Drei Schlüsselfaktoren zur Absicherung von Microsoft 365

Barracuda

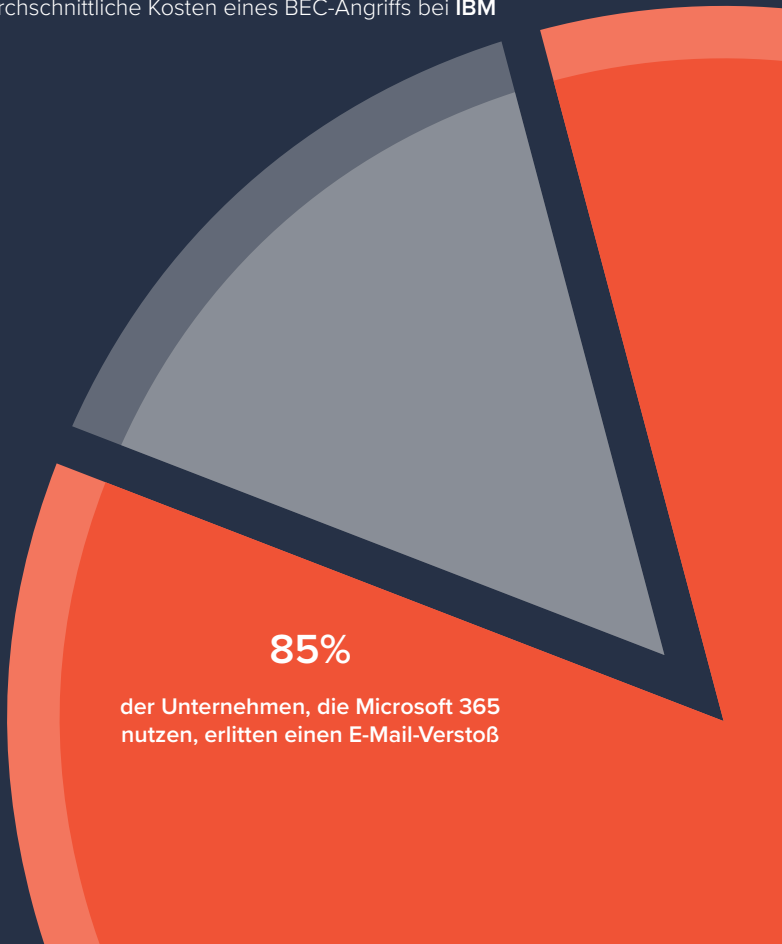
Durch Popularität zum beliebten Angriffsziel

Über 1 Million Unternehmen verlassen sich heute auf Microsoft 365, eine Reihe von Tools, die die Produktivität und Kommunikation unterstützen. Sie umfassen E-Mail-Dienste, Cloud-Speicher, Dokumentenaustausch und Messenger-Dienste. Microsoft Outlook sowie Teams haben sich aufgrund der COVID-19 Pandemie und der breiteren Akzeptanz des Arbeitens im Home-Office zu einem noch wichtigeren Bestandteil der Geschäftskommunikation entwickelt.

Allerdings hat Microsoft 365 auch seine Schwächen. Untersuchungen von Egress ergaben, dass 85% der Firmen, die Microsoft 365 verwenden, seit März 2020 einen E-Mail-Verstoß erlitten und einen Anstieg der auf E-Mails basierenden Datenlecks um 67% gemeldet haben. Wenn IBM die durchschnittlichen Kosten eines Business Email Compromise (BEC)-Angriffs mit gewaltigen 4,89 Millionen USD angibt, ist eines klar: E-Mail-Angriffe bleiben ein beliebter und lukrativer Angriffsvektor für Cyberkriminelle.

$4,89M

durchschnittliche Kosten eines BEC-Angriffs bei **IBM**



Microsoft 365 weist Sicherheitslücken auf

Obwohl Microsoft 365 über eine eigene Sicherheitsinfrastruktur verfügt — Microsoft Defender für Office 365 (MDO) — weist diese Sicherheitslücken auf.

