7 razones críticas para hacer backup de Microsoft 365

La razón por la que las organizaciones deben proteger los datos de Microsoft 365

Introducción

¿Tiene control sobre sus datos de Microsoft 365? ¿Tiene acceso a todos los elementos que necesita? La respuesta automática suele ser, "Por supuesto que sí" o "Microsoft ya se ocupa de eso". Pero si lo piensa detenidamente, ¿está seguro de ello ?

Microsoft se encarga de bastante. Ofrecen un excelente servicio a sus clientes, gestionan la infraestructura de Microsoft 365 y mantienen el tiempo de actividad de sus usuarios. Pero, por otro lado, le están confiriendo a USTED la responsabilidad de sus datos. Existe la idea errónea y común de que Microsoft realiza copias de seguridad de sus datos por usted de forma predeterminada, pero un backup completo de sus datos no está incluido en una licencia estándar de Microsoft 365. Sin un cambio de mentalidad, podría haber repercusiones dañinas cuando esta responsabilidad se deja desatendida.

En última instancia, debe asegurarse de tener acceso y control sobre sus datos de Exchange Online, SharePoint Online, OneDrive for Business y Microsoft Teams. Es más, incluso si no desea gestionar la infraestructura de backup, existen servicios de backup que se despliegan rápidamente sin necesidad de mantenimiento o gestión manual continua. Piense en el acceso instantáneo a una protección de datos personalizable, en una recuperación ultrarrápida y en la tranquilidad de saber que siempre tiene el control. Ahora piense en lo que está arriesgando al no tenerlos.

Este informe explora los riesgos de no tener un plan de backup de Microsoft 365 en su arsenal. Hablaremos sobre cómo las soluciones de backup para Microsoft 365 (en particular, los servicios de backup basados en la nube) solucionan la brecha de la protección de datos y retención a largo plazo y son realmente críticos para las organizaciones modernas.

> "Sun Chemical es una empresa verdaderamente global: Cada día, empleados de todo el mundo confían en las aplicaciones de Microsoft 365 para intercambiar datos críticos. Veeam Data Cloud for Microsoft 365 protege esta parte esencial de nuestro entorno, ayudando a nuestros empleados a trabajar de forma más productiva y ofreciéndonos una capa extra de ciberresiliencia."

Stuart Hudson
Director de Infraestructura Global de TI
Programas de infraestructura estratégica: AP, Sun Chemical

El gran malentendido de Microsoft 365

El malentendido se produce entre la percepción de que la responsabilidad recae en Microsoft, y la responsabilidad real del usuario en cuanto a la protección y retención a largo plazo de sus datos de Microsoft 365. La resiliencia y retención que ofrece Microsoft en una licencia estándar de Microsoft 365 y lo que los usuarios creen que tienen es frecuentemente bien distinto. Esto quiere decir que, dejando a un lado las precauciones estándar que Microsoft 365 tiene en marcha, puede que tenga que volver a evaluar el nivel de control que tiene de sus datos y cuál es el nivel de acceso real que tiene a los mismos.

Microsoft 365 ofrece geo-redundancia, lo cual se entiende con frecuencia como backup. La geo-redundancia, por el contrario, protege frente a un fallo del sitio o hardware, de forma que si se produce un fallo de la infraestructura o interrupción, los usuarios seguirán operando con normalidad ajenos a estos problemas subyacentes. Los backups, por otro lado, tienen lugar cuando se realiza una copia histórica de los datos y luego se almacenan en otra ubicación, separada del entorno de producción. Esto garantiza que existe una copia de sus datos con independencia de lo que ocurra en Microsoft 365, y que la opción de recuperación siempre está ahí.

Los backups, más que la redundancia geográfica, son la última línea de defensa de una organización, pero, tan importante como tenerlos es asegurarse de tener acceso directo y control sobre ellos. Cuando se pierden datos, se borran accidentalmente o sufren ataques malintencionados, necesita estar seguro de que podrá recuperarlos rápidamente.

Microsoft 365 es una responsabilidad compartida

> "Para todos los tipos de implementaciones en la nube, usted es el propietario de sus datos e identidades."

Fuente: [Responsabilidad compartida en la nube, Microsoft]

7 razones por las que es fundamental contar con un plan de backup de Microsoft 365

Como plataforma de Software as a Service (SaaS) robusta y de gran capacidad, Microsoft 365 satisface a la perfección las necesidades de muchas organizaciones. Microsoft 365 proporciona disponibilidad de aplicaciones y tiempo de funcionamiento para garantizar que sus usuarios nunca se vean afectados. Pero una solución de backup integral puede protegerle frente a otras muchas amenazas de seguridad y proporcionarle tranquilidad y una protección de datos sólida.

