AIRNITE

ZERO DAY

NÚMERO 17/2026 · SEGURIDAD INFORMÁTICA

Ataque a través de la copia de seguridad: cómo un servicio de backup abrió la puerta a Microsoft 365

En octubre de 2026, unos atacantes abusaron de los accesos del servicio ConnectWise Cloud Backup para entrar en cientos de entornos de Microsoft 365 de clientes. Qué pasó y por qué cada app con permisos en su nube es un riesgo.

Publicado: 21 de noviembre de 2026 Tiempo de lectura: 6 min Autor: Redacción de Airnite

// LA SITUACIÓN EN CIFRAS

300+
inicios de sesión logrados en tenants de M365
de unos 1.000 tenants con actividad sospechosa (Huntress según heise)

15/10/2026
primeros accesos no autorizados
intentos desde el 13/10/2026 (heise)

7
identidades de aplicación desactivadas
el 17/10/2026, servicio suspendido (ConnectWise)

7 / 30 días
conservación de los registros de inicio de sesión
Entra ID sin o con licencia P1/P2 (heise)

Las copias de seguridad deben salvarnos cuando algo sale mal. En octubre de 2026, precisamente un servicio de backup se convirtió en la puerta de entrada: unos atacantes usaron los accesos de **ConnectWise Cloud Backup** (antes SkyKick) para iniciar sesión en los entornos de Microsoft 365 de sus clientes. El portal alemán heise habló de un ataque a la cadena de suministro que afectó a cientos de tenants.

// ¿Qué ha pasado?

El **16 de octubre de 2026**, ConnectWise informó en su página de seguridad de que investigaba intentos de acceso no autorizado. El 17 de octubre, según el proveedor, desactivó **siete identidades de aplicación** y suspendió Cloud Backup revocando los certificados de las conexiones afectadas; por precaución pausó otros servicios. El 20 de octubre, ConnectWise confirmó un **acceso no autorizado a identidades de aplicación** de Cloud Backup.

Según heise, los intentos de inicio de sesión empezaron el 13 de octubre y los primeros accesos no autorizados se produjeron el **15 de octubre**. Según el artículo de heise, la empresa de seguridad Huntress encontró primero accesos no autorizados en 162 tenants y después actividad sospechosa en unos **1.000 tenants**, de los que más de **300 tuvieron éxito**; se revisaron unos 10.000 tenants de Microsoft 365 con apps de ConnectWise. A finales de octubre, ConnectWise inició una recuperación por fases mediante una nueva aplicación.

// ¿Cómo funciona el ataque?

Un servicio de backup para Microsoft 365 necesita permisos amplios: debe poder leer buzones, archivos y datos de Teams. Para ello, el cliente configura en su tenant una aplicación que inicia sesión con certificados o secretos del proveedor. Quien obtiene esas credenciales puede, según heise, entrar en los tenants de los clientes con los permisos del servicio de backup. heise apunta como vía probable a una aserción de autenticación de la aplicación robada, aunque no estaba confirmado.

ConnectWise subraya que sus archivos de copia siguen cifrados, aislados y conservados, sin indicios de compromiso. A la vez, el proveedor afirma que no puede determinar para cada cliente si su tenant de Microsoft 365 se vio afectado: cada tenant debe comprobarlo por su cuenta. Un inicio de sesión exitoso no demuestra por sí solo que se copiaran datos.

// ¿A quién afecta?

Se vieron afectados clientes de ConnectWise Cloud Backup, a menudo a través de proveedores de servicios informáticos que gestionan el servicio para muchas empresas. Eso convierte el caso en un ejemplo típico de ataque a la cadena de suministro: un proveedor con acceso a muchos clientes vale más para los atacantes que cualquier cliente aislado.

El patrón vale para cualquier empresa con Microsoft 365 u otra nube. Herramientas de backup, soluciones de seguridad, archivado, conectores de CRM: muchas apps tienen en el tenant permisos que casi nadie revisa. Y quien conserva poco tiempo los registros de inicio de sesión apenas puede aclarar después lo ocurrido. Según heise, Entra ID borra estos registros a los siete días sin licencia adicional y a los 30 días con licencia P1/P2.

