Barracuda
Your business, secured.

¿Es la protección del correo electrónico de Microsoft lo suficientemente buena?

Las 7 principales brechas en la protección del correo electrónico de Microsoft 365

Muchas organizaciones se preguntan si la seguridad nativa del correo electrónico en Exchange Online Protection o Microsoft Defender para Office 365 proporciona protecciones adecuadas para salvaguardar a sus usuarios, datos y comunicaciones. Desafortunadamente, la protección varía según la licencia de cada usuario, y aunque Microsoft mejora continuamente sus capacidades de seguridad del correo electrónico, persisten las brechas. Como resultado, los profesionales de seguridad de TI deben determinar si la seguridad nativa de Microsoft cumple con sus requisitos empresariales. Hemos identificado siete capacidades en las que la seguridad de Microsoft puede ser insuficiente.

01 | Eficacia en la detección de amenazas

Microsoft 365 por sí solo no ofrece una protección adecuada contra los ataques avanzados por correo electrónico que bloquea la solución Barracuda Impersonation Protection, basada en inteligencia artificial. Para evaluar la eficacia de detección de Barracuda en comparación con la de Microsoft, hemos analizado más de 10.000 millones de correos electrónicos recibidos en cuentas de Microsoft de todos los tipos de licencia.

Limitaciones de Microsoft

Microsoft 365 tiene una tasa media de error del 47 % en ataques avanzados por correo electrónico, como el secuestro de conversaciones, el phishing y la suplantación de identidad. En el caso de ataques más sofisticados, como los de secuestro de conversaciones, la tasa de error de Microsoft se dispara hasta el 88 %. Las funciones de seguridad nativas de Microsoft 365 son insuficientes para que las organizaciones protejan a sus usuarios frente a las complejas amenazas actuales.

4,2M	1,99M	47%
ATAQUES BLOQUEADOS POR BARRACUDA	ATAQUES QUE MICROSOFT NO DETECTÓ	TASA DE ERROR DE MICROSOFT

Cómo puede ayudar Barracuda

Barracuda ofrece seguridad integral para Microsoft 365 con una protección eficaz impulsada por IA contra el phishing, el fraude del correo electrónico empresarial y la usurpación de cuentas. Con un potente motor de IA que utiliza los metadatos de correos electrónicos históricos de remitentes internos y externos combinados con el procesamiento del lenguaje natural, la protección contra la suplantación de Barracuda mejora la seguridad de los usuarios de Microsoft 365 con una eficacia de detección superior.

02 | Backup de datos de Microsoft 365

Microsoft ha adoptado numerosas medidas para reducir el riesgo de pérdida de datos debido a un fallo por su parte. Sin embargo, no puede protegerle de las acciones de sus usuarios ni de amenazas que escapan a su control. Estos riesgos representan la mayoría de los casos habituales de pérdida de datos. Por lo tanto, Microsoft le recomienda que realice copias de seguridad de sus datos con regularidad o que utilice aplicaciones y servicios de backup de terceros.

Limitaciones de Microsoft

Según el Modelo de Responsabilidad Compartida de Microsoft, su organización sigue siendo en última instancia responsable de la protección de sus datos. Determinar si un archivo, carpeta, correo electrónico o sitio de SharePoint es recuperable de forma nativa puede ser un desafío. Los diferentes activos tienen diferentes limitaciones, como restricciones de tipo de archivo; opciones de punto de recuperación; períodos de retención; configuraciones predeterminadas o máximos configurables; recuperación desde la navegación de carpetas o búsqueda de e-discovery; o si el usuario, administrador o Microsoft mismos deben realizar la recuperación.

Cómo puede ayudar Barracuda

Barracuda Cloud-to-Cloud Backup permite a los clientes realizar backups diarios de datos críticos dentro de Exchange Online, OneDrive, Teams, OneNote y SharePoint directamente de la nube a la nube, ofreciendo escalabilidad instantánea y sin necesidad de gestión. Además, las copias de seguridad están inherentemente aisladas de las redes de producción de Microsoft, y se mantienen múltiples copias seguras de los datos en diferentes ubicaciones.

03 | Aislamiento de archivos adjuntos de vulnerabilidades de día cero

Microsoft Safe Attachments proporciona una capa adicional de protección para los archivos adjuntos de correo electrónico que ya han sido analizados por la protección antimalware en EOP y está incluido en el Plan MSDO 1 y 2, Business Premium y E5. Específicamente, Safe Attachments detona archivos adjuntos en un entorno virtual para detectar amenazas de día cero.

