6 razones fundamentales para realizar backup de Office 365

El caso de por qué las organizaciones deben proteger los datos de Office 365

VEEAM

Introducción

¿Tiene usted el control de sus datos de Office 365? ¿Tiene acceso a todos los elementos que necesita? La típica respuesta instintiva es "Claro que sí" o "Microsoft se encarga de todo".

Pero si realmente lo piensa, ¿está seguro de que es así?

Microsoft se ocupa de una gran parte y proporciona un gran servicio a sus clientes. Sin embargo, el enfoque principal de Microsoft es administrar la infraestructura de Office 365 y mantener el tiempo de actividad para sus usuarios. Ellos le otorgan a USTED la responsabilidad de sus datos. El concepto erróneo de que Microsoft realiza backups completos de todos sus datos por usted es bastante común y, sin un cambio en el modo de pensar, podría tener repercusiones dañinas cuando nadie se hace cargo de esa responsabilidad.

Básicamente, usted debe asegurarse de que tiene acceso a sus datos en Exchange Online, SharePoint Online y OneDrive para empresas, así como control de los mismos

Este informe explora los riesgos de no tener un backup de Office 365 en su arsenal, y por qué las soluciones de backup para Microsoft Office 365 llenan la brecha de la protección de datos y retención a largo plazo.

"Nos preocupan las políticas de retención y backup en Office 365. Microsoft se ocupa de nuestros datos, y la protección de datos de correos electrónicos históricos es importante. Es por eso que hemos decidido asegurarnos de que contamos con un backup de nuestros datos en Office 365".

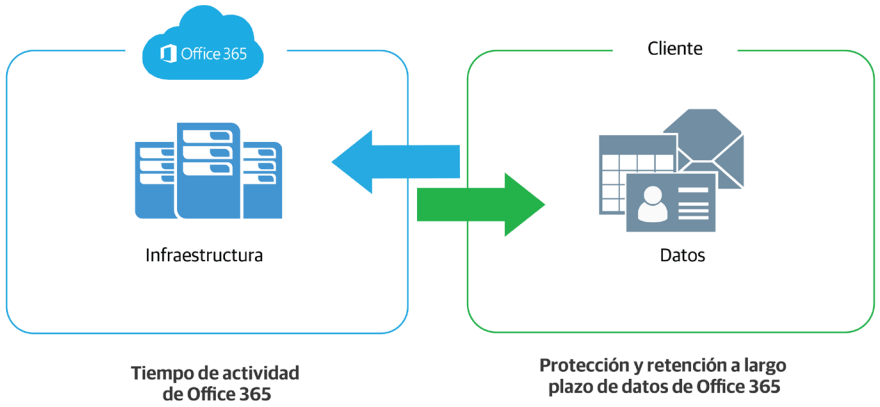
— ***Karen St.Clair***, Gerente de TI,
Columbia Power & Water Systems

El gran concepto erróneo de Office 365

Este malentendido se encuentra entre la responsabilidad percibida de Microsoft y la responsabilidad actual del usuario en la protección y retención a largo plazo de sus datos de Office 365. El backup y la recuperabilidad que Microsoft proporciona y lo que los usuarios asumen que obtienen suelen ser cosas diferentes. Esto quiere decir que, aparte de las precauciones estándar que Office 365 tiene disponibles, es posible que deba volver a evaluar el nivel de control que posee sobre sus datos y cuánto acceso tiene en realidad.

Microsoft Office 365 ofrece redundancia geográfica, lo que generalmente se confunde con el backup. El backup se realiza cuando se crea una copia de los datos del historial y es almacenada en otra ubicación. Sin embargo, es aún más importante que usted tenga acceso directo a ese backup y control sobre él. De esta manera, si los datos se pierden, son eliminados por accidente o son atacados malintencionadamente, usted podrá recuperarlos rápidamente. En cambio, la redundancia geográfica brinda protección contra fallas del sitio o del hardware. Por lo tanto, si hay una interrupción o la infraestructura se cae, sus usuarios permanecerán activos y generalmente ajenos a estos problemas subyacentes.

