachte im Durchschnitt 25 oder mehr Stunden Nicht Produktive Zeit**, einige Unternehmen berichten sogar, dass Ihre Systeme für mehr als 100 Stunden nicht aktiv waren.

> “Gezielte Email Angriffe mit Hilfe eines gehackten Email Kontos war die”

1. 2018 Data Security Incident Response Report, BakerHostetler, March 2018.

2. Protecting Against Account Takeover Based Email Attacks, Osterman, April 2018.

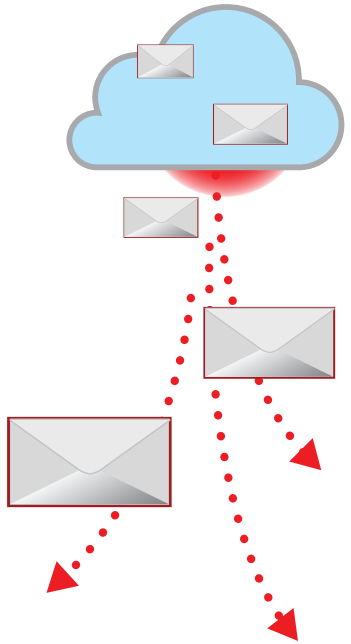
3. Second Annual State of Ransomware Report, Malwarebytes, July 2017.



Nutzen Sie die MSP Chance

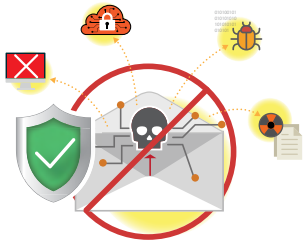
Die meisten Emails werden heutzutage über die Cloud oder über cloud basierte Dienste zugestellt. Wenn man hier angesichts der unglaublichen Menge an Emails das riesen Bedrohungspotential bedenkt, ist es nicht verwunderlich, dass der cloud basierte Email Sicherheitsmarkt im Jahr 2017 auf 701.9 Millionen USD geschätzt wird. Diese Einnahmen werden voraussichtlich spätestens im Jahr 2023 ein Volumen von 1.1 Milliarden USD haben, und somit unter dem Strich eine jährliche Wachstumsrate von 7.8 Prozent erreichen. Dabei wird ein Großteil dieser Einnahmen durch diejenigen Managed Service Provider (MSP) erreicht werden, welche die notwendige Erfahrung für ein herausragendes Email-Security Angebot mitbringen.

Dazu kommt : Im Cybersicherheitssektor herrscht nahezu Vollbeschäftigung. Kleine bis mittlere Unternehmen haben es daher besonders schwer, entsprechendes Personal mit der passenden Expertise zur Cybersecurity zu finden, zu bezahlen und vor allem auch zu halten. Da heutzutage Email die wichtigste Form der Unternehmenskommunikation ist, werden die meisten dieser Unternehmen gar nicht anders können, als sich die passenden externen Dienstleister zu suchen, die ihre Email Systeme adäquat schützen.



> "Der Cloud basierte Email Security Markt hatte 2017 ein Volumen von $701.9 Millionen. Die für 2023 veranschlagten Einnahmen bewegen sich im Bereich von $1.1 Millarden."

4. Cloud-Based Email Security Market, Orbis Research, February 2018.



Neue Email Herausforderungen für MSPs

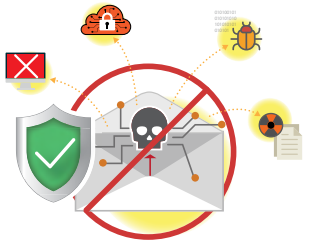
Die Hauptaufgabe eines jedes MSPs, welches sich auf Cyber Sicherheit spezialisiert hat, ist es Security Services auch adäquat anzubieten. Unternehmen jeder Größe erwarten heutzutage von ihren MSPs, dass sie als Teil eines großen Serviceportfolios auch die IT-Infrastruktur schützen. Das bedeutet im Besonderen was Emails anbelangt, dass ein MSP die E-Mail Kommunikation nicht nur schützt sondern auch sichert und archiviert.