Usted o su jefe podría pensar, "Bueno, con la papelera de reciclaje puede que tenga suficiente". Aquí es donde muchas personas se equivocan. El tiempo que transcurre desde el momento en que los datos se ven comprometidos hasta que esto se descubre es de unos 140 días, lo que representa un periodo de tiempo sorprendentemente largo. Es muy probable que no se dé cuenta de que algo falta o se ha perdido hasta que ya sea demasiado tarde para la papelera de reciclaje, y este no es ni mucho menos el problema más acuciante.

Fuente: 7 pasos para una estrategia de seguridad integral, Microsoft

Hemos conversado con cientos de profesionales de TI de todo el mundo que han migrado a Microsoft 365, y a partir de sus análisis, hemos observado siete vulnerabilidades de la protección de datos:

1. Borrado accidental
2. Vacíos en la política de retención y confusión
3. Amenazas de seguridad internas
4. Amenazas de seguridad externas
5. Requisitos legales y de cumplimiento
6. Gestión de implementaciones de correo híbrido y migraciones a Microsoft 365
7. Estructura de datos de Teams

1. Borrado accidental

Supongamos que elimina a un usuario. Si elimina un usuario, tanto si es lo que quería, como si no, ese borrado se replica a través de la red, junto con la eliminación de su cuenta y buzón de correo de OneDrive for Business. Sin alternativas, las papeleras de reciclaje nativas y el historial de versiones de Microsoft 365 tienen una protección limitada contra la pérdida de datos, lo que convierte un trabajo de backup sencillo en un gran problema una vez que Microsoft 365 elimina georredundantemente esos datos para siempre, o si ha finalizado el periodo de retención.

Existen dos tipos de eliminaciones en la plataforma Microsoft 365: eliminación suave y eliminación dura. Un ejemplo de eliminación suave es vaciar la carpeta "Elementos eliminados". También se conoce como "Eliminados permanentemente", aunque en este caso, permanente no es completamente permanente, ya que el elemento aún se puede encontrar en la carpeta "Elementos recuperables". Una eliminación dura se produce cuando el elemento se marca para purgarse de la base de datos del buzón por completo. Una vez que esto sucede, es irrecuperable. Punto. Pero con una solución de backup como mecanismo de seguridad, la pérdida de datos por un borrado accidental es imposible.

2. Vacíos en la política de retención y confusión

El ritmo vertiginoso de los negocios en la era digital se presta a la constante evolución de las políticas, entre las que se incluyen las de retención, que son complicadas de mantener por no hablar de su gestión. Al igual que el borrado temporal y permanente, Microsoft 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, la restauración de elementos a un punto en el tiempo del buzón de correo, no está incluida en una licencia estándar de Microsoft 365. En el caso de un problema serio, una solución de backup puede proporcionar la posibilidad de volver a un punto en el tiempo anterior al problema y salvar el día. Es más, con una solución de backup específicamente diseñada para Microsoft 365, no existen brechas en la política de retención o falta de flexibilidad en la restauración. Backups a corto plazo o archivado a largo plazo, restauraciones granulares o a un punto en el tiempo: todo está siempre al alcance de su mano, lo que hace que la recuperación de datos sea rápida, fácil y confiable.

3. Amenazas de seguridad internas

La idea de amenaza para la seguridad nos trae a la mente la imagen de virus y hackers. Sin embargo, las empresas experimentan amenazas internas, y estas ocurren con más frecuencia de la que uno piensa. Las organizaciones caen víctimas de las amenazas que plantean sus propios empleados, bien sean intencionadas o accidentales. El acceso a los archivos y contactos cambia tan rápidamente que puede ser complicado vigilar a aquellos en los que ha depositado toda su confianza.

Microsoft no tiene forma de conocer la diferencia entre un usuario normal y un empleado despedido intentando eliminar datos críticos de la empresa antes de su marcha. Además de eso, algunos usuarios generan sin saberlo serias amenazas al descargar archivos infectados o divulgar de forma accidental nombres de usuarios y contraseñas en sitios que pensaban que eran de confianza. Otro ejemplo grave es la manipulación de pruebas. Imagine un empleado que elimine estratégicamente emails o archivos incriminatorios, dejando estos objetos fuera del alcance de los departamentos legales, del cumplimiento de la normativa o del departamento de RR. HH. Cuando sus datos de Microsoft 365 están protegidos adecuadamente, off-site y en la nube, se agregan capas de protección para combatir estas amenazas internas, lo que garantiza que sus datos permanezcan seguros y recuperables.

