

A segurança de e-mail da Microsoft é suficientemente boa?

As 7 principais lacunas na segurança de e-mail do Microsoft 365

Muitas organizações questionam-se se a segurança de e-mail nativa no Exchange Online Protection ou no Microsoft Defender for Office 365 proporciona proteções adequadas para salvaguardar os seus utilizadores, dados e comunicações. Infelizmente, a proteção varia consoante a licença de cada utilizador, e embora a Microsoft esteja continuamente a melhorar as suas capacidades de segurança de e-mail, ainda existem lacunas. Como resultado, os profissionais de segurança de TI devem determinar se a segurança nativa da Microsoft atende aos requisitos do seu negócio. Identificámos sete capacidades onde a segurança da Microsoft pode ser insuficiente.

01 | Eficácia da deteção de ameaças

O Microsoft 365 sozinho não proporciona proteção adequada contra ataques de e-mail avançados bloqueados pela Proteção contra falsificação de identidade da Barracuda, potenciada por IA. Para medir a eficácia de deteção da Barracuda em comparação com a Microsoft, processámos mais de 10 mil milhões de emails entregues a contas Microsoft em todos os tipos de licença.

Limitações da Microsoft

Em média, o Microsoft 365 falhou em 47% dos ataques de e-mail avançados, como sequestro de conversas, phishing e falsificações de identidade. Para os ataques mais sofisticados, como os ataques de sequestro de conversas, a taxa de falhas da Microsoft sobe para 88%. As funcionalidades de segurança nativas do Microsoft 365 são insuficientes para as organizações protegerem os seus utilizadores das ameaças complexas de hoje.

4,2M

ATAQUES BLOQUEADOS
PELA BARRACUDA

1,99M

ATAQUES QUE A
MICROSOFT FALHOU

47%

MICROSOFT MISS RATE

Como a Barracuda pode ajudar

A Barracuda oferece segurança abrangente para o Microsoft 365 com proteção eficaz habilitada por IA contra phishing, comprometimento de e-mail empresarial e apropriação de conta. Com um motor de IA poderoso que utiliza os metadados de e-mails históricos de remetentes internos e externos combinados com processamento de linguagem natural, a Proteção de E-mail da Barracuda melhora a segurança dos utilizadores do Microsoft 365 com eficácia de deteção superior.

02 | IA explicável e transparência na decisão

À medida que a segurança de e-mail baseada em IA se torna padrão, a capacidade de compreender, rever e reverter decisões de IA torna-se crítica para as equipas de segurança. As organizações precisam de transparência sobre por que os e-mails são bloqueados ou permitidos, especialmente ao investigar falsos positivos ou ao formar analistas juniores.

Limitações da Microsoft

O Microsoft Defender para Office 365 fornece veredictos de ameaça e pontuações, mas explicações limitadas em linguagem simples para decisões baseadas em IA. As equipas de segurança têm de interpretar registos técnicos, indicadores de inteligência de ameaças e correspondência de regras de política para compreender por que razão um email foi sinalizado. Isto requer uma profunda especialização em segurança e torna difícil para equipas com poucos recursos rever rapidamente as decisões ou treinar novos analistas.

Como a Barracuda pode ajudar

O assistente de IA Bailey™ da Barracuda fornece explicações em linguagem simples para cada deteção em veredictos da Microsoft, Google e Barracuda. As equipas de segurança podem rever, supervisionar e reverter decisões sem necessidade de conhecimentos aprofundados. Esta abordagem de “IA supervisionada por humanos” proporciona visibilidade e controlo em vez de automação em caixa preta, permitindo investigações mais rápidas, redução de falsos positivos e melhores resultados de segurança com equipas reduzidas.

03 | Escalabilidade da política e limites de proteção do utilizador

O Microsoft Defender for Office 365 impõe limites rigorosos sobre quantos utilizadores podem receber proteção contra falsificação de identidade, forçando as organizações a escolher quais funcionários merecem segurança avançada e quais devem permanecer vulneráveis. Para muitas organizações, estas restrições criam uma superfície de ataque explorável.

