

La sicurezza e-mail di Microsoft è sufficiente?

Le 7 principali lacune nella sicurezza della posta elettronica di Microsoft 365

Molte organizzazioni si chiedono se la sicurezza email nativa in Exchange Online Protection o Microsoft Defender for Office 365 fornisca protezioni adeguate per salvaguardare i loro utenti, dati e comunicazioni. Purtroppo, la protezione varia a seconda della licenza di ciascun utente e, sebbene Microsoft stia continuamente migliorando le sue capacità di sicurezza email, permangono lacune. Di conseguenza, i professionisti della sicurezza IT devono determinare se la sicurezza nativa di Microsoft soddisfa i requisiti aziendali. Abbiamo identificato sette capacità in cui la sicurezza di Microsoft potrebbe risultare carente e insufficiente.

01 | Efficacia del rilevamento delle minacce

Microsoft 365 da solo non fornisce una protezione adeguata contro gli attacchi email avanzati bloccati da Barracuda Impersonation Protection, alimentato dall'IA. Per misurare l'efficacia di rilevamento di Barracuda rispetto a Microsoft, abbiamo elaborato oltre 10 miliardi di email consegnate agli account Microsoft su tutti i tipi di licenza.

Limitazioni di Microsoft

In media, Microsoft 365 non ha rilevato il 47% degli attacchi email avanzati come l'hijacking delle conversazioni, il phishing e le impersonificazioni. Per gli attacchi più sofisticati, come gli attacchi di hijacking delle conversazioni, il tasso di mancato rilevamento di Microsoft sale all'88%. Le funzionalità di sicurezza native di Microsoft 365 sono insufficienti per consentire alle organizzazioni di proteggere i propri utenti dalle minacce complesse odierne.

4,2M

ATTACCHI BARRACUDA
BLOCCATI

1,99M

ATTACCHI MANCATI DA
MICROSOFT

47%

TASSO DI ERRORE
MICROSOFT

In che modo Barracuda può essere di aiuto

Barracuda offre una sicurezza completa per Microsoft 365 con una protezione efficace abilitata dall'IA contro il phishing, la compromissione delle email aziendali e il dirottamento degli account. Con un potente motore AI che utilizza i metadati delle email storiche da mittenti interni ed esterni combinati con l'elaborazione del linguaggio naturale, la protezione email di Barracuda migliora la sicurezza degli utenti di Microsoft 365 con un'efficacia di rilevamento superiore.

02 | Intelligenza artificiale spiegabile e trasparenza delle decisioni

Man mano che la sicurezza email alimentata dall'IA diventa standard, la capacità di comprendere, rivedere e invertire le decisioni dell'IA diventa fondamentale per i team di sicurezza. Le organizzazioni hanno bisogno di trasparenza sui motivi per cui le email vengono bloccate o consentite, soprattutto durante l'indagine di falsi positivi o la formazione di analisti junior.

Limitazioni di Microsoft

Microsoft Defender per Office 365 fornisce verdetti e punteggi sulle minacce ma spiegazioni in linguaggio semplice limitate per decisioni guidate dall'IA. I team di sicurezza devono interpretare i registri tecnici, gli indicatori di intelligence sulle minacce e le corrispondenze delle regole di politica per capire perché un'email è stata contrassegnata. Questo richiede una profonda competenza in materia di sicurezza e rende difficile per i team con risorse limitate rivedere rapidamente le decisioni o formare nuovi analisti.

In che modo Barracuda può essere di aiuto

L'assistente AI Bailey™ di Barracuda fornisce un ragionamento in linguaggio semplice per ogni rilevamento tra i verdetti di Microsoft, Google e Barracuda. I team di sicurezza possono rivedere, supervisionare e invertire le decisioni senza una profonda esperienza. Questo approccio di "AI supervisionata dall'uomo" fornisce visibilità e controllo anziché un'automazione a scatola nera, consentendo indagini più rapide, una riduzione dei falsi positivi e migliori risultati di sicurezza con team ridotti.

03 | Scalabilità della politica e limiti di protezione dell'utente

Microsoft Defender per Office 365 impone limiti rigidi sul numero di utenti che possono ricevere la protezione dall'impersonificazione, costringendo le organizzazioni a scegliere quali dipendenti meritano una sicurezza avanzata e quali devono rimanere vulnerabili. Per molte organizzazioni, questi vincoli creano una superficie di attacco sfruttabile.