Limitaciones de Microsoft

Safe Attachments no está incluido con EOP, lo que significa que no está incluido con Business Basic, Business Standard, E1, o E3. Está incluido en Business Premium y E5. Los buzones compartidos requieren una licencia para aprovechar Safe Attachments. Microsoft utiliza un entorno virtualizado basado en la tecnología de hipervisor de MS para escanear archivos adjuntos, que algunos tipos de malware pueden eludir.

Cómo puede ayudar Barracuda

Barracuda Email Gateway Defense aprovecha múltiples motores antivirus para bloquear el malware conocido. El malware desconocido (día cero/hora cero) es identificado por una protección frente a amenazas avanzadas en múltiples capas que utiliza IA, heurística, análisis de comportamiento y un sandbox dinámico. A diferencia de los sandboxes tradicionales que dependen de una infraestructura de hipervisor, Barracuda emula dinámicamente diferentes plataformas en cada ejecución. Los buzones compartidos no requieren una licencia para aprovechar la protección frente a amenazas avanzadas.

04 | Sandboxing de URL en el momento del clic

Microsoft Safe Links ayuda a proteger contra enlaces de phishing maliciosos y otros ataques, y está incluido en el Plan MSDO 1 y 2, Business Premium y E5. Los enlaces sin una reputación válida se analizan de manera asincrónica en segundo plano. También añade protección en el momento del clic contra URLs maliciosas al proporcionar análisis y reescritura de URLs para mensajes entrantes. Cuando está habilitado, las URLs se escanean antes de la entrega, independientemente de si las URLs son reescritas.

Limitaciones de Microsoft

Safe Links no está incluido con EOP, lo que significa que no está incluido con Business Basic, Business Standard, E1 o E3. Está incluido en Business Premium y E5, pero está deshabilitado por defecto. Existen varias limitaciones en Safe Links en lo que respecta al malware consciente del hipervisor, la anulación por parte del usuario final, los protocolos de transporte no compatibles, las carpetas públicas no compatibles y la falta de formación en concienciación sobre la seguridad "en el momento".

Cómo puede ayudar Barracuda

La **protección de enlaces de Barracuda** se incluye con todos los planes de protección del correo electrónico, está habilitada de forma predeterminada y requiere una configuración mínima o nula. Los usuarios finales no pueden anular la pantalla de advertencia de la protección de enlaces y son dirigidos a la formación en concienciación de seguridad a través de la integración con la solución de Barracuda. El malware consciente del hipervisor también tiene menos probabilidades de evadir el sandbox dinámico de Barracuda, y se admite FTP/S además de FTP. Se admiten las carpetas públicas habilitadas para correo y los buzones compartidos no requieren licencias de protección de enlaces de Barracuda.

05 | Protección contra la suplantación de identidad

Protección contra la suplantación de identidad en MS Defender para Office 365 (MSDO) Plan 1 y 2, Business Premium (BP) y E5 es inteligencia artificial (IA) que determina patrones de correo electrónico con los contactos frecuentes de los usuarios para distinguir entre mensajes de remitentes legítimos y suplantados.

Limitaciones de Microsoft

La protección contra la suplantación de identidad (IP) no está incluida con Exchange Online Protection (EOP), lo que significa que no está incluida con Business Basic, Business Standard, E1 o E3. Está incluida en Business Premium y E5, pero deshabilitada por defecto. Hay varias limitaciones relacionadas con IP dependiendo de si el remitente y el destinatario han comunicado previamente o no, y no puede proteger a más de 350 usuarios o 50 dominios para evitar la suplantación. Los falsos positivos suelen resultar de remitentes con nombres comunes, cuentas personales, cuentas de proveedores y socios internos, y exempleados.

Cómo puede ayudar Barracuda

La **protección contra la suplantación de identidad de Barracuda** está incluida en todos los planes y funciona de inmediato, sin necesidad de especificar, habilitar ni configurar reglas o políticas, y sin limitar el número de direcciones de remitente, usuarios o dominios.

06 | Archivado de correo electrónico

El archivo de Microsoft es un buzón especializado que aparece junto al buzón principal del usuario en Outlook. Las políticas de retención pueden mover automáticamente elementos al archivo para reducir el tamaño del buzón y mejorar su rendimiento.