Limitações da Microsoft

A Microsoft limita a proteção contra falsificação de identidade a um máximo de 350 utilizadores por política de anti-phishing. As organizações devem priorizar manualmente quais os utilizadores que recebem proteção — tipicamente executivos e autoridades financeiras — deixando a maioria dos funcionários expostos. Se um utilizador já estiver incluído numa política de anti-phishing, adicioná-lo a outra política gera erros. A Microsoft recomenda manter os utilizadores protegidos abaixo de 50 para evitar falsos positivos, restringindo ainda mais cobertura. As atualizações de política demoram 30 minutos a propagar-se pelo inquilino, e as listas de remetentes e domínios confiáveis são limitadas a 1.024 entradas. As equipas de segurança empresarial enfrentam uma escolha impossível: proteger a liderança ou proteger a força de trabalho.

Como a Barracuda pode ajudar

A Barracuda Email Protection dimensiona a proteção contra falsificação de identidade e phishing para cada utilizador sem limites artificiais de política. A deteção baseada em IA funciona em toda a organização, eliminando a necessidade de priorizar quais os colaboradores que merecem proteção. A monitorização contínua protege todas as caixas de correio de forma igual, quer seja o CEO ou um colaborador de nível inicial — porque os atacantes não visam apenas os executivos. Eles visam qualquer utilizador vulnerável. A abordagem da Barracuda garante que nenhum utilizador se torna o elo fraco devido a restrições de licenciamento ou políticas.

04 | Proteção contra apropriação de conta

A apropriação de conta (ATO) ocorre quando atacantes obtêm acesso não autorizado a credenciais de utilizador e usam contas comprometidas para lançar campanhas de phishing internas, exfiltrar dados sensíveis ou realizar transações fraudulentas. Detetar e remediar a apropriação de conta requer análise comportamental e capacidades de resposta automatizada que identifiquem atividade anómala a partir de contas confiáveis.

Limitações da Microsoft

Microsoft Defender para Office 365 Plano 1 (agora incluído no Microsoft 365 E3 e Office 365 E3) não fornece capacidades de proteção contra apropriação de conta. O Plano 2 (incluído no Microsoft 365 E5) oferece deteção limitada de apropriação de conta através de Investigação e Resposta Automatizada (AIR). Quando as contas são comprometidas em ambientes do Plano 1, as organizações devem investigar manualmente usando registos de início de sessão e relatórios de risco, uma vez que não há deteção automatizada de padrões de envio anómalos, regras de encaminhamento suspeitas ou comportamento de login anormal. Além disso, a proteção contra falsificação de identidade da Microsoft exclui automaticamente pares de remetente/destinatário com histórico de comunicação anterior, permitindo que atacantes que sequestram contas legítimas contornem as defesas ao visar contactos estabelecidos.

Como a Barracuda pode ajudar

Barracuda Email Protection fornece deteção de apropriação de conta Baseado em IA. A Barracuda identifica anomalias de comportamento e de encaminhamento de conteúdo em contas comprometidas, detetando regras de caixa de entrada suspeitas e padrões de envio anormais. Ao contrário da abordagem da Microsoft, a Barracuda utiliza análise comportamental para detetar Falsificação de identidade mesmo quando existe comunicação prévia entre remetente e destinatário. Quando uma conta comprometida é detetada, a Barracuda remedia automaticamente as ameaças em segundos, removendo e-mails maliciosos enviados da conta comprometida em todas as caixas de correio.

05 | Resposta e resiliência limitadas após a entrega

A segurança de e-mail não termina quando uma mensagem é entregue. Os ataques modernos dependem de execução retardada, ações de utilizadores comprometidos e apropriação de conta após um e-mail chegar à caixa de entrada. Quando isso acontece, as organizações devem rapidamente compreender o alcance, conter o impacto e recuperar utilizadores e dados afetados, não apenas identificar a mensagem original.

Limitações da Microsoft

O Defender para Office 365 está principalmente focado na filtragem pré-envio e proteção no momento do clique. Quando ameaças transmitidas por e-mail contornam esses controles, a resposta é largamente limitada a alertas e ações de remediação isoladas, como remoção de mensagens. O Defender para Office 365 não fornece nativamente investigações coordenadas, contenção ou fluxos de trabalho de recuperação entre utilizadores, identidades e impacto a jusante. Como resultado, as equipas de TI têm de avaliar manualmente o âmbito, redefinir contas e recuperar dados usando ferramentas e processos separados.

