Barracuda
Your business, secured.

Reicht die E-Mail-Sicherheit von Microsoft aus?

Die 7 größten Lücken in der E-Mail-Sicherheit von Microsoft 365

Viele Unternehmen fragen sich, ob die systemeigene E-Mail-Sicherheit der Exchange Online Protection oder von Microsoft Defender für Office 365 ausreichend Schutz bietet, um ihre Benutzer, Daten und Kommunikation zu schützen. Leider variiert der Schutz je nach Benutzerlizenz, und obwohl Microsoft seine E-Mail-Sicherheitsfunktionen kontinuierlich verbessert, bleiben Lücken bestehen. Aus diesem Grund müssen IT-Sicherheitsexperten bestimmen, ob die systemeigenen Sicherheitsfunktionen von Microsoft ihren Geschäftsanforderungen entsprechen. Wir haben sieben Funktionen identifiziert, bei denen die Sicherheit von Microsoft den Anforderungen möglicherweise nicht gerecht wird und unzureichend sein kann.

01 | Wirksamkeit der Bedrohungserkennung

Microsoft 365 allein bietet keinen ausreichenden Schutz vor fortschrittlichen E-Mail-Angriffen, die von der KI-gestützten Barracuda Impersonation Protection abgewehrt werden. Um die Erkennungsleistung von Barracuda im Vergleich zu Microsoft zu messen, haben wir mehr als 10 Milliarden E-Mails verarbeitet, die über alle Lizenztypen an Microsoft-Konten gesendet wurden.

Einschränkungen von Microsoft

Im Durchschnitt hat Microsoft 365 47 % der fortgeschrittenen E-Mail-Angriffe wie Conversation Hijacking, Phishing und Identitätsmissbrauch nicht erkannt. Bei den ausgefeiltesten Angriffen, wie z. B. Conversation Hijacking, steigt die Microsoft Fehlerquote auf 88 %. Die nativen Sicherheitsfunktionen von Microsoft 365 reichen für Unternehmen nicht aus, um ihre Nutzer vor den komplexen Bedrohungen von heute zu schützen.

4,2M	1,99M	47%
ANGRIFFE VON BARRACUDA BLOCKIERT	ANGRIFFE, DIE MICROSOFT ÜBERSEHEN HAT	MICROSOFT-FEHLERQUOTE

Wie Barracuda Sie unterstützen kann

Barracuda bietet umfassende Sicherheit für Microsoft 365 mit effektivem KI-gestütztem Schutz vor Phishing, Business E-Mail Compromise und Account Takeover. Mit einer leistungsstarken KI-Engine, die die Metadaten historischer E-Mails von internen und externen Absendern in Kombination mit der Verarbeitung natürlicher Sprache verwendet, verbessert der E-Mail-Schutz von Barracuda die Sicherheit der Microsoft 365-Nutzer mit hervorragender Erkennungseffizienz.

02 | Erklärbare KI und Entscheidungstransparenz

Die KI-gestützte E-Mail-Sicherheit wird zum Standard und die Fähigkeit, KI-Entscheidungen zu verstehen, zu überprüfen und rückgängig zu machen, ist somit für Sicherheitsteams entscheidend. Organisationen benötigen Transparenz darüber, warum E-Mails blockiert oder zugelassen werden, insbesondere bei der Untersuchung von Falschmeldungen oder der Schulung von Nachwuchsanalysten.

Einschränkungen von Microsoft

Microsoft Defender for Office 365 liefert Risikoeinstufungen und Bewertungen, jedoch nur begrenzte Erläuterungen zu den KI-gestützten Entscheidungen in verständlicher Sprache. Sicherheitsteams müssen technische Protokolle, Indikatoren von Bedrohungsanalysen und Übereinstimmungen mit Richtlinienregeln interpretieren, um zu verstehen, warum eine E-Mail markiert wurde. Dies erfordert eine fundierte Security-Expertise und erschwert es unterbesetzten Teams, Entscheidungen schnell zu überprüfen oder neue Analysten auszubilden.

Wie Barracuda Sie unterstützen kann

Der KI-Assistent „Bailey“ von Barracuda™ liefert für jede Erkennung eine Begründung in einfacher Sprache auf der Grundlage der Bewertungen von Microsoft, Google und Barracuda. Security-Teams können Entscheidungen überprüfen, überwachen und rückgängig machen, ohne über fundiertes Fachwissen zu verfügen. Dieser „von Menschen überwachte KI“-Ansatz bietet Transparenz und Kontrolle anstelle von Black-Box-Automatisierung, ermöglicht schnellere Untersuchungen, reduzierte Fehlmeldungen und bessere Security-Ergebnisse mit schlanken Teams.