Limitazioni di Microsoft

Microsoft limita la protezione dall'impersonificazione a un massimo di 350 utenti per politica anti-phishing. Le organizzazioni devono dare priorità manualmente a quali utenti ricevere protezione — tipicamente dirigenti e autorità finanziarie — lasciando la maggior parte dei dipendenti esposti. Se un utente è già incluso in una politica anti-phishing, aggiungerlo a un'altra politica genera errori. Microsoft consiglia di mantenere gli utenti protetti sotto i 50 per evitare falsi positivi, limitando ulteriormente copertura. Gli aggiornamenti delle policy impiegano 30 minuti per propagarsi su tutto il tenant e le liste di mittenti e domini attendibili sono limitate a 1.024 voci. I team di sicurezza aziendale affrontano una scelta impossibile: proteggere la leadership o proteggere la forza lavoro.

In che modo Barracuda può essere di aiuto

La protezione email di Barracuda estende la protezione contro l'impersonificazione e il phishing a ogni utente senza limiti artificiali di policy. Il rilevamento basato sull'intelligenza artificiale funziona in tutta l'organizzazione, eliminando la necessità di stabilire quali dipendenti meritano protezione. Il monitoraggio continuo protegge tutte le caselle di posta in modo equo, che si tratti del CEO o di un dipendente al primo livello — perché gli aggressori non prendono di mira solo i dirigenti. Prendono di mira qualsiasi utente vulnerabile. L'approccio di Barracuda garantisce che nessun utente diventi l'anello debole a causa di vincoli di licenza o di politica.

04 | Protezione contro la presa di controllo dell'account

Il takeover dell'account (ATO) si verifica quando gli aggressori ottengono l'accesso non autorizzato alle credenziali dell'utente e utilizzano account compromessi per avviare campagne di phishing interne, esfiltrare dati sensibili o condurre transazioni fraudolente. Rilevare e risolvere il takeover dell'account richiede un'analisi comportamentale e capacità di risposta automatizzate che identificano attività anomale all'interno di account fidati.

Limitazioni di Microsoft

Microsoft Defender per Office 365 Piano 1 (ora incluso in Microsoft 365 E3 e Office 365 E3) non fornisce funzionalità di protezione dal sequestro dell'account. Il Piano 2 (incluso in Microsoft 365 E5) offre un rilevamento limitato del sequestro dell'account tramite Automated Investigation and Response (AIR). Quando gli account vengono compromessi in ambienti Piano 1, le organizzazioni devono indagare manualmente utilizzando i registri di accesso e i report sui rischi poiché non esiste un rilevamento automatico di modelli di invio anomali, regole di inoltramento sospette o comportamenti di accesso anomali. Inoltre, la protezione contro l'impersonificazione di Microsoft esclude automaticamente le coppie mittente/destinatario con una cronologia di comunicazione precedente, consentendo agli attaccanti che dirottano account legittimi di bypassare le difese quando prendono di mira contatti stabiliti.

In che modo Barracuda può essere di aiuto

La protezione email di Barracuda fornisce il rilevamento di acquisizioni di account basato sull'intelligenza artificiale. Barracuda identifica anomalie comportamentali e di inoltramento dei contenuti all'interno di account compromessi, rilevando regole di casella di posta sospette e modelli di invio anomali. A differenza dell'approccio di Microsoft, Barracuda utilizza l'analisi comportamentale per rilevare l'impersonificazione anche quando esiste una comunicazione precedente tra mittente e destinatario. Quando viene rilevato un account compromesso, Barracuda risolve automaticamente le minacce in pochi secondi, rimuovendo le email dannose inviate dall'account compromesso su tutte le caselle di posta.

05 | Risposta e resilienza limitate post-consegna

La sicurezza delle email non termina quando un messaggio viene consegnato. Gli attacchi moderni si basano su esecuzioni ritardate, azioni compromesse degli utenti e presa di controllo degli account dopo che un'email raggiunge la casella di posta. Quando ciò accade, le organizzazioni devono rapidamente comprendere l'ambito, contenere l'impatto e recuperare utenti e dati coinvolti, non solo identificare il messaggio originale.