MSP Services sollen dabei insbesondere EingangsEmails auf einen etwaigen Virus filtern, um Phishing Attacken und um Spam zu eliminieren. Ein mögliches Filtern von AusgangsEmails erweitert das Angebotsportfolio dahingehend, dass Datenverluste verhindert werden können und zum anderen sensible Daten automatisch verschlüsselt werden können. Advanced Threat Protection, abgekürzt ATP, blockiert sogenannte advanced zero hour attacks. **Die Serviceangebote, die somit einen Rundumschutz bieten sollen, beinhalten ein Sender Virus Scanning, eine Spam Bewertung, eine Echtzeit Intent Analyse, einen URL Link Schutz, Reputationsprüfungen, einen Sender Manipulationsschutz und vielzählige Domain Validation Techniken.** Es wird zudem von MSPs erwartet, dass sie in der Lage sind, outbound spam Mails und Viren zu blocken, End User oder andere infizierte Clients davor zu schützen, unwissentlich infizierte Mails zu senden sowie Mail Server IP Adressen und Domänen von Spam Blocking Listen zu halten.

Hinzu kommen Themen wie Machine Learning, Verhaltensanalyse kombiniert mit CPU Emulation basierter Sandbox um eine möglichst allumfassende Bedrohungsvermeidung zu erreichen, ohne Latenzzeiten/Wartezeiten zu verursachen. Dies wird bald als Schlüsselfaktoren gesehen werden.

> "Unternehmen aller Größen erwarten heutzutage von Ihren MSP einen full service, der die gesamte IT-Infrastruktur absichert."

Das "Neue Must-Have" für MSPs



Abschließend werden MSPs in der Lage sein müssen, Compliance Richtlinien zu entwickeln und aufrechtzuerhalten um sensible Daten wie zum Beispiel Kreditkartennummern, Sozialversicherungsnummern, HIPAA Daten, Kundenlisten und andere private Informationen davor zu bewahren, per Email versendet zu werden. Die gesetzten Policies sollten zudem in der Lage sein, automatisch zu verschlüsseln, in Quarantäne zu versetzen oder sogar bestimmte outbound Emails aufgrund ihres Inhalts, Senders oder Empfängers zu blockieren. Neue Regularien wie zum Beispiel die EU Datenschutzgrundverordnung (DSVGO), erfordern es, jederzeit in der Lage zu sein, persönlich zuordenbare Information (= personally identifiable information - PII) zu verwalten und wenn nötig zu löschen. So werden neue Compliance Herausforderungen geschaffen, wie zum Beispiel die Meldung von einer Verletzung der Verordnung an die relevanten Behörden innerhalb von drei Tagen nach dem Vorfall.

Die Herausforderung endet hier jedoch nicht. **Cloud basierte Archive** müssen so gestaltet werden, dass Unternehmen im Rahmen der Beweispflicht jeder Art von Regularien oder sogar Gerichtsbeschlüssen nachkommen können und es muss jederzeit nachvollziehbar sein, wann welche Nachricht von wem gesendet wurde.

Cloud basierte Backup Lösungen werden zudem heutzutage nicht nur verwendet, um Daten vor einem versehentlichen oder sogar bösartigen Löschen zu schützen, sondern auch um über eine identische Version mit den ursprünglichen Daten zu verfügen. Diese ist so im Falle eines Angriffs durch Ransomeware gesichert und die Daten des Unternehmens sind verschlüsselt abgelegt.

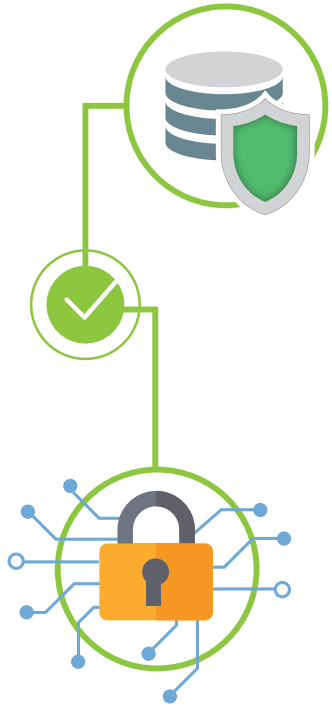
> "78% der Unternehmen sahen die EU-DSGVO und die damit verbunden Anforderungen, EU-DSGVO konform zu werden, als seine riesen Herausforderung an.[5]"

5. ISCA poll, July 2018.

Aufsetzen eines einheitlichen Sicherheitskonzepts

Heutzutage erwarten Kunden, dass Cybersicherheit und Datenschutz aus einem Guss kommen. Wenn eine Ransomware Attacke stattgefunden hat, wird ein schnellstmöglicher Recovery Prozess erwartet, um die Wahrscheinlichkeit eines kompletten Datenverlusts so gering wie möglichzuhalten.