Como a Barracuda pode ajudar

A Barracuda expande a proteção de e-mail para um modelo de segurança orientado para a resiliência. Ao correlacionar ameaças de e-mail com atividade pós-entrega, o Barracuda Managed Cloud XDR ajuda as equipas a compreenderem o contexto completo de um incidente e responder de forma mais eficaz. Quando os ataques levam ao uso indevido de contas ou impacto nos dados, Barracuda Cloud-to-Cloud Backup e Entra ID Backup apoiam a recuperação de e-mails, dados de colaboração e configurações de identidade. Esta abordagem ajuda equipas com recursos limitados a limitar o raio de explosão e restaurar operações quando a prevenção por si só não é suficiente.

06 | Backup de dados do Microsoft 365

A Microsoft tomou medidas extensivas para reduzir o risco de perda de dados devido a uma falha da sua parte. No entanto, não podem protegê-lo das ações dos seus utilizadores ou das ameaças além do seu controlo. Esses riscos representam a maioria dos eventos de perda de dados. Portanto, a Microsoft recomenda que faça backup dos seus dados regularmente ou utilize aplicações e serviços de backup de terceiros.

Limitações da Microsoft

De acordo com o Modelo de Responsabilidade Partilhada da Microsoft, a sua organização continua a ser, em última análise, responsável pela proteção dos seus dados. Determinar se um ficheiro, pasta, email ou site do SharePoint é recuperável nativamente pode ser um desafio. Diferentes ativos têm limitações variadas, incluindo:

- Restrições de tipo de ficheiro
- Opções de ponto de recuperação
- Períodos de retenção
- Definições padrão ou máximos configuráveis
- Recuperação da navegação em pastas ou pesquisa de e-discovery
- Se o utilizador, administrador ou o pessoal de suporte da Microsoft deve realizar a recuperação

Como a Barracuda pode ajudar

O Barracuda Cloud-to-Cloud Backup permite que os clientes façam backup diário de dados críticos no Exchange Online, OneDrive, Teams, OneNote e SharePoint diretamente da nuvem para a nuvem, oferecendo escalabilidade instantânea e sem necessidade de gestão. Além disso, os backups são inerentemente isolados das redes de produção da Microsoft, e várias cópias seguras dos dados são mantidas em diferentes locais.

07 | Arquivamento de e-mail

Um Arquivo Microsoft é uma caixa de correio especializada que aparece ao lado da caixa de correio principal do utilizador no Outlook. As políticas de retenção podem mover automaticamente itens para o arquivo para reduzir a caixa de correio e melhorar o seu desempenho.

Limitações da Microsoft

Os arquivos estão limitados a 50GB para Business Basic, Standard e E1, e 100GB para Business Premium e E3/E5. O conteúdo do arquivo não é imutável por padrão, e apenas as caixas de correio com Retenção por Litígio retêm mensagens apagadas além de 14 dias. A opção de auto-expansão oferece um máximo artificial de 1.5TB através de incrementos complexos de 100GB geridos pelo Microsoft Purview. Aplicam-se inúmeras limitações, incluindo restrições de crescimento diário, limites de tamanho e tipo de ficheiro de importação, restrições de pesquisa, constrangimentos de gestão de pastas e complicações em ambientes híbridos.

Como a Barracuda pode ajudar

O Barracuda Cloud Archive Service fornece armazenamento verdadeiramente ilimitado de forma simples e previsível por utilizador. Os dados de arquivo são imutáveis e armazenados fora dos dados de produção. Não há necessidade de criar segmentos de armazenamento intermediários a intervalos de 100GB. O crescimento não é limitado. Não há custos para reter dados em caixas de correio inativas, independentemente do tamanho ou da necessidade de uma Retenção para Litígios.

Supere as limitações de segurança de e-mail nativas do Microsoft 365 utilizando a Proteção de E-mail Barracuda.

