¿Está cometiendo estos cinco enormes errores de copia de seguridad en la nube?

¿Está cometiendo estos cinco enormes errores de copia de seguridad en la nube? ¿Está creando o manteniendo copias de seguridad en la nube para su negocio y no está seguro de qué problemas de seguridad puede enfrentar en 2020 y más allá?

La protección de datos y la recuperación ante desastres ahora son más importantes que nunca. Los datos empresariales están creciendo a un ritmo más rápido que nunca, hasta el punto de que muchas soluciones de respaldo tradicionales no pueden mantenerse al día. Ahí es donde entra la nube.

Con su inmensa flexibilidad, capacidad casi infinita y facilidad de conectividad, el almacenamiento en la nube es una opción atractiva a la hora de hacer una copia de seguridad de sus archivos e infraestructura.

Sin embargo, si no tienes cuidado, puede ser una espada de doble filo.

Cometa cualquiera de estos cinco errores con su copia de seguridad, ¡y pronto lo lamentará!

5 problemas de seguridad de la copia de seguridad en la nube que no puede ignorar

Aquí hay cinco problemas esenciales que debe tener en cuenta al crear, monitorear y mantener copias de seguridad en la nube:

1. Ignorando el cifrado y haciendo copias de seguridad sin cifrar

Ha habido una serie de violaciones de datos de alto perfil en los últimos años . Estos deberían servir como advertencia para su negocio. La nube es tan segura como la crea. Si no cifra sus datos y controla el acceso a través de la autenticación de dos factores, sus copias de seguridad están en riesgo

Copias de seguridad cifradas

La seguridad no es algo que pueda ignorar, sin importar dónde estén almacenadas sus copias de seguridad. Si está almacenando sus copias de seguridad sin cifrado, corren el riesgo de verse comprometidas.

Con los ataques de ransomware cada vez más frecuentes, si las copias de seguridad almacenadas no están encriptadas, también pueden ser atacadas. Esto puede llevar a que los datos sean robados o eliminados «.
El cifrado es una capa crítica de seguridad para las copias de seguridad que debe tener implementadas. Con soluciones de respaldo líderes como Acronis Cyber □□Backup, todas las copias de respaldo están encriptadas.

Simplemente no olvide su clave de copia de seguridad, porque sin ella, no se puede acceder o restaurar su copia de seguridad.

Autenticación multifactor (MFA)

Al conectarse a sus servicios en la nube, asegúrese de habilitar la autenticación multifactor (MFA), también conocida como autenticación de dos factores (2FA).

MFA asegura su inicio de sesión en su sistema de respaldo con métodos adicionales de autenticación , como un mensaje de texto o un correo electrónico que confirma su inicio de sesión. Esto hace que los piratas informáticos tengan que

comprometer tanto sus credenciales de inicio de sesión como su teléfono o correo electrónico para obtener acceso ilegítimo a su servidor de respaldo.

2. Falla al probar y monitorear las copias de seguridad

La nube elimina una gran cantidad de sobrecarga, pero eso no significa que pueda olvidarse por completo de su sistema y esperar que todo funcione como un reloj. Es imprescindible que supervise su nube en busca de posibles problemas y pruebe regularmente las copias de seguridad para asegurarse de que todo sigue funcionando según lo previsto.

Ha habido innumerables ocasiones en las que una organización fue el objetivo de un ataque, y cuando fueron a restaurar servidores a partir de copias de seguridad, descubrieron que sus copias de seguridad estaban dañadas o les faltaba algún elemento clave.

Pruebe regularmente las copias de seguridad y supervise los registros de eventos para asegurarse de que no surjan problemas como este y que las copias de seguridad estén listas para restaurarse cuando las necesite.

Entre las pruebas de las copias de seguridad y los registros de monitoreo, los sistemas deben mantenerse y es posible que sea necesario agregar o eliminar nuevos datos de las copias de seguridad. ¡El espacio de almacenamiento también debe ser monitoreado!

Intente monitorear lo siguiente:

- Registros de acceso a archivos
- Qué archivos se están respaldando y si se están respaldando o no correctamente
- Actividad inusual o sospechosa, como la duplicación de archivos sin causa, picos de ancho de banda,

3. No planificar situaciones de desastre y recuperación de desastres

Las copias de seguridad en la nube pueden ser un gran servicio y proteger los datos de muchas maneras. Pero tener un sistema de respaldo en la nube no significa que pueda olvidarse de posibles dificultades en situaciones de desastre.