Die Bereitstellung solcher Recovery Dienste erfordert im Normalfall erhebliche Investitionen in Sicherheits - und Netzwerkbetriebszentren, welche die Möglichkeiten und das Kapital der meisten MSPs weit übersteigen. Und selbst wenn sie das Kapital tatsächlich aufbringen könnten, wäre eine Investition in eine derartige IT-Infrastruktur wenig sinnvoll, wenn gleichzeitig Cloud-Dienste bereits verfügbar sind, die MSPs unter ihren Bedingungen die notwendigen Kapazitäten bereitstellen können. **Neben der Einführung solcher Dienste als Herausforderung sehen MSPs der noch größeren Herausforderung entgegen , eine Service Level-Integration rund um die Uhr anbieten zu können.**



Kunden möchten sicher sein, dass jeder, der ihre Geschäftskommunikation verwaltet - unabhängig davon, ob sie sich auf Microsoft Office 365, Microsoft Exchange oder G Suite von Google verlassen –die technischen und finanziellen Ressourcen besitzt um dieses Versprechen heute und vor allem auch in der Zukunft zu erfüllen. Die für die Integration von Sicherheits- und Datenschutzdiensten erforderlichen Skills sind wahrlich nicht leicht zu finden, daher müssen MSPs Prioritäten bezüglich der Investments setzen.

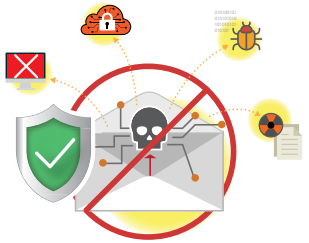
> "Kunden möchten sicher sein, eine lückenlose Bereitstellung jederzeit erforderlich sind."

Training-as-a-Service

Einer der am meisten unterschätzen Aspekte für Provider im MSP Bereich sind die notwendigen Ausgaben für persönlicheres Training. Man muss bei den End Usern erst ein gewisses Know-How Level aufbauen, dass sie Malware überhaupt erkennen können. Auf den Punkt gebracht bedeutet das, mit jedem nicht heruntergeladenen Stück Malware gibt es einen Vorfall weniger, bei dem ein MSP eingreifen muss. Das spart Zeit und Kosten und stärkt das Vertrauen in den MSP. **Es gibt die Möglichkeit, die End User so zu trainieren, so dass sie in der Lage sind, Pishing Attacken sofort zu erkennen. Daraus ergibt sich eine einzigartige Win-win- Situation für den MSP.** Der MSP kann einen abrechenbaren Service anbieten, der zusätzlich das Risiko im normalen Tagesgeschäft des gelieferten Service minimiert.

Tatsächlich sitzen End User mehr oder weniger an allererster Front und können richtig geschult einen umfangreichen, auf mehrere Eben abzielenden Angriff im Keim ersticken. Um sicher zu stellen, dass End User diese Rolle auch wirklich einnehmen können, benötigt man zu Trainingszwecken eine Saas Application, mit Hilfe derer MSPs verschiedene Arten von simulierten Pishing Attacken Nachrichten generieren können. MSPs können einerseits eine Click Raten basierte Metric zum Einsatz bringen, die trackt, wie oft Angestellte auf eine verkehrte URL klicken oder ein Stück infizierten Content herunterladen oder sie-können eine mit dem Trainingsansatz auf eine viel weiterentwickelte Technik zurückgreifen. So kann deutlich effizienter die höchste Anzahl von Attacken gemessen und dahingehend eine ganze Serie von Vorfällen verhindert werden.

Oft herrscht zwischen der IT Abteilung und den End Usern eine Kluft. Die IT-Abteilung will die End User und letztendlich das Unternehmen mit Sicherheitsvorkehrungen schützen, die End User hingegen fühlen sich durch diese Sicherheitsvorgaben in ihrem Tagesgeschäft eingeschränkt. Mit dem oben genannten Trainingsansatz können End User die IT Regularien besser verstehen und tragen aktiv zu einer Umsetzung des gesamten Sicherheitskonzepts bei.

