CYREN

WARUM MICROSOFTS ATP OFT NICHT AUSREICHT

2019 veröffentlichte Osterman Research einen Bericht zur Sicherheit in Office 365. Die Osterman-Forscher kamen zu der Schlussfolgerung, dass Office 365 zwar eine robuste und leistungsfähige Plattform ist, eine Plattform vom Umfang und von der Größe von Office 365 aber nie in der Lage sein wird, alle Aufgaben für jede Organisation und in jedem Szenario abzudecken.

In dem Bericht wurde eine Reihe von Problemen mit der Suite von Sicherheitslösungen von Microsoft offengelegt. Zum Beispiel behauptet Microsoft, dass seine Lösungen Advanced Threat Protection und Exchange Online Protection jeden Monat 600 Millionen schädliche E-Mails unter 400 Milliarden E-Mails identifizieren, was eine Bedrohungserkennungsrate von 0,15 Prozent bedeutet. Dies ist aber signifikant niedriger als die Bedrohungserkennungsrate für schädliche E-Mails anderer Lösungsanbieter.

Forschung wie diese und häufige Medienberichte über Cyberangriffe, die die Sicherheitslösungen von Microsoft passieren, heben hervor, wie unzureichend solche Lösungen allein sind. Microsoft entwickelt seit langem Sicherheits-Tools, mit denen die Hauptproduktkategorien des Unternehmens ergänzt werden. Während diese Tools selten in diesen Kategorien als „Best of Breed"-Produkte gelten, herrscht auch Verwirrung in Bezug auf die E-Mail-Sicherheitsangebote von Microsoft und riesige Lücken bei deren Anwendbarkeit und Ergebnissen.

Microsoft hat ganz einfach zu viele Lösungen, von denen manche überlappen und andere beträchtliche Lücken lassen. Dies hat wiederum zur Folge, dass keine kohärente Strategie zum Schutz der Unternehmens-Mailboxen besteht.

Hier wird erläutert, warum die Lösungen von Microsoft Unternehmen nicht vor Cyberangriffen schützen und was Unternehmen bewerkstelligen müssen, um vollständig geschützt zu werden.

ERFAHREN

WAS IST ATP?

Im April 2015 erfolgte die Einführung von Office 365 Advanced Threat Protection (ATP) durch Microsoft. Zum Zeitpunkt der Einführung war ATP (damals noch als Exchange Online Advanced Threat Protection bezeichnet) darauf ausgelegt, als E-Mail-Filterservice zum Schutz vor bestimmten Arten fortgeschrittener Bedrohungen zu fungieren.

ATP bietet zusätzlich zu Exchange Online Protection (EOP) von Microsoft, einem cloudbasierten Filterservice zum Schutz vor Spam und Malware, eine weitere Sicherheitsebene. Der Standardsicherheitsservice scannt jede in Transit befindliche Nachricht in Office 365 und blockiert alle in einer Nachricht enthaltenen schädlichen Hyperlinks. Außerdem setzt er auf drei verschiedenen Engines basierenden Antivirenschutz gegen bekannte Malware und Viren ein. Als zusätzliche Sicherheitsstufe bietet Microsoft auch Zero-Hour-Auto-Purge (Automatische Bereinigung zur Nullstunde) oder ZAP. Diese Funktion erfasst und neutralisiert rückblickend schädliche Phishing-, Spam- oder Malware-Nachrichten, die bereits Exchange Online-Mailboxen zugestellt wurden.

Während EOP bei allen Microsoft 365-Installationen mit Exchange Online-Mailboxen enthalten ist, muss für ATP eine zusätzliche Gebühr entrichtet werden. ATP weitet den EOP-Schutz mithilfe einer als „Sichere Anlagen" bezeichneten Funktion aus, die Messaging-Systeme vor unbekannter Malware und Viren schützt sowie Zero-Day-Schutz bietet.