03 | Skalierbarkeit von Richtlinien und Nutzerschutzgrenzen

Microsoft Defender for Office 365 schränkt die Nutzeranzahl für Impersonation Protection stark ein, sodass Unternehmen entscheiden müssen, welche Mitarbeiter fortschrittliche Security verdienen und welche verwundbar bleiben müssen. Für viele schaffen diese Einschränkungen eine ausnutzbare Angriffsfläche.

Einschränkungen von Microsoft

Microsoft beschränkt Impersonation Protection auf maximal 350 Nutzer pro Anti-Phishing-Richtlinie. Organisationen müssen manuell priorisieren, welche Nutzer — typischerweise Führungskräfte und Finanzverantwortliche — Schutz erhalten, während die Mehrheit der Mitarbeiter ungeschützt bleibt. Wenn ein Nutzer bereits in einer Anti-Phishing-Richtlinie enthalten ist, führt das Hinzufügen zu einer weiteren Richtlinie zu Fehlern. Microsoft empfiehlt, maximal 50 Nutzer zu schützen, um Fehlalarme zu vermeiden und schränkt die Abdeckung weiter ein. Richtlinienaktualisierungen benötigen 30 Minuten, um sich im Mandanten zu verbreiten, und vertrauenswürdige Absender- und Domainlisten sind auf 1.024 Einträge begrenzt. Sicherheitsteams in Unternehmen stehen vor einer unmöglichen Entscheidung: die Führungskräfte oder die Belegschaft schützen?

Wie Barracuda Sie unterstützen kann

Barracuda Email Protection skaliert den Schutz vor Identitätsmissbrauch und Phishing für jeden Nutzer ohne künstliche Richtlinienbeschränkungen. Die KI-gestützte Erkennung funktioniert im gesamten Unternehmen und eliminiert die Notwendigkeit, Prioritäten zu setzen und festzulegen, welche Mitarbeiter Schutz verdienen. Die kontinuierliche Überwachung schützt alle Postfächer gleichermaßen, egal ob es sich um das Postfach des CEOs oder eines neu eingestellten Mitarbeiters handelt, denn Angreifer zielen nicht nur auf Führungskräfte ab. Sie zielen auf jeden anfälligen Nutzer ab. Der Ansatz von Barracuda stellt sicher, dass kein Nutzer aufgrund von Lizenz- oder Richtlinienbeschränkungen zur Schwachstelle wird.

04 | Schutz vor Account Takeover

Account Takeover (ATO) tritt auf, wenn Angreifer unbefugten Zugriff auf Zugangsdaten von Nutzern erhalten und über kompromittierte Konten interne Phishing-Kampagnen starten, sensible Daten exfiltrieren oder betrügerische Transaktionen durchführen. Account Takeover zu erkennen und beheben erfordert Verhaltensanalysen und automatisierte Reaktionsfähigkeiten, die anomale Aktivitäten innerhalb vertrauenswürdiger Konten identifizieren.

Einschränkungen von Microsoft

Microsoft Defender for Office 365 Plan 1 (jetzt in Microsoft 365 E3 und Office 365 E3 enthalten) bietet keine Funktionen zum Schutz vor Account Takeover. Plan 2 (in Microsoft 365 E5 enthalten) bietet eine begrenzte Erkennung von Account Takeover durch Automated Investigation and Response (AIR). Wenn Konten in Plan-1-Umgebungen kompromittiert werden, müssen Unternehmen dies manuell anhand von Anmeldeprotokollen und Risikoberichten untersuchen, da anomale Sendemuster, verdächtige Weiterleitungsregeln oder abnormales Anmeldeverhalten nicht automatisch erkannt werden. Darüber hinaus schließt Impersonation Protection von Microsoft automatisch Absender-Empfänger-Paare aus, die einen früheren Kommunikationsverlauf haben, sodass Angreifer, die legitime Konten kapern, Abwehrmaßnahmen umgehen können, wenn sie es auf etablierte Kontakte abgesehen haben.