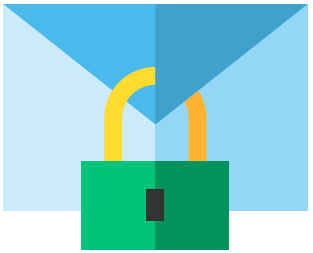


Weitere Security Möglichkeiten

Email Security und die damit verbundenen Trainingsmöglichkeiten sind nur ein Teil eines mehrschichtigen Ansatzes im Cybersecurity Bereich. Wenn ein MSP sein Secure Mail Service startet, ist der Schritt zu einem umfangreicheren Service nur noch klein: mit Hilfe einer breiten Angebotspalette von Tag täglich neuen Cybersecurity Technologien können auch die Firewalls und die Endpoint Software leicht verwaltet werden.

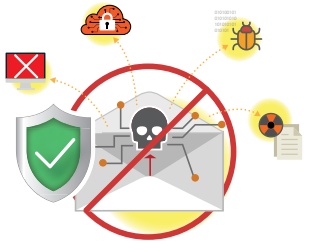
MSPs sind außerdem in der einzigartigen Position, intelligente Security Applikationen aufzusetzen, die proaktiv die Thread Prevention unterstützen. Angesichts der Tatsache, dass die Komplexität der Attacken im Cybersecurity Umfeld deutlich zunimmt, sollten MSPs sich vor Augen halten, dass sich Malware heutzutage nicht nur in den Systemen der Kunden befindet, sondern sich auch gerne in den Applikationen selbst verbergen oder umgekehrt.

Sogenannte Threat Hunting Technologien machen es deutlich einfacher, Malware proaktiv zu lokalisieren und zwar bevor sie aktiviert wird. Mittlerweile durchkämmen Intelligente Security Services das Internet nicht nur, um neue und gefährliche Bedrohungen im Dark Net ausfindig zu machen, sondern sie finden auch raus, ob und wo es sensible Daten von Unternehmen zu kaufen gibt.



Die tatsächliche Menge von angebotenen Managed Services auf dem Markt ist unübersichtlich. Jedes MSP muss demnach jeden Service einer genauen Kosten Nutzen Analyse unterziehen. Für welchen Service sich ein MSP auch immer entscheidet, **den es im Bereich Cybersecurity anbieten – alle Mangend Services sollten im Bereich Email Protection gestartet werden**. Email Kommunikation ist einfach das am häufigsten genutzte Einfallstor für alle Malware und somit der am meisten gefährdete Bereich einer IT Infrastruktur.

> “Wenn ein MSP mit einem Secure Email Service startet, ist es nur noch ein kurzer Schritt auch Firewalls und Enpoint Protection Software Services anzubieten.”



Herausforerungen und Überlegungen

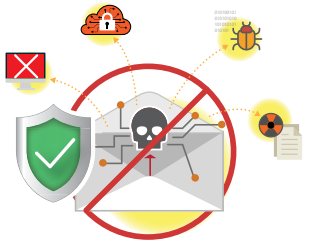
Einen Managed Security Service anzubieten ist nichts für schwache Nerven. **Es gibt keine perfekte Security, das heißt, es werden immer Security Vorfälle passieren und leider auch Malware zu finden sein, die man entfernen muss.**

Diese Aktivitäten sind enorm zeitfressend, was bedeutet, dass sicherheitsorientierte MSPs den Zeitfaktor bei ihren Kostenberechnungen mit berücksichtigen müssen. Dazu kommt das Personalproblem: In der heutigen Marktsituation sind IT Professionals mit der entsprechenden Expertise um einen Cybersecurity Service einerseits zu implementieren und anderseits Malware zu entfernen, rar gesät. Vor allem wenn diese Expertise noch dazu branchenübergreifend vorhanden sein muss. **Genau diese mangelnde Expertise im Bereich Cybersecurity macht IT Techniker zu einem den bestbezahlten Berufe in der Industrie.**

MSP müssen in Ihrer Kalkulation auch die Kosten für die entsprechenden Trainings mit berücksichtigen, einfach deswegen, weil jemand besseren einzustellen, mit bereits vorhandenen Fähigkeiten wird nahezu unerschwinglich. Aus diesem Grund müssen MSPs den angebotenen Service genau evaluieren. Je mehr Funktionalität die genutzte Plattform bietet, desto größer ist die Chance, dass auch Normalsterbliche die IT handlen können.