Erstens reichen die nativen Funktionen von Microsoft einfach nicht aus, um vor gezielten personalisierten Bedrohungen zu schützen. Zum Schutz vor diesen Bedrohungen unterstützt Gartner die Empfehlung Lösungen von Drittanbietern zu verwenden und betont, dass es wichtig ist:

"Die nativen Funktionen Ihrer vorhandenen E-Mail-Lösungen in der Cloud mit Sicherheitslösungen von Drittanbietern zu ergänzen, Phishing-Schutz für Zusammenarbeitstools bereitzustellen und sowohl für mobile als auch BEC-Phishing-Szenarien gerüstet zu sein."

Barracuda

Zweitens sind Ihre Microsoft 365-Daten nicht vor versehentlichem oder böswilligem Löschen geschützt.Tatsächlich empfiehlt Microsoft in seiner Servicevereinbarung, „Inhalte und Daten, die Sie mit Apps und Diensten von Drittanbietern speichern, regelmäßig zu sichern“ und räumt ein, dass Unternehmen ohne eine Drittanbieterlösung zur Datensicherung Gefahr laufen, wichtige Informationen zu verlieren.

Um die Lücken, die durch die unzureichenden Sicherheitsfunktionen von MDO entstehen, zu schließen, empfehlen wir bei Barracuda einen 3-Säulen-Ansatz zur Absicherung von Microsoft 365 — **pAbwehr und Erkennung von sowie Reaktion auf Bedrohungen, Datenschutz und Compliance**. In diesem E-Book erfahren Sie, wie Sie jede dieser Säulen angehen, die Sicherheit Ihrer Microsoft 365-Anwendungen sicherstellen und ein Schutzkonzept gegen kostspielige E-Mail-Bedrohungen erstellen.

Threat prevention

Prävention ist immer die bessere Option.Doch welcher Präventionsansatz ist der richtige, wenn es um Angriffe geht, bei denen große Mengen an E-Mails versendet werden und die immer raffinierter werden?Wirksame Prävention findet statt, bevor E-Mails die Postfächer der Unternehmen erreichen.Alles, was danach kommt, gilt als Vorfallsbehebung und gefährdet Ihre Systeme.

Erfolgreiche E-Mail Angriffe gefährden sowohl Ihre Daten als auch Ihre Geschäftskontinuität. Daher ist es wichtig, dass Sie Systeme einrichten, um solche Ausfälle zu verhindern.KI-gestützte E-Mail-Schutztools können Phishing-Angriffe bekämpfen und Zero Trust Network Access (ZTNA) — die Sicherung des Benutzerzugriffs auf geschäftskritische Anwendungen — sollte Ihre erste Maßnahme sein.ZTNA sorgt für einen sicheren Zugriff, indem Sie genau festlegen, welcher Benutzer auf verschiedene Bereiche des Netzwerks zugreifen kann und Benutzern keinen unnötigen Zugriff gewähren, wenn diese ihn nicht benötigen — was zu Problemen beim Zugriff auf oder der Weitergabe von vertraulichen Daten führen könnte.

Herkömmliche E-Mail-Gateways sollen Angriffe unterbinden und als erste Verteidigungslinie fungieren, um zu verhindern, dass Spam, Malware und andere E-Mail-Nachrichten mit bösartigen Payloads in den Posteingängen der Benutzer landen.Allerdings nutzen Hacker Social Engineering-Taktiken, um diesen Schutz zu umgehen.Drittanbieterlösungen gehen einen Schritt über den herkömmlichen Gateway-Schutz hinaus und nutzen API-basierte Sicherheitsmechanismen auf Inbox-Ebene, die jene Bedrohungen erkennen, die das Gateway umgehen, um in die E-Mail-Posteingänge der Benutzer zu gelangen.API-basierte Sicherheitsmechanismen lassen sich in die Postfächer der Mitarbeiter integrieren und greifen auf den historischen internen und externen E-Mail-Verkehr zu.Sie lernen die Verhaltensmuster jedes Benutzers, um Anomalien zu erkennen und Angriffe abzuwehren, einschließlich solcher, die von internen Konten ausgehen — eine entscheidende Funktion zur Erkennung von Kontoübernahmen.