Warum diese Tools nicht ausreichen

Microsoft bietet keine Enterprise-Cybersicherheits-Teams mit kohärenter Strategie zum Kampf gegen Phishing und Geschäfts-E-Mail-Compromise-Angriffen.

Das E-Mail-Sicherheitsportfolio von Microsoft besteht aus nicht miteinander verbundenen Lösungen, wodurch signifikante Komplexität für alle entsteht, die versuchen, eine umfassende Strategie zu verstehen, zu implementieren und zu verwalten und diese überall in ATPv1, ATPv2, EOP und ZAP einzuführen. Es kann äußerst schwierig sein zu wissen, welche Einstellung in welcher Funktion Vorrang hat bzw. in welchem Tool sich die relevanten Einstellungen befinden.

Trotz der in ATP und EOP von Microsoft enthaltenen Funktionen schaffen es schädliche E-Mails in die Mailboxen und werden Benutzer Opfer böswilliger Kampagnen.

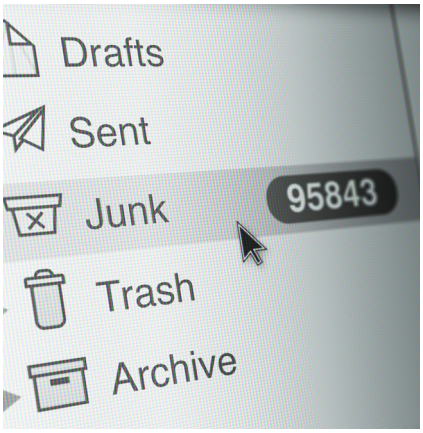
Das liegt daran, dass Angreifer Kampagnen erstellen, die speziell darauf ausgerichtet sind, Schwachstellen in ATP auszunutzen. Mit 180 Millionen Benutzern ist Microsoft einer der beliebtesten E-Mail-Dienste der Welt und wird dadurch zu einem Hauptziel von Cyberangreifern.

Die Lösungen von Microsoft sind aber unzureichend, um Angriffe jeder Art abzuwehren. Sie erfassen Spam und Malware, können aber BEC-Angriffe und selbst bestimmte Phishing-Kampagnen nicht effektiv erkennen. Die meisten Anti-Phishing-Softwarelösungen verlassen sich auf Listen bekannter Bedrohungen. Die Bedrohungen entwickeln sich aber ständig weiter. Bis eine Kampagne erkannt und in die Datenbank aufgenommen wurde, sind bereits fünf neue an ihrer Stelle entstanden. Diese Lösungen ignorieren auch File-Sharing, Messaging und andere Phishing-Angriffsvektoren.

Microsoft ATP verlässt sich auf seine Sicherer-Link-Funktion, die URLs in E-Mails umschreibt, bevor diese dem Benutzer zugestellt werden. Dies kann dazu genutzt werden, die URL an den URL-Prüfservice zuleiten, um Time-of-Click-Analyseschutz zu bieten. Die Herausforderung bei diesem Ansatz ist die Benutzererfahrung. Wenn Benutzer auf eine URL klicken, erwarten sie, die Ziel-Website in einer Sekunde zu erreichen. Dadurch bleibt keine Zeit für eine gründliche Echtzeitanalyse der URL und Ziel-Website, wodurch Microsoft sich auf Listen bekannter schädlicher URLs verlassen muss.

Techniken zur Umgehung der Phishing-Detektion entwickeln sich ständig weiter, daher können wir einen Anstieg bei Angriffen beobachten, bei denen die Phishing-URLs in Anlagen versteckt werden. Microsoft kann zwar URLs in Office-Dokumenten umschreiben und ersetzen, allerdings nur in diesen. Anlagen wie PDF-Dateien, HTML-Dateien, Archive (ZIP-Dateien) und selbst angehängte E-Mails (die oft eingesetzt werden), bleiben ungeschützt.