Los programas automatizados de recuperación de desastres pueden ser útiles para mantener su negocio funcionando sin problemas, pero tener un plan para desastres es imprescindible para mantener las copias de seguridad «.
Las personas necesitan saber qué procesos seguir en una crisis, como la actual pandemia de coronavirus y la fuerza laboral cada vez más remota, y quién es responsable de hacer qué. Cuanta más confusión haya, mayor será su tiempo de inactividad.

Saber cómo acceder a sus copias de seguridad o quién necesita implementar un plan de recuperación es importante cuando ocurre un desastre. Su tiempo es valioso y su proceso debe ser fluido y bien pensado de antemano.

Además del daño del desastre, perderá tiempo y dinero sin un plan sólido.

SUGERENCIA: Mantener las copias de seguridad almacenadas fuera del sitio protege los datos y garantiza la seguridad de las copias de seguridad.

4. Centrarse solo en sus archivos

Si solo está haciendo una copia de seguridad de archivos y ciertas carpetas importantes, se está perdiendo algunos datos vitales que ayudan a reducir el daño de un compromiso.

Asegúrese de mantener copias de seguridad de software, bases de datos e incluso registros, además de sus archivos

importantes. Cualquier dato que te falte de una copia de seguridad puede volver a atormentarte.

Puede haber un pequeño ingrediente faltante en su copia de seguridad que deja una configuración importante que falta y puede llevar a reelaborar aplicaciones completas.

Al crear y programar copias de seguridad, también debe realizar capturas de pantalla completas del sistema. Esto incluirá el sistema operativo y todo lo que contenga. Esto significa que en caso de desastre o ataque, puede implementar todo el sistema sin tener que configurar previamente un nuevo servidor con aplicaciones, reglas de firewall e información de dominio «.

Tener múltiples copias de seguridad que cubran cada parte de su infraestructura es importante para una recuperación rápida. Cualquier tiempo perdido durante un compromiso es un tiempo valioso, y cuanto más rápido pueda restaurar su servidor, más rápido podrá usted o su organización recuperarse.

5. Pobres horarios de respaldo

Es importante comprender qué diferentes programas de respaldo tiene disponibles y qué necesitará en una situación de compromiso o desastre.

Entre todos los días, cada hora, cada semana y cada minuto, hay muchas maneras de programar sus copias de seguridad, cada una de las cuales ofrece algo diferente del resto.

Si su sitio o servidor recibe un gran volumen de tráfico, cambios en la base de datos y registros o datos financieros importantes, es importante realizar copias de seguridad con frecuencia para mantener y restaurar sus datos.

Si trabaja con una empresa que obtiene cientos de entradas o cambios de datos en una hora, es posible que desee realizar una copia de seguridad por minutos o por hora, ya que hay

mucho dinero en juego por cada cambio que falta.

Si está ejecutando un servidor que no recibe mucho tráfico, una copia de seguridad diaria o semanal podría funcionar para usted. Todo depende del rendimiento de sus servidores y de la cantidad de datos que procesa.

Las copias de seguridad incrementales son una opción popular para muchas circunstancias, que son copias de seguridad solo realizadas a medida que cambian los datos y sin volver a copiar todo el sistema «.
Conozca sus recursos disponibles, su ancho de banda y su espacio para encontrar el programa de respaldo adecuado para usted. En la mayoría de los casos, realizar copias de seguridad con demasiada frecuencia es un gran problema.

Mantenga su juicio libre

La nube es una poderosa herramienta de respaldo, pero también puede causar más daño que bien si no sabe lo que está haciendo.

Afortunadamente, no es particularmente difícil de usar. Y si prefiere dejar los detalles técnicos a otra persona, siempre puede usar una solución de terceros como HostDime.

Al crear copias de seguridad, cronogramas y planes de recuperación, es fácil pasar cosas pequeñas durante un proceso de recuperación.

Sea diligente para probar las copias de seguridad y los horarios, realice pruebas completas de recuperación ante desastres y aprenda de las personas que han estado en estas situaciones antes «.
Es fácil pensar que una copia de seguridad semanal o diaria está bien para sus sistemas, hasta que esté en una posición en la que le falta información increíblemente vital que se ingresó en el último día u hora.

Comprender el tipo de datos que tiene puede brindarle una excelente perspectiva de lo que necesitará en caso de desastre o compromiso.

Tómese el tiempo extra para comprender sus copias de seguridad en la nube y lo que necesita de ellas. Las copias de seguridad pueden ser la diferencia entre un ataque que cierra una empresa por completo o solo durante unas horas.

Leer también: Copia de seguridad, restauración y recuperación de Bare Metal: 7 cosas que los profesionales de TI deben saber;¿Qué es BaaS? Backup as a Service, definición, concepto, significado ; Cómo hacer un backup de un cloud server