Microsoft se encarga de la infraestructura,
pero los datos siguen siendo responsabilidad de usted



"Con Office 365, son sus datos. Le pertenecen. Usted los controla".

— ***The Office 365 Trust Center***

6 razones por las que realizar backup de Office 365 es fundamental

Como una plataforma de Software como Servicio (SaaS, por sus siglas en inglés) sólida y altamente capaz, Microsoft Office 365 adapta perfectamente a las necesidades de muchas organizaciones. Office 365 proporciona Disponibilidad de aplicaciones y tiempo de actividad para asegurar que sus usuarios nunca se vean afectados, pero un backup de Office 365 puede protegerlo contra muchas otras amenazas de seguridad.

Usted o su jefe podrían pensar: "Probablemente con la papelera de reciclaje es más que suficiente".

Aquí es donde muchos se equivocan. El tiempo promedio desde el momento en que los datos se ven comprometidos hasta que esto se descubre es de más de 140 días [1]. Un lapso sorprendentemente grande. Existe una enorme probabilidad de que usted no se dé cuenta de que algo falla o hace falta hasta que sea demasiado tarde para la papelera de reciclaje.

Tras hablar con cientos de profesionales informáticos en todo el mundo que han migrado a Office 365, seis vulnerabilidades en la protección de datos encabezan la lista:

Eliminación accidental

Confusión y brechas en la política de retención

Amenazas a la seguridad interna

Amenazas a la seguridad externa

Requisitos legales y de cumplimiento

Manejo de implementaciones de correo híbrido y migraciones a Office 365

[1] https://discover.office.com/6-steps-to-holistic-security/chapter1/

Núm. 1 Eliminación accidental

Si usted elimina a un usuario, ya sea de forma intencional o no, esa eliminación se replica en la red junto con la eliminación de su sitio personal de SharePoint y sus datos de OneDrive.

La papelera de reciclaje nativa y las versiones de historiales incluidas en Office 365 solo pueden brindarle una protección contra la pérdida de datos de manera limitada, lo que puede convertir a una simple recuperación con un backup adecuado en un gran problema una vez que Office 365 haya eliminado los datos para siempre a través de redundancia geográfica o se agote el período de retención.

Existen dos tipos de eliminaciones en la plataforma de Office 365: la eliminación suave y la eliminación dura. Un ejemplo de eliminación suave es vaciar la carpeta de Elementos eliminados. Eso también es conocido como "Eliminado permanentemente". En este caso, el término permanente no significa que lo sea por completo, ya que el elemento puede encontrarse en los Elementos recuperables del buzón.

Una eliminación dura es cuando un elemento se etiqueta para ser borrado de la base de datos del buzón por completo. Una vez que esto ocurre, es irrecuperable, y punto.

Núm. 2 Confusión y brechas en la política de retención

El ritmo acelerado de los negocios en la era digital lleva a una continua evolución de las políticas, incluidas las de retención, que son difíciles de seguir y mucho más de gestionar. Al igual que la eliminación suave y dura, Office 365 tiene políticas limitadas de backup y retención que solo pueden repeler ciertas situaciones de pérdida de datos, y no pretenden ser una solución de backup integral.

Otro tipo de recuperación, una restauración en un punto en el tiempo de los elementos del buzón, no está dentro del alcance de Microsoft. En caso de un problema catastrófico, una solución de backup puede proporcionar la capacidad de retroceder a un punto en el tiempo anterior a ese problema y solucionar todo.

Con una solución de backup de Office 365, no existen brechas en la política de retención o inflexibilidad en la restauración. Backups a corto plazo o archivos a largo plazo, restauraciones granulares o en un punto en el tiempo: todo está al alcance de su mano, lo que permite una recuperación de datos rápida, fácil y confiable.