// ¿Qué hay que hacer ahora?

Los administradores deben saber qué apps de terceros trabajan en su tenant y con qué permisos, eliminar las innecesarias y vigilar los inicios de sesión de las entidades de servicio. Tras un aviso de un proveedor: bloquear accesos, renovar secretos y asegurar y analizar los propios registros. Y planificar las copias para que funcionen aunque caiga el servicio de backup. La lista de control de abajo resume los pasos.

// ¿Cómo ayuda Airnite?

En la **consultoría**, Airnite revisa su tenant de Microsoft 365 en busca de apps de terceros y permisos y configura la vigilancia y conservación de registros. Con **pruebas de penetración** mostramos hasta dónde llegaría un atacante con el acceso de un proveedor. En la **formación**, los administradores aprenden a reconocer inicios de sesión sospechosos de aplicaciones.

> Nota: no hemos comprobado en el original los datos sobre la autoría, por lo que no los recogemos. Las cifras de tenants afectados proceden de Huntress a través de heise. Estado de la investigación: 21 de noviembre de 2026.

Lista de control: qué hacer ahora

- [+] Enumere todas las aplicaciones empresariales y apps de terceros del tenant de Microsoft 365 y revise sus permisos.
- [+] Elimine las apps que ya no necesite y reduzca los permisos al mínimo.
- [+] Analice con regularidad los registros de inicio de sesión de las entidades de servicio y consérvelos lo bastante para poder reconstruir incidentes.
- [+] Tras un aviso de un proveedor, bloquee de inmediato sus accesos, renueve secretos y certificados y controle la reactivación.
- [+] Planifique copias de seguridad que sigan siendo utilizables aunque falle el propio servicio de backup.

[+] Obligue por contrato a los proveedores a notificar, ser transparentes y colaborar en incidentes de seguridad.

Cómo ayuda Airnite

- Consultoría – Una mirada externa sobre sus planes y proyectos.
- Pruebas de penetración y seguridad – Ataques controlados con un informe claro y un plan de medidas.
- Formación – Su equipo aprende nuestras herramientas y procesos.

¿Qué apps pueden entrar en su Microsoft 365?

Airnite revisa su tenant de Microsoft 365 en busca de aplicaciones empresariales, entidades de servicio y permisos de terceros, analiza los registros de inicio de sesión y configura alertas. Así sabrá quién está en su nube y con qué permisos, antes que un atacante.

Solicitar una primera conversación · Escribir un correo · Por WhatsApp

Contacto

¿Preguntas sobre este artículo? Escríbanos por WhatsApp: +49 174 6834842

Leer en línea: https://airnite.de/es/revista/connectwise-cloud-backup-m365-cadena-suministro/

Fuentes

Cada dato de este artículo se basa en las fuentes indicadas a continuación. Las fuentes primarias están señaladas.

1. **ConnectWise Trust Center · Advisories: Cloud Backup (formerly known as SkyKick) Service Interruption** · desde el 16/10/2026, actualizado de forma continua · FUENTE PRIMARIA
   Fuente primaria (proveedor): acceso no autorizado a identidades de aplicación, desconexión, estado de las copias, recuperación
   https://www.connectwise.com/company/trust/advisories
2. **heise online · Lieferkettenangriff auf Backup-Dienst trifft Hunderte M365-Tenants** · 21/10/2026
   Prensa especializada: desarrollo, cifras de Huntress, consejos para administradores
   https://www.heise.de/news/Angriffe-via-ConnectWise-Cloud-Backup-11495835.html
3. **Borns IT- und Windows-Blog · „Black October" 2026: IT-Katastrophen der letzten Tage** · 22/10/2026
   Blog especializado: contexto de los incidentes de octubre de 2026
   https://borncity.com/blog/2026/10/22/black-october-2026-it-katastrophen-der-letzten-tage/

Información editorial general, no constituye asesoramiento jurídico ni una evaluación de sus sistemas concretos. Vigencia: fecha de publicación.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de