Die Lösungen von Microsoft bieten auch nur geringes Benutzer-Engagement, obgleich sich genau das als eine Kernkomponente jeder erfolgreichen Anti-Phishing-Strategie erwiesen hat. Von ZAP ausgeführte Aktionen bleiben für Benutzer unsichtbar, weil sie nicht benachrichtigt werden, wenn eine ihrer E-Mails gezappt wurde, und ihnen auch nicht mitgeteilt wird, warum E-Mails im Junk-Ordner enden. Microsoft bietet keine Möglichkeit für Mitarbeiter an vorderster Front, einen Live-Scan einzuleiten, und auch keinen definierten Zeitrahmen für die Meldung falsch positiver oder falsch negativer Ergebnisse an beim Benutzer. Microsoft bietet keine Benutzerbenachrichtigungen, wodurch nicht nur die Benutzerbeteiligung auf der Strecke bleibt, sondern Benutzer auch uninformiert bleiben.



Die Microsoft-Lösung bietet keinerlei Flexibilität. Alle E-Mail-Nachrichten werden unabhängig vom Ursprung der E-Mail oder deren Lesestatus in den Junk-Ordner befördert. Darüber hinaus müssen Benutzer in ATP Benachrichtigungen konfigurieren, um eine automatisierte Untersuchung einzuleiten. Remediationsaktionen werden zwar empfohlen, es werden aber keine Maßnahmen automatisch ergriffen.

> **Diese Unzulänglichkeiten zeigen, warum schädliche Kampagnen die Verteidigungslinien von Microsoft immer wieder erfolgreich durchbrechen.**

Was Sie wirklich brauchen

Unternehmen benötigen eine klare und umfassende Strategie und Plattform mit einem integrierten Funktionssatz, der eine intuitive Benutzererfahrung bereitstellt, die ganz auf die individuellen Systembenutzer zugeschnitten ist.

Für einen vollständigen Schutz benötigen Unternehmen eine Lösung mit durchgängigen, robusten integrierten Funktionen. Zu einigen kritischen Merkmalen zählen:

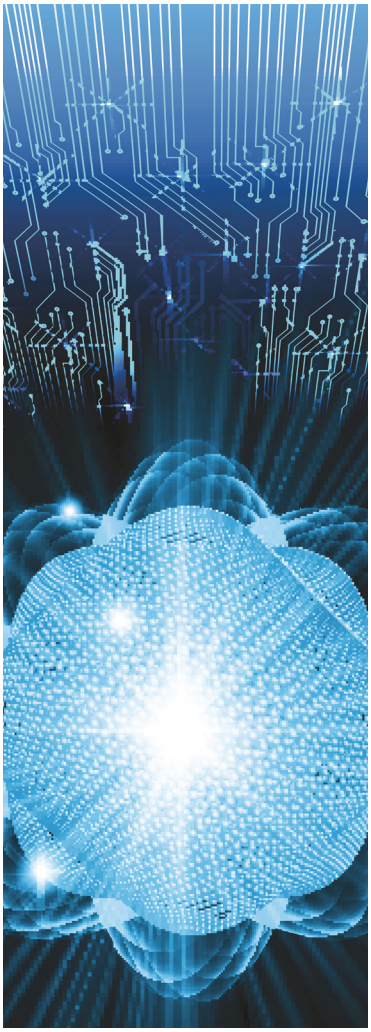
ONBOARDING-ERFAHRUNG FÜR IT/SECOP-TEAMS

Von der Onboarding-Erfahrung ausgehend benötigen Unternehmen eine schnelle und effiziente Lösung, die leicht mit Office 365 integriert werden kann. Dies sollte automatische Konfigurationen und native Abonnementintegration mit Office 365 umfassen. Die Lösung sollte auch unabhängig von sicheren E-Mail-Gateways operieren und eine pro Benutzer bzw. Gruppe verwaltete Remediationsrichtlinie bieten.

Bei der Einrichtung der Plattform ist eine flexible Remediationsrichtlinie ausschlaggebend. Dies sollte die Berücksichtigung des E-Mail-Ursprungs (extern/intern) sowie des Lesestatus von E-Mail-Nachrichten umfassen.