Núm. 3
Amenazas a la seguridad interna

La idea de una amenaza de seguridad lleva a pensar en hackers y virus. Sin embargo, las empresas experimentan amenazas desde su interior, y suelen ocurrir más veces de lo que usted cree. Las organizaciones han sido víctimas de amenazas provocadas por sus propios empleados, tanto intencional como accidentalmente.

El acceso a los archivos y contactos varía tan rápido, que resulta difícil vigilar aquellos en los usted que ha depositado su mayor confianza. Microsoft no tiene manera de saber la diferencia entre un usuario regular y un empleado despedido que intenta eliminar los datos críticos de la empresa antes de su partida. Además, algunos usuarios crean amenazas graves sin darse cuenta al descargar archivos infectados o filtrando accidentalmente nombres de usuarios y contraseñas a sitios que pensaban que eran confiables.

Otro ejemplo es la manipulación de la evidencia. Imagine a un empleado que elimina archivos o correos electrónicos incriminatorios estratégicamente, manteniéndolos fuera del alcance de los departamentos legal, de cumplimiento o de RR. HH.

Núm. 4
Amenazas a la seguridad externa

El malware y los virus, como el ransomware, han provocado daños graves a organizaciones a nivel mundial. No solo se pone en riesgo la reputación de la empresa, sino también la privacidad y seguridad de los datos internos y del cliente.

Las amenazas externas pueden introducirse sigilosamente a través de correos electrónicos o archivos adjuntos, y no siempre es suficiente con educar a los usuarios sobre el cuidado que se debe tener, especialmente cuando esos mensajes infectados parecen ser tan atractivos. Las funciones limitadas de backup/recuperación de Exchange Online no son adecuadas para manejar ataques graves. Los backups frecuentes ayudarán a asegurar que una copia por separado de sus datos no esté infectada y que pueda recuperarla rápidamente.

Núm. 5
Requisitos legales y de cumplimiento

Algunas veces, usted tendrá la necesidad de recuperar correos electrónicos, archivos u otros tipos de datos en medio de una acción legal de forma inesperada. Algo que usted piensa que nunca va a suceder, hasta que ocurre. Microsoft ha creado un par de redes de seguridad (Retención por juicio) pero, nuevamente, no son una solución de backup sólida capaz de mantener a su empresa libre de problemas legales. Por ejemplo, si usted elimina accidentalmente a un usuario, su buzón en retención, sitio personal en SharePoint y cuenta en OneDrive también se eliminarán.

Los requisitos legales y de cumplimiento, así como las regulaciones de acceso, varían en cada industria y país, pero las multas, penalidades y las disputas legales son tres cosas que no pueden estar en su lista de tareas pendientes.

Núm. 6
Manejo de implementaciones de correo híbrido y migraciones a Office 365

Las organizaciones que adoptan Office 365 generalmente necesitan una ventana de tiempo para que sirva como una ventana de transición entre Exchange en las instalaciones y Office 365 Exchange Online. Algunos incluso dejan una pequeña porción de su sistema tradicional en funcionamiento para tener una mayor flexibilidad y control adicional. La implementación de estos correos híbridos es común, pero plantea desafíos adicionales de administración.

La solución adecuada de backup para Office 365 debería ser capaz de manejar las implementaciones de correo híbrido y también tratar los datos de intercambio, de forma que la ubicación original se vuelva irrelevante.

Conclusión

Continúe y eche un vistazo más de cerca. Existen brechas de seguridad que quizá no haya podido ver antes.

Usted ya ha tomado una decisión empresarial inteligente al implementar Microsoft Office 365, ahora encuentre una solución de backup que le ofrezca acceso completo a sus datos de Office 365 y control total de los mismos para evitar riegos innecesarios de pérdida de datos.

Más información sobre el backup de Office 365 en:
https://www.veeam.com/es-lat/backup-microsoft-office-365.html


VEEAM