Limitazioni di Microsoft

Defender per Office 365 è principalmente focalizzato sul filtraggio pre-consegna e sulla protezione al momento del clic. Quando le minacce trasmesse via email superano questi controlli, la risposta è in gran parte limitata ad avvisi e azioni di rimedio isolate, come la rimozione dei messaggi. Defender per Office 365 non fornisce nativamente flussi di lavoro coordinati di indagine, contenimento o recupero tra utenti, identità e impatti a valle. Di conseguenza, i team IT devono valutare manualmente l'ambito, reimpostare gli account e recuperare i dati utilizzando strumenti e processi separati.

In che modo Barracuda può essere di aiuto

Barracuda estende la protezione delle email in un modello di sicurezza basato sulla resilienza. Correlando le minacce email con l'attività post-consegna, Barracuda Managed Cloud XDR aiuta i team a comprendere il contesto completo di un incidente e rispondere in modo più efficace. Quando gli attacchi portano a un uso improprio degli account o a un impatto sui dati, Barracuda Cloud-to-Cloud Backup ed Entra ID Backup supportano il recupero di email, dati di collaborazione e configurazioni di identità. Questo approccio aiuta i team con risorse limitate a limitare il raggio di azione e ripristinare le operazioni quando la sola prevenzione non è sufficiente.

06 | Backup dei dati di Microsoft 365

Microsoft ha adottato misure estese per ridurre il rischio di perdita di dati a causa di un errore da parte sua. Tuttavia, non possono proteggerti dalle azioni dei tuoi utenti o da minacce al di fuori del loro controllo. Questi rischi rappresentano la maggior parte degli eventi di perdita di dati. Pertanto, Microsoft raccomanda di eseguire regolarmente il backup dei dati o di utilizzare app e servizi di backup di terze parti.

Limitazioni di Microsoft

Secondo il Modello di Responsabilità Condivisa di Microsoft, la tua organizzazione rimane in ultima analisi responsabile della protezione dei tuoi dati. Determinare se un file, una cartella, un'email o un sito di SharePoint è recuperabile nativamente può essere impegnativo. I diversi asset hanno limitazioni varie, tra cui:

- Restrizioni sui tipi di file
- Opzioni punto di ripristino
- Periodi di conservazione
- Impostazioni predefinite o massimi configurabili
- Recupero dalla navigazione delle cartelle o dalla ricerca e-discovery
- Se l'utente, l'amministratore o il personale di supporto Microsoft deve eseguire il ripristino

In che modo Barracuda può essere di aiuto

Il backup Barracuda Cloud-to-Cloud consente ai clienti di eseguire il backup dei dati critici quotidianamente all'interno di Exchange Online, OneDrive, Teams, OneNote e SharePoint direttamente dal cloud al cloud, offrendo scalabilità immediata e nulla da gestire. Inoltre, i backup sono intrinsecamente isolati dalle reti di produzione di Microsoft e vengono mantenute copie sicure multiple dei dati in diverse località.

07 | Archiviazione delle email

Un archivio Microsoft è una cassetta postale specializzata che appare accanto alla cassetta postale principale dell'utente in Outlook. Le politiche di conservazione possono spostare automaticamente gli elementi nell'archivio per ridurre le dimensioni della cassetta postale e migliorarne le prestazioni.

Limitazioni di Microsoft

Gli archivi sono limitati a 50GB per Business Basic, Standard e E1, e a 100GB per Business Premium ed E3/E5. Il contenuto dell'archivio non è immutabile per default, e solo le cassette postali con il blocco per controversia legale conservano i messaggi eliminati oltre 14 giorni. L'opzione di espansione automatica fornisce un massimo artificiale di 1.5TB attraverso incrementi complessivi di 100GB gestiti da Microsoft Purview. Si applicano numerose limitazioni, tra cui restrizioni sulla crescita giornaliera, limiti di dimensione e tipo di file per l'importazione, restrizioni di ricerca, vincoli sulla gestione delle cartelle e complicazioni negli ambienti ibridi.

In che modo Barracuda può essere di aiuto

Il Barracuda Cloud Archive Service fornisce un vero spazio di archiviazione illimitato su base semplice e prevedibile per utente. I dati archiviati sono immutabili e conservati al di fuori dei dati di produzione. Non ci sono segmenti di archiviazione intermedia da creare a intervalli di 100GB. La crescita non è limitata. Non ci sono costi per conservare i dati in caselle di posta inattive, indipendentemente dalle dimensioni o dall'esigenza di un blocco per contenzioso.

**Supera le limitazioni della sicurezza e-mail
nativa di Microsoft 365 utilizzando Barracuda
Email Protection.**