4. Amenazas de seguridad externas

Luego, por supuesto, están las amenazas externas maliciosas. El malware y los virus, como ransomware, han hecho un gran daño a muchas organizaciones en todo el mundo. No solamente ponen en riesgo la reputación de la empresa, sino que la privacidad y seguridad de los datos internos y de clientes también es puesta en compromiso.

Las amenazas externas a menudo se cuelan fácilmente a través de correos electrónicos y archivos adjuntos. No siempre es suficiente educar a los usuarios sobre lo que deben tener en cuenta, especialmente cuando los mensajes infectados parecen tan convincentes. Las funciones limitadas de backup y recuperación de Exchange Online son inadecuadas para manejar ataques graves. Los backups periódicos, especialmente aquellos que se administran off-site y en la nube a través de un servicio de backup, garantizan que una copia independiente de sus datos permanezca sin infectar y que se pueda recuperar rápidamente, lo que supera con creces las funciones limitadas de backup y recuperación de Exchange Online. Además, las mejores soluciones de servicios de backup se han integrado con Microsoft 365 Backup Storage, lo que hace que la recuperación rápida de grandes conjuntos de datos tras un ataque de ransomware sea una realidad para las organizaciones.

5. Requisitos legales y de cumplimiento

A veces, necesita recuperar inesperadamente correos electrónicos, archivos u otros tipos de datos en medio de una acción legal. Algo que nunca piensa que le va a pasar hasta que sucede. Microsoft 365 incluye un número reducido de redes de seguridad (retención por litigio y retención) integradas en el software, pero están muy lejos de ser una solución de backup robusta, y no evitarán que su empresa incurra en problemas legales.

Con un servicio de backup confiable, si por accidente borra correos electrónicos o documentos antes de implementar una retención legal, aún podrá recuperarlos para garantizar el cumplimiento de sus obligaciones legales. Los requisitos legales, de cumplimiento y la regulación normativa en materia de acceso pueden variar dependiendo de las industrias y los países, pero las multas, sanciones y litigios son tres cosas que no deberían tener cabida en su agenda.

Mejor aún, si no sabe por dónde empezar (ya que muchos de nosotros simplemente no tenemos la capacidad para mantenernos al día con los cambios en la legislación, las regulaciones y los requisitos), un servicio de backup se encargará de esto por usted. Con las capacidades de monitorización y generación de informes para ayudarle a cumplir los requisitos normativos y de cumplimiento, y la velocidad y facilidad de que son capaces las implementaciones de servicios de backup, puede tener la tranquilidad de saber que está cumpliendo con estos requisitos en cuestión de minutos.

6. Gestión de implementaciones de correo híbrido y migraciones a Microsoft 365

Las organizaciones que adoptan Microsoft 365 normalmente necesitan una ventana transitoria entre Exchange local y Microsoft 365 Exchange Online. Esta configuración, en la que una parte del sistema de correo electrónico permanece en las instalaciones locales mientras que el resto se traslada a Microsoft 365 Exchange Online, puede ofrecer mayor flexibilidad y control, y de hecho es muy común. Pero, a su vez, introduce complejidades adicionales de gestión, especialmente cuando se trata de backups. La administración de múltiples entornos requiere una supervisión cuidadosa para que los datos fluyan sin problemas y estén protegidos.

Aquí es donde un servicio de backup de Microsoft 365 se vuelve indispensable. El servicio de backup de Microsoft adecuado gestiona las implementaciones de correo electrónico híbrido de manera eficiente, tratando de la misma manera los datos de Exchange de los sistemas en las instalaciones locales y de Microsoft 365. Hace que la ubicación de origen sea irrelevante, simplifica el proceso de backup y elimina la necesidad de administrar sistemas múltiples y separados.

7. Estructura de datos de Teams

Más que nunca, las personas están creando Teams para la colaboración en proyectos e iniciativas especiales, todo a un ritmo cada vez más rápido. Pero una vez que complete un proyecto, es importante conservar una copia del mismo para necesidades a largo plazo, como requisitos legales y de cumplimiento. Aquí es donde las organizaciones suelen encontrar problemas. Con más frecuencia de la que le gustaría, estos Teams se eliminan por error o se les aplican incorrectamente las políticas de retención y, al hacerlo, el resultado es que los archivos y documentos esenciales no están disponibles.