Wie Barracuda Sie unterstützen kann

Barracuda Email Protection bietet KI-gestützte Erkennung von Account Takeover. Barracuda identifiziert Anomalien von Verhalten und Inhaltsweiterleitungen in kompromittierten Konten und erkennt verdächtige Posteingangsregeln sowie ungewöhnliche Sendemuster. Im Gegensatz zum Ansatz von Microsoft verwendet Barracuda Verhaltensanalysen, um Identitätsmissbrauch zu erkennen, selbst wenn bereits eine Kommunikation zwischen Absender und Empfänger besteht. Wenn ein kompromittiertes Konto erkannt wird, behebt Barracuda automatisch Bedrohungen in Sekundenschnelle und entfernt bösartige E-Mails, die von dem kompromittierten Konto aus an alle Postfächer gesendet werden.

05 | Begrenzte Reaktion und Widerstandsfähigkeit nach der Zustellung

E-Mail-Sicherheit endet nicht mit der Zustellung einer Nachricht. Moderne Angriffe basieren auf verzögerter Ausführung, kompromittierten Benutzeraktionen und Account Takeover, nachdem eine E-Mail im Posteingang landet. Wenn dies passiert, müssen Organisationen schnell den Umfang verstehen, die Auswirkungen eindämmen und die betroffenen Nutzer und Daten wiederherstellen, anstatt nur die ursprüngliche Nachricht zu identifizieren.

Einschränkungen von Microsoft

Defender for Office 365 konzentriert sich hauptsächlich auf die Filterung vor der Auslieferung und den Time-of-Click-Schutz. Wenn Bedrohungen per E-Mail diese Kontrollmechanismen umgehen, beschränkt sich die Reaktion weitgehend auf Warnmeldungen und vereinzelte Abhilfemaßnahmen, wie beispielsweise das Entfernen der Nachricht. Defender for Office 365 bietet nicht von Haus aus koordinierte Ermittlungs-, Eindämmungs- oder Wiederherstellungs-Workflows für Nutzer, Identitäten und nachgelagerte Auswirkungen. Daher müssen IT-Teams den Umfang manuell beurteilen, Konten zurücksetzen und Daten mithilfe separater Tools und Prozesse wiederherstellen.

Wie Barracuda Sie unterstützen kann

Barracuda erweitert den E-Mail-Schutz zu einem resilienzorientierten Security-Modell. Durch die Korrelation von E-Mail-Bedrohungen mit Aktivitäten nach der Zustellung hilft Barracuda Managed Cloud XDR Teams, den vollständigen Kontext eines Vorfalls zu verstehen und effektiver darauf zu reagieren. Wenn Angriffe zu Kontomissbrauch oder Datenbeeinträchtigungen führen, unterstützen Barracuda Cloud-to-Cloud Backup und Entra ID Backup die Wiederherstellung von E-Mails, Kollaborationsdaten und Identitätskonfigurationen. Dieser Ansatz hilft ressourcenbeschränkten Teams, den Explosionsradius zu begrenzen und den Betrieb wiederherzustellen, wenn Prävention allein nicht ausreicht.

06 | Microsoft 365-Daten-Backup

Microsoft hat umfangreiche Maßnahmen ergriffen, um das Risiko eines Datenverlusts aufgrund eines Fehlers seinerseits zu verringern. Jedoch kann es Sie nicht vor den Aktionen Ihrer Nutzer oder vor Bedrohungen schützen, die sich seiner Kontrolle entziehen. Diese Risiken stellen die Mehrheit der typischen Datenverlustereignisse dar. Daher empfiehlt Microsoft ein regelmäßiges Backup Ihrer Daten oder die Verwendung von Backup-Apps und -Diensten von Drittanbietern.

Einschränkungen von Microsoft

Gemäß dem Modell der gemeinsamen Verantwortlichkeit von Microsoft bleibt Ihr Unternehmen letztendlich selbst für Ihre Data Protection verantwortlich. Zu bestimmen, ob eine Datei, ein Ordner, eine E-Mail oder eine SharePoint-Site nativ wiederhergestellt werden kann, kann schwierig sein. Verschiedene Assets haben unterschiedliche Beschränkungen, einschließlich:

- Einschränkungen beim Dateityp
- Optionen für Wiederherstellungspunkte
- Aufbewahrungszeiträume
- Standardeinstellungen oder konfigurierbare Höchstwerte
- Wiederherstellung durch Ordnernavigation oder E-Discovery-Suche
- Ob der Nutzer, Administrator oder Microsoft-Supportmitarbeiter die Wiederherstellung durchführen muss

Wie Barracuda Sie unterstützen kann

Mit Barracuda Cloud-to-Cloud Backup können Kunden täglich wichtige Daten in Exchange Online, OneDrive, Teams, OneNote und SharePoint direkt aus der Cloud in die Cloud sichern, wodurch Sie ohne Verwaltungsaufwand sofortige Skalierbarkeit erhalten. Darüber hinaus sind die Backups von den Produktionsnetzwerken von Microsoft isoliert, und es werden mehrere sichere Kopien der Daten an verschiedenen Orten aufbewahrt.

