AIRNITE

ZERO DAY

ISSUE 17/2026 · IT SECURITY

Attack through the backup: how a backup service became a way into Microsoft 365

In October 2026, attackers abused the access of the ConnectWise Cloud Backup service to sign in to hundreds of customers' Microsoft 365 environments. What happened and why every app with rights to your cloud is a risk.

Published: 21 November 2026 Reading time: 6 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

300+
successful sign-ins to M365 tenants
out of around 1,000 tenants with suspicious activity (Huntress via heise)

15 Oct 2026
first unauthorised sign-ins
attempts from 13 Oct 2026 (heise)

7
application identities disabled
on 17 Oct 2026, service suspended (ConnectWise)

7 / 30 days
retention of sign-in logs
Entra ID without or with P1/P2 licence (heise)

Backups are supposed to save you when something goes wrong. In October 2026, of all things a backup service became the way in: attackers used the access of **ConnectWise Cloud Backup** (formerly SkyKick) to sign in to customers' Microsoft 365 environments. The German IT news site heise called it a supply chain attack that hit hundreds of tenants.

// What happened?

On **16 October 2026**, ConnectWise reported on its security page that it was investigating attempts at unauthorised access. On 17 October, the vendor says it disabled **seven application identities** and suspended Cloud Backup by revoking the certificates of the affected application connections; further services were paused as a precaution. On 20 October, ConnectWise confirmed **unauthorised access to application identities** of Cloud Backup.

According to heise, sign-in attempts began on 13 October, with the first unauthorised sign-ins on **15 October**. According to the heise report, security firm Huntress initially found unauthorised sign-ins in 162 tenants, later suspicious activity in around **1,000 tenants**, of which more than **300 were successful**; around 10,000 Microsoft 365 tenants with ConnectWise apps were reviewed. At the end of October, ConnectWise began a phased recovery via a new application.

// How does the attack work?

A backup service for Microsoft 365 needs extensive rights: it must be able to read mailboxes, files and Teams data. For this, the customer sets up an application in their own tenant that signs in with the vendor's certificates or secrets. Whoever gets hold of these vendor credentials can, according to heise, log in to customers' tenants – with the backup service's rights. heise names a stolen application sign-in assertion as the likely route, but this had not been confirmed.

ConnectWise stresses that its backup archives remain encrypted, isolated and preserved, with no indication of compromise. At the same time, the vendor says it cannot determine for each customer whether their Microsoft 365 tenant was affected – each tenant has to check for itself. A successful sign-in alone does not prove that data was copied.

// Who is affected?

ConnectWise Cloud Backup customers were affected, often through IT service providers that run the service for many companies. That makes the case typical of supply chain attacks: a vendor with access to many customers is more valuable to attackers than any single customer.

The pattern applies to every company using Microsoft 365 or another cloud. Backup tools, security solutions, archiving, CRM connectors – many apps hold rights in the tenant that rarely anyone reviews. And anyone who keeps sign-in logs only briefly can hardly establish afterwards what happened. According to heise, Entra ID deletes these logs after seven days without an additional licence and after 30 days with a P1/P2 licence.

// What should you do now?

Administrators should know which third-party apps work in their tenant with which rights, remove unnecessary ones and monitor service principal sign-ins. After a vendor warning: block access, renew secrets, secure and analyse your own logs. And plan backups so they work even if the backup service fails. The checklist below sums up the steps.

// How does Airnite help?

In **consulting**, Airnite checks your Microsoft 365 tenant for third-party apps and permissions and sets up monitoring and log retention. With **penetration tests**, we show how far an attacker would get with a service provider's access. In **training**, administrators learn to recognise suspicious app sign-ins.

> Note: we have not verified attribution claims in the original and therefore have not included them. Figures on affected tenants come from Huntress via heise. Research status: 21 November 2026.

Checklist: what to do now

[+] List all enterprise applications and third-party apps in your Microsoft 365 tenant and review their permissions.

[+] Remove apps you no longer need and reduce permissions to the minimum.

[+] Regularly analyse service principal sign-in logs – and keep them long enough for incidents to remain traceable.

[+] After a vendor warning, immediately block its access, renew secrets and certificates and control re-enablement deliberately.

[+] Plan backups so they remain usable even if the backup service itself fails.

[+] Contractually oblige service providers to notify, be transparent and cooperate in security incidents.

How Airnite helps

- Consulting – An outside view of your plans and projects.
- Penetration Testing & Security – Controlled attacks with a clear report and action plan.
- Training – Your team learns our tools and processes.

Which apps are allowed into your Microsoft 365?

Airnite checks your Microsoft 365 tenant for enterprise applications, service principals and third-party permissions, analyses sign-in logs and sets up alerts. You see who is in your cloud with which rights – before an attacker does.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/connectwise-cloud-backup-m365-supply-chain/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **ConnectWise Trust Center · Advisories: Cloud Backup (formerly known as SkyKick) Service Interruption** · from 16 Oct 2026, continuously updated · PRIMARY SOURCE
   Primary source (vendor): unauthorised access to application identities, shutdown, state of backups, recovery
   https://www.connectwise.com/company/trust/advisories
2. **heise online · Lieferkettenangriff auf Backup-Dienst trifft Hunderte M365-Tenants** · 21 Oct 2026
   Trade press: sequence, Huntress figures, advice for administrators
   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 Oct 2026
   Trade blog: context of the October 2026 incidents
   https://borncity.com/blog/2026/10/22/black-october-2026-it-katastrophen-der-letzten-tage/

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

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