Con un servicio de backup de Microsoft 365, esto nunca sucede. Sus datos siempre están ahí, sin importar quién o qué los elimine. Incluso puede ayudar en escenarios a corto plazo. Por ejemplo, si un empleado dice algo inapropiado en una conversación de Teams y luego borra el mensaje, es fácil acceder a los backups. Los datos de Teams siempre están a solo un par de clics de recuperarse y estar disponibles para que RR. HH los revise.

Más que nada, la confianza en sus backups es fundamental. Saber que existen y que están debidamente protegidos proporciona protección de lo desconocido, pero también ofrece una variedad de formas de restaurar Teams o canales perdidos o borrados accidentalmente. Adoptar un servicio de backup diseñado específicamente para Microsoft Teams garantiza que sus datos estén siempre disponibles, no importa lo que suceda o cuándo.

Razón adicional: gestión de identidades y acceso

Entra ID (anteriormente Azure Active Directory) actúa como la columna vertebral de Microsoft 365, manteniendo conectados todos los servicios de administración de identidades y accesos, proporcionando a las cuentas de usuario y grupos acceso a los recursos que están autorizados a usar. Su importancia no se puede exagerar, por lo que los actores de amenazas reconocen que la forma más rápida de poner de rodillas a una organización es apuntando a Entra ID, con ataques que ascienden a 600 millones cada día.

La necesidad de proteger Entra ID va más allá de las amenazas de ciberseguridad, los desafíos a los que se enfrentan las organizaciones reflejan los encontrados en las secciones anteriores: requisitos de cumplimiento complejos, límites de la papelera de reciclaje, eliminaciones accidentales y configuraciones incorrectas de políticas. En última instancia, es su responsabilidad proteger la identidad de su empresa. Una parte importante de la seguridad de los datos de Microsoft 365 es garantizar una protección completa para los usuarios, grupos, registros de aplicaciones y otros objetos relacionados de Entra ID.

Fuente: Informe de defensa digital de Microsoft 2024

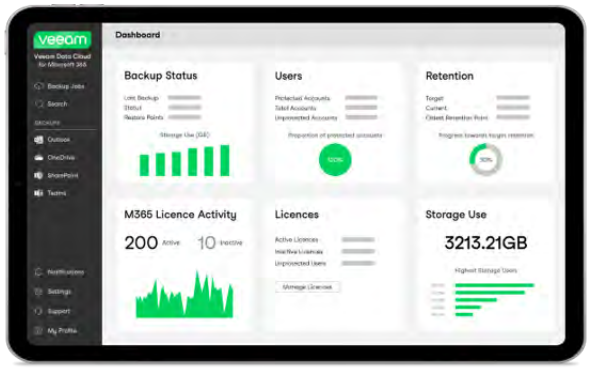
Conclusión

Tómese un momento para evaluar su postura de seguridad actual. Puede haber brechas que no sabía que existían. Ya ha tomado una decisión inteligente al implementar Microsoft 365. Ahora, combínelo con un servicio de backup que le proporcione acceso completo y control total sobre sus datos, y evite riesgos innecesarios de pérdida de datos.

Ya no es necesario invertir el tiempo, el dinero y los recursos asociados con una solución de software. Con **Veeam Data Cloud *for Microsoft 365***, puede aprovechar un servicio todo en uno con almacenamiento ilimitado incluido y elegir entre tres planes para cumplir sus objetivos de backup y recuperación ante desastres. Tanto si necesita velocidad y escalabilidad para backup y recuperación, control y flexibilidad, o una combinación de ambas, Veeam se ha asociado con Microsoft para garantizar que sus datos estén siempre protegidos, sean recuperables y escalables según las necesidades de su negocio.

Si este informe le ha sido de utilidad, le animamos a que lo reenvíe a un compañero: reenviar este informe.

Veeam Data Cloud *for Microsoft 365*: protección de datos resiliente simplificada



- Tecnología de backup para Microsoft 365 líder en la industria y de confianza
- Servicio de backup todo incluido con almacenamiento ilimitado
- Ahora con el nuevo Microsoft 365 Backup Storage

→ Solicitar demostración

→ Contáctenos

→ **¿Está interesado en la protección de Entra ID? Lea el white paper sobre las 6 razones para hacer *backup de Microsoft Entra ID*.**