Für 100-GB-Postfächer ermöglicht die automatische Erweiterungsoption ein künstliches Maximum von 1,5 TB. Microsoft Purview bestimmt automatisch, welche Archivordner in jede neue 100-GB-Erweiterung verschoben werden, wie viele Unterordner erstellt werden und welche Elemente auf diese Ordner verteilt werden, um die anfängliche 100-GB-Grenze künstlich zu überwinden. Es gibt viele Beschränkungen, darunter eine maximale tägliche Wachstumsrate, Beschränkungen der Importgröße und des Dateityps, Suchbeschränkungen, Beschränkungen der angemessenen Nutzung, wann das Archiv vergrößert werden kann, die Zeitverzögerung für jede Erweiterung, ob die Ordner nach einer Erweiterung gelöscht werden können, ob Ordner nach dem Löschen wiederhergestellt werden können, Ungenauigkeiten von gelesenen/ungelesenen Nachrichten und andere Beschränkungen bei hybriden On-Premises/Cloud-Umgebungen.

Wie Barracuda Sie unterstützen kann

Barracuda Cloud Archive Service bietet echten unbegrenzten Speicherplatz auf einfacher und vorhersehbarer Basis pro Benutzer. Archivdaten sind unveränderlich und werden außerhalb von Produktionsdaten gespeichert. Es müssen keine Zwischenspeichersegmente mit 100-GB-Intervallen erstellt werden. Das Wachstum wird nicht gedrosselt. Für die Aufbewahrung von Daten in inaktiven Postfächern fallen keine Gebühren an, unabhängig von der Größe oder der Notwendigkeit eines „Litigation Hold“.

07 | E-Mail-Archivierung

Ein Microsoft-Archiv ist ein spezialisiertes Postfach, das neben dem primären Postfach des Benutzers in Outlook erscheint. Aufbewahrungsrichtlinien können Elemente automatisch in das Archiv verschieben, um das Postfach zu verkleinern und die Leistung zu verbessern.

Einschränkungen von Microsoft

Die Archive sind auf 50 GB für Business Basic, Standard und E1 sowie 100 GB für Business Premium und E3/E5 begrenzt. Archivinhalte sind nicht standardmäßig unveränderlich, und nur Postfächer mit Beweissicherungsverfahren speichern gelöschte Nachrichten länger als 14 Tage. Die automatische Erweiterungsoption bietet ein künstliches Maximum von 1,5 TB durch komplexe 100-GB-Schritte, die von Microsoft Purview verwaltet werden. Es gelten zahlreiche Einschränkungen, einschließlich täglicher Wachstumsbeschränkungen, begrenzte Importgröße und Dateitypen, Suchbeschränkungen, Einschränkungen bei der Ordnerverwaltung und Komplikationen in Hybridumgebungen.

Wie Barracuda Sie unterstützen kann

Barracuda Cloud Archive Service bietet echten unbegrenzten Speicherplatz auf einfacher und vorhersehbarer Basis pro Benutzer. Archivdaten sind unveränderlich und werden außerhalb von Produktionsdaten gespeichert. Es müssen keine Zwischenspeichersegmente mit 100-GB-Intervallen erstellt werden. Das Wachstum wird nicht gedrosselt. Für die Aufbewahrung von Daten in inaktiven Postfächern fallen keine Gebühren an, unabhängig von der Größe oder der Notwendigkeit eines „Litigation Hold“.

Überwinden Sie die Einschränkungen der nativen E-Mail-Sicherheit von Microsoft 365 mit Barracuda Email Protection.

Barracuda
Your business, secured.

Barracuda Networks und das Barracuda Networks-Logo sind eingetragene Warenzeichen von Barracuda Networks, Inc. in den Vereinigten Staaten. Alle anderen Namen sind Eigentum ihrer jeweiligen Rechteinhaber.