Die guten Neuigkeiten sind Vorteile, die sich bei einem hohen Automatisierungsgrad ergeben. Dieser senkt beständig die laufenden Kosten in der Administration und verringert gleichzeitig die komplexen Anforderungen bei Cybersecurity as a service. Aber ein hoher Automatisierungsgrad bedeutet eine gewisse Anfangsinvestition. Wenn man in die Zukunft schaut, ist bereits jetzt ersichtlich, dass die nächste Generation von Cybersecurity Solutions auf einem sehr hohen Level maschinen basiert sind. Sie benötigen einen Deep Learning Algorithmus, um die AI weiterzuentwickeln. Diese Algorithmen entwickeln sich nur mit der Analyse von riesigen Datenmengen effektiv weiter. Das ist ein weiterer Grund für ein MSP, sich mit einem Cloud Service Partner zusammen zu finden- ganz einfach deshalb, weil die meisten MSPs für sich alleine Datenmengen für ein effizientes AI Modell nicht sinnvoll aufbereiten können. Eine Weiterentwicklung für einen automatisierten und verkaufbaren Cybersecurity Prozess ist so scheinbar unmöglich.

Tatsächlich ist die AI auch ein vorrangiger Grund für MSPs, sich auf einen Cloud Service zu verlassen, gerade wenn sie einen Emails Security Service anbieten. Einen Email Security Dienst anzubieten, der On Premise Hardware and Software nutzt, ist teuer und aufwendig. Um für die AI relevante Daten zu sammeln und zu verwahren, ist es deutlich einfacher und kostengünstiger einen Hersteller zu suchen, der Email Security Services genau auf die jeweiligen Bedürfnisse eines MSPs zugeschnitten anbietet.



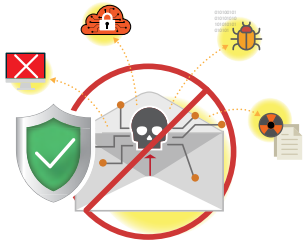
Der tatsächliche Wert von Email Security Services

Am Ende der Tage muss ein MSP sicherstellen, dass der angebotene Security Service im Vergleich einen echten Mehrwert bietet. Dashboards, die high-level Reports anbieten, sind hier immens wichtig, um eine Skalierung des angebotenen Service aufzuzeigen.

Allzuoft bewerten Kunden die Qualität eines Service Anbieters nur nach der Anzahl der negativ Erfahrungen, die sie gemacht haben. Wenn man Cybersecurity allerdings nur nach diesem Kriterium beurteilt, kann das problematisch sein. Oft zeigt sich die Qualität und demzufolge der tatsächliche Wert eines Services erst bei der Threat Prevention. Wenn allerdings nichts weiter passiert, wird der Service automatisch als „schlechter" bewertet. Das ist insofern kurzsichtig, da ja im Hintergrund genannte Präventionsmaßnahmen laufen. Bleibt man in diesem Gedankenmodell, bedeutet das aber auch im Umkehrschluss, dass diese als „schlechter" bewerteten Service automatisch billiger sein müssen.

Für ein MSP gestaltet es sich schwierig, einerseits dem hohen Qualitätsstandard im Security Business gerecht zu werden, aber letztendlich in der Wahrnehmung nach Aussen nur nach den tatsächlich eingetretenen Schadensfällen bewertet zu werden. Hält man sich die menschliche Schwäche vor Augen, wird es immer Sicherheitsvorfälle geben, auf die reagiert werden muss. Das kritische an dieser Tatsache ist, dass zwar einerseits auf diese Vorfälle sofort reagiert werden muss, aber auf der anderen Seite diese Vorfälle nicht die einzige Sache sein darf, an die sich der Kunde erinnert. Sonst wird die Qualität eins Services nur Schadensvorfällen bemessen.

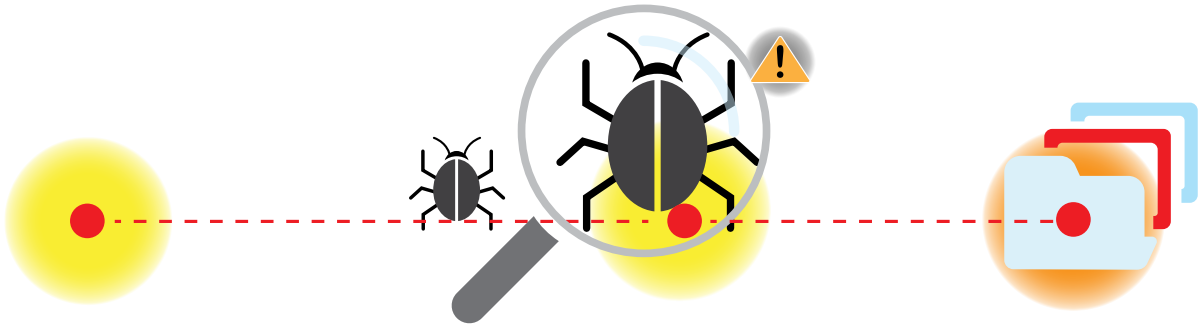
> "Dashboards, die hoch standardisierte Reports anbieten, können die Skalierung eines Services bestmöglichst aufzeigen."