Das Herzstück einer solchen Lösung ist eine KI-Engine, die Social Engineering-Angriffe in Echtzeit erkennt, blockiert und die am stärksten gefährdeten Mitarbeiter identifiziert.Die Engine nutzt mehrere Klassifikatoren, um die sozialen Netzwerke jedes Einzelnen im Unternehmen abzubilden, erkennt anomale Signale in den Metadaten und Inhalten der Nachrichten und bietet so Echtzeitschutz vor gezielten Angriffen.Herkömmliche sichere E-Mail-Gateways geben keine Einblicke in die interne Kommunikation und können daher Angriffe von internen Benutzern nicht abfangen.Darüber hinaus führt ihre übermäßige Abhängigkeit von vorab festgelegten Richtlinien dazu, dass ihnen diese gezielten Angriffe entgehen.API-basierte Abwehrmechanismen gehen über diese herkömmlichen Lösungen hinaus und erkennen Risikofaktoren in der internen und externen Kommunikation, um Unternehmen in beiden Fällen vor Anomalien oder Angriffen zu schützen.Wie bereits erwähnt, stellen Lösungen wie diese die zusätzliche Verteidigungsebene dar, die von Gartner empfohlen wird.

Für eine erfolgreiche Abwehr von E-Mail-Bedrohungen ist es von entscheidender Bedeutung Lösungen zu implementieren, die von Anfang an bösartige E-Mails daran hindern, über das Gateway in die Geschäfts-E-Mail-Konten zu gelangen.

Obwohl MDO Funktionen gegen Spam, Malware und Datendiebstahl umfasst, können komplexere Angriffe wie laterales Phishing und Identitätsmissbrauch dennoch ihren Weg in die Posteingänge finden.Diese Angriffe zielen darauf ab, herkömmliche E-Mail-Gateway-Lösungen zu umgehen. Daher ist es wichtig, Lösungen von Drittanbietern einzusetzen, um Ihre Geschäfts-E-Mail-Konten zu schützen.

Erkennung und Reaktion

So gut jede Präventionsmethode für sich auch ist, besteht immer die Gefahr, dass ausgefeilte, bösartige E-Mails doch in den Posteingängen der Benutzer landen.Ihre Mitarbeiter können bei der Gewährleistung der Sicherheit Ihres Unternehmens eine entscheidende Rolle spielen.Es ist wichtig, Ihre Mitarbeiter über die Risiken von E-Mail-Bedrohungen aufzuklären und darüber zu informieren, was zu tun ist, sobald diese auftauchen, unabhängig davon, wie zuverlässig die von Ihnen eingesetzte Lösung ist.

Durch den Einsatz eines API-basierten Schutzkonzepts, kann man einen großen Teil des mit BEC verbundenen Risikos beseitigen. Schulungen zum richtigen Verhalten im Fall einer Bedrohung, die im Posteingang eines Benutzers landet, sollten jedoch integraler Bestandteil Ihrer Strategie zur Absicherung von Microsoft365 sein.Der Einsatz eines Tools für Schulungen zur Stärkung des Risikobewusstseins (SAT), die Benutzer über die Risiken von Phishing- und Social-Engineering-Angriffen aufklären und darüber informieren, wie man sie erkennt, ist unerlässlich, wenn Ihre Mitarbeiter dazu in der Lage sein sollen, potenzielle Bedrohungen in ihren Posteingängen zu identifizieren und bestmöglich darauf zu reagieren.Neben der Fähigkeit potenzielle Bedrohungen zu erkennen, ist es wichtig, dass die Mitarbeiter wissen, an wen sie diese melden sollen.Das sollte Teil Ihrer Phishing-Schulung sein und durch zusätzliche SAT-Tools oder Übungen ergänzt werden.

Sobald Sie Erkennungs-Tools implementiert und Ihre Mitarbeiter geschult haben, ist der nächste Schritt die Risikominderung — wie geht es weiter, wenn ein versuchter oder erfolgreicher E-Mail-Angriff erkannt wurde?Sie benötigen Tools, die Bedrohungen nach der Zustellung untersuchen, erkennen, abgrenzen und beseitigen.Viele dieser Tools nutzen KI und Automatisierung, um automatisch alle Instanzen einer gefährlichen E-Mail aus den Posteingängen Ihres Unternehmens zu entfernen.Die automatisierte Reaktion auf Vorfälle gewährleistet die schnelle und umfassende Beseitigung aller Bedrohungen aus den Posteingängen der Mitarbeiter, was manuell viel schwieriger und zeitaufwändiger ist.