Limitaciones de Microsoft

Los archivos para todos los buzones estándar y compartidos están limitados a 50 GB para Business Basic, Standard y E1. Los archivos comienzan en 100 GB para Business Premium y E3/E5. Por defecto, el contenido del archivo no es inmutable, y solo los buzones con licencia y habilitados para la retención por litigio pueden conservar los mensajes eliminados más allá de una ventana de 14 días. Los archivos de usuario sin licencia que superen los 50 GB o aquellos colocados en retención por litigio requieren una licencia de pago de Exchange Online Plan 1 y una licencia complementaria de archivado o Plan Exchange Online 2. A veces, los archivos de 100 GB todavía se anuncian como "ilimitados", pero en realidad no pueden exceder los 1,5 TB después de habilitar la expansión.

Para los buzones de 100 GB, la opción de expansión automática permite un máximo artificial de 1,5 TB. Microsoft Purview determina automáticamente qué carpetas de archivo se trasladan a cada nuevo incremento de 100 GB, cuántas subcarpetas crear y qué elementos se distribuyen a estas carpetas para superar sintéticamente el máximo inicial de 100 GB. Hay muchas limitaciones, incluidas una tasa máxima de crecimiento diario, restricciones de tamaño de importación y tipo de archivo, restricciones de búsqueda, restricciones de uso apropiado, cuándo se puede aumentar el archivo, el retraso de tiempo para cada aumento, si las carpetas se pueden eliminar después de una expansión, si las carpetas se pueden recuperar después de la eliminación, inexactitud de lectura/no lectura y otras limitaciones con entornos híbridos locales/nube.

Cómo puede ayudar Barracuda

Barracuda Cloud Archive Service ofrece almacenamiento verdaderamente ilimitado de manera simple y predecible por usuario. Los datos archivados son inmutables y se almacenan fuera de los datos de producción. No hay segmentos de almacenamiento intermedios que deban crearse a intervalos de 100 GB. El crecimiento no está limitado. No hay cargos por retener datos en buzones inactivos, independientemente del tamaño o del requisito de una retención por litigio.

07 | Respuesta y resiliencia limitadas después de la entrega

La protección del correo electrónico no termina cuando se entrega un mensaje. Los ataques modernos dependen de la ejecución retardada, acciones comprometidas de los usuarios y la usurpación de cuentas después de que un correo electrónico llega a la bandeja de entrada. Cuando esto sucede, las organizaciones deben comprender rápidamente el alcance, contener el impacto y recuperar los usuarios y datos afectados, no solo identificar el mensaje original.

Limitaciones de Microsoft

Defender para Office 365 se centra principalmente en el filtrado previo a la entrega y la protección en el momento del clic. Cuando las amenazas por correo electrónico eluden estos controles, la respuesta se limita en gran medida a alertas y acciones de remediación aisladas, como la eliminación de mensajes. Defender para Office 365 no ofrece de forma nativa flujos de trabajo coordinados de investigación, contención o recuperación a través de usuarios, identidades e impacto posterior. Como resultado, los equipos de TI deben evaluar manualmente el alcance, restablecer cuentas y recuperar datos utilizando herramientas y procesos separados.

Cómo puede ayudar Barracuda

Barracuda amplía la protección del correo electrónico hacia un modelo de seguridad impulsado por la resiliencia. Al correlacionar las amenazas de correo electrónico con la actividad posterior a la entrega, Barracuda Managed Cloud XDR ayuda a los equipos a comprender el contexto completo de un incidente y a responder de manera más efectiva. Cuando los ataques provocan el mal uso de cuentas o impacto en los datos, Barracuda Cloud-to-Cloud Backup y Entra ID Backup apoyan la recuperación de correo electrónico, datos de colaboración y configuraciones de identidad. Este enfoque ayuda a los equipos con recursos limitados a limitar el radio de impacto y restaurar las operaciones cuando la prevención por sí sola no es suficiente.

Supere las limitaciones de seguridad del correo electrónico nativas de Microsoft 365 utilizando Barracuda Email Protection.

Barracuda
Your business, secured.

Barracuda Networks y el logotipo de Barracuda Networks son marcas registradas de Barracuda Networks, Inc. en los Estados Unidos. Todos los demás nombres son propiedad de sus respectivos dueños.