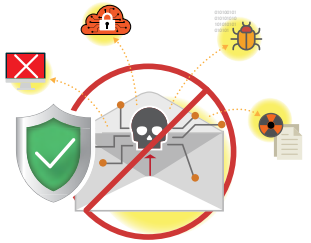


MSPs sollten außerdem kritisch bei der Auswahl ihrer Kunden sein. Organisationen, die zum Beispiel ältere Windows Versionen haben, sind deutlich teuer zu supporten als solche, die bereits in neuere Technologien und dazugehörige IT Equipment investiert haben. Ältere Versionen von Applikationen und Betriebssystemen haben eine deutlich höre Einfallsquote für Cyberattacken und erfordern so von Seiten des MSPs einen immensen Aufwand für das Patch Management.

Die meisten Infektionen mit Malware passieren tatsächlich auf Grund der Tatsache , dass Applikationen und Systeme nicht vernünftig auf dem neuesten Stand der Technik verwaltet wurden. Tatsächlich sind oft Organisationen, die ältere Versionen im IT Bereich laufen haben, auch keine innovativen Organisationen. Sie vertreten häufig den Standpunkt, dass eine vernünftige und moderne IT Strategie einen erheblichen Mehrwert für das Unternehmen bringt. Die Chancen bei solchen Kunden stehen also hoch, dass sie einerseits die Kosten für Security Service möglich gering halten wollen, aber zur gleichen Zeit deutlich mehr Ressourcen benötigen und diese auch noch zu einem möglich geringen Preis. Bevor also ein MSP in die unangenehme Lage gerät, so einen Kunden eines Tages kündigen zu müssen, sollten sie lieber gleich im Vorfeld solche Art von Kunden bei der Akquise hinten an stellen.

> “Die meisten Malware Infektionen können auf unzureichend gewartete und veraltete IT Systeme zurückgeführt werden.”





Zusammenfassung

Es ist nicht möglich heutzutage ein neues IT Projekt herauszubringen, was sich nicht mit Security beschäftigt. Wenn ein MSP also zukunftsfähig bleiben will, müssen sie Managed Services in ihr Portfolio mit aufnehmen und zwar entweder auf Basis ihrer eigenen Ressourcen oder sie partnern mit einem andern Service Anbieter.

Kunden werden außerdem nur MSPs beauftragen, die Security Produkte für den Kommunikationsprozess anbieten und zwar genau auf ihr Business zugeschnitten. Sie werden keine MSPs beauftragen, die nur die Geschäftsprozesse ohne Email Security managen. Das ist unter anderem deswegen so wichtig, weil viele Organisationen aktuell auf eine digitale Transformation fokussiert sind. Angesichts der Tatsache wieviel Anteil Emails am heutigen Tagesgeschäft haben, werden die meisten Kunden lieber auf ihren Telefonanbieter verzichten, bevor die Emails nicht mehr funktionieren.

Um die notwendige Expertise zu erhalten, um wirklich sichere Email Services anzubieten, müssen MSPs mit einem Hersteller partnern, der für sich selbst die Notwendigkeit von Investment in den Security Bereich erkannt und diese dann auch getätigt hat. Der Sieger im Cybersecurtity Game setzt auf Prävention. Je weniger Malware über Emails in die Systemen eindringen können, desto weniger Vorfälle passieren. Im Bereich Cybersecurity, ist Prävention das Maß aller Dinge.

Erfolgreiche Cyberattacken kosten sowohl die MSPs Unsummen bei den Recovery Maßnahmen und verursachen anderseits bei den Kunden immense Kosten bei einem Datenverlust. Wenn also MSPs wettbewerbsfähig und erfolgreich bleiben wollen, müssen sie sich auf die Bedürfnisse ihrer Kunden einstellen, vor allem im Bereich E-Mail Protection.

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 platform. 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.