AUTONOME DETEKTION UND REMEDIATION

Unternehmen benötigen eine Lösung mit autonomer Detektion und Remediation. Dies sollte Echtzeit-URL-Analyse von E-Mails und Anlagen sowie E-Mail-Bedrohungsbeurteilung basierend auf Indikatoren wie Kopfzeilen, Text, Anlagen und URLs umfassen. Die Lösung muss eine kontinuierliche Detektion mit stets aktuellen Bedrohungsdaten bieten. Um effektiv zu sein, sollte die Lösung auch rückblickendes Scannen von E-Mails bis zu 14 Tage in der Vergangenheit, adaptive Compromise-Indikatoren und Selbstreparatur bei falschen Positiven bieten.



Ein umfassender rückblickender Scan jeder Mailbox über 14 Tage ist von grundlegender Bedeutung, wenn neue Benutzer auf der Plattform integriert werden, um schädliche E-Mails zu beseitigen, die den bestehenden Schutz bereits überwinden konnten.

Die URL-Analyse sollte sowohl für die E-Mail selbst als auch die Anlage in Echtzeit erfolgen. Die Phishing-URL-Detektion von Microsoft basiert auf einer statischen Liste. URLs werden einmal bei der Lieferung und einmal beim Klick mithilfe der Sicherer-Link-Funktion geprüft. Diese Funktion ist aber lediglich auf die Analyse der anfänglichen URL beschränkt.

Während Microsoft-Lösungen Spam und Malware entdecken, erfassen sie nur manche Phishing-Angriffe und BEC überhaupt nicht.

FALLMANAGEMENT UND -UNTERSUCHUNG

Hinsichtlich Fallmanagement und -untersuchung sollte die Lösung automatische Incident-Fall- sowie E-Mail-Bedrohungssuche und manuelle Fallerstellung umfassen.

Die Plattform sollte die Anforderungen und Verfahren der SOC-Analysten berücksichtigen, die mit der Vorfalluntersuchung betraut werden. In Zusammenhang stehende Vorfälle sollten zu Fällen aggregiert werden. Wenn z. B. ein Link an mehrere Empfänger gesendet wurde, sollte ein einziger Fall mit klaren Remediationsaktionen für alle darin enthaltenen Vorfälle erstellt werden.

Den SOC-Analysten sollten relevante Fallinformationen mit detaillierter Forensik einschließlich Compromise-Indikatoren für URLs (mit Website-Screenshot), Absenderverkörperung und schädliche Dateien bereitgestellt werden.

Lösungen sollten auch verwaltete 24/7-Vorfallreaktionsdienste umfassen, die präzise auf Untersuchung, Analyse, Lösung und Remediation offener, von Benutzern gemeldeter Vorfälle sowie die Untersuchung ähnlicher E-Mails und verdächtiger Low-Confidence-Vorfälle fokussieren.

BESCHAFFEN SIE BENUTZERINTELLIGENZ PER CROWDSOURCING

Mitarbeiter in den Kampf gegen Phishing und BEC einzubinden ist für den Erfolg des Programms ausschlaggebend. Effektive Lösungen nutzen in E-Mails integrierte Banner, um Benutzer zu benachrichtigen und ihr Bewusstsein um Phishing- und Verkörperungsangriffe zu steigern. Mithilfe von Bannern werden Benutzer am Kampf gegen das Phishing beteiligt.

Darüber hinaus kann ein Live-Scan der E-Mails durch Benutzer und Mitarbeiter helfen, falsch Positive oder falsch Negative zu melden.

Um sich vor schädlichen E-Mails zu schützen, benötigen Unternehmen bessere Werkzeuge. Cyren Inbox Security kann Ihr Unternehmen auch vor den ausgetüfteltsten Evasive-Phishing-Angriffen schützen und sicherstellen, dass schädliche E-Mails nicht in falsche Hände geraten. Weitere Informationen finden Sie hier.