Datensicherung und Compliance

Die letzte Säule zum Schutz Ihrer Microsoft 365-Anwendungen stellen Datenschutz und Compliance dar. Untersuchungen von Barracuda ergaben, dass 67% der Unternehmen, die Microsoft 365 nutzen, sich ausschließlich auf die in die Software integrierten Funktionen verlassen, wenn es darum geht, Microsoft 365-Daten zu sichern und wiederherzustellen. Wie Microsoft bestätigt, ist das Vertrauen auf die Cloud-basierte Datenspeicherung von Microsoft 365 keine Garantie für die Sicherheit Ihrer Daten. Es besteht immer noch die Gefahr, dass diese Daten von Ransomware gekapert und offline genommen werden, und menschliches Versagen — die häufigste Ursache für Datenlecks — kann immer noch zu Datenverlust und möglichen Betriebsunterbrechungen führen, wenn auf kritische Daten nicht mehr zugegriffen werden kann.

Deshalb ist es wichtig, dass Sie Ihre Microsoft 365-Daten regelmäßig mit der Cloud-Backup-Lösung eines Drittanbieters sichern.

Viele Unternehmen sind mit behördlichen Auflagen zur Aufbewahrung und sicheren Archivierung ihrer E-Mail-Kommunikation konfrontiert.Eine gute Lösung zur E-Mail-Archivierung stellt sicher, dass Sie eine unveränderliche, manipulationssichere Kopie jeder von Ihrem Unternehmen gesendeten und empfangenen E-Mail aufbewahren können.

Barracuda

Microsoft 365 verfügt über eine eigene Archivierungslösung, doch die Implementierung einer Cloud-basierten Archivierungslösung eines Drittanbieters stellt sicher, dass Sie unabhängig von den Vorgängen in Microsoft 365, weiterhin Zugriff auf Ihr E-Mail-Archiv haben, um Compliance-Anforderungen durch manipulationssichere Archive und granulare Aufbewahrungsrichtlinien zu erfüllen.

Es stehen auch andere Methoden zur Verfügung, um Ihre Compliance-Bemühungen zu unterstützen.Eine dieser Methoden ist die Verwendung eines Tools zur Datenklassifizierung und -erkennung, die Ihre Umgebung vor nicht ordnungsgemäß gespeicherten sensiblen Daten und latenter Malware schützt. Diese Tools geben Ihnen Einblicke in bestehende und neue Instanzen sensibler Daten, um ein Höchstmaß an Compliance zu gewährleisten und Ihnen dabei zu helfen, das Risiko eines Reputationsschadens und hoher Geldstrafen zu vermeiden.

Wie Barracuda Sie unterstützen kann

Ihr Ansatz zur Verbesserung des Sicherheitsstatus von Microsoft 365 erfordert ein fundiertes Verständnis für die Bedrohungen, die in Ihren E-Mail-Posteingängen lauern.Hier kommt Barracuda ins Spiel.

Barracuda Email Protection™

Für Unternehmen, die ihre Geschäftsbereiche, ihre Marken und ihre Mitarbeiter vor modernen E-Mail-Bedrohungen schützen wollen, ist Barracuda Email Protection eine umfassende, benutzerfreundliche Lösung, die Gateway-Schutz, API-basierten Schutz vor Identitätsmissbrauch und Phishing, Incident Response, Data Protection und Compliance-Funktionen bietet.

Barracuda Email Threat Scanner™

Probieren Sie noch heute unseren Email Threat Scanner aus. Es handelt sich dabei um einen kostenlosen, einfach zu handhabenden Service, der die Daten der letzten 12 Monate in Ihren Microsoft 365-E-Mail-Posteingängen überprüft.Anschließend erhalten Sie einen detaillierten Bericht und eine Aufschlüsselung aller gefundenen Bedrohungen inklusive einer individuellen Analyse.

Sie können kostenlos auf unseren Email Threat Scanner zugreifen, um herauszufinden, welche Bedrohungen sich aktuell in Ihrem Posteingang befinden.

Barracuda

Über Barracuda

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu erwerben, zu implementieren und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen. Mehr als 200.000 Unternehmen weltweit vertrauen auf Barracuda und darauf, dass wir sie auch vor Risiken schützen, die ihnen möglicherweise gar nicht bewusst sind. Daher können sich diese Unternehmen ganz auf ihr Wachstum konzentrieren. Weitere Informationen finden Sie auf de.barracuda.com.