AIRNITE

ZERO DAY

NUMÉRO 17/2026 · SÉCURITÉ INFORMATIQUE

L’attaque par la sauvegarde : comment un service de backup est devenu une porte d’entrée vers Microsoft 365

En octobre 2026, des attaquants ont détourné les accès du service ConnectWise Cloud Backup pour se connecter à des centaines d’environnements Microsoft 365 de clients. Ce qui s’est passé et pourquoi chaque application ayant des droits sur votre cloud est un risque.

Publié le: 21 novembre 2026 Temps de lecture: 6 min Auteur: Rédaction Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUATION EN CHIFFRES

300+
connexions réussies à des tenants M365
sur environ 1 000 tenants avec activité suspecte (Huntress selon heise)

15/10/2026
premières connexions non autorisées
tentatives dès le 13/10/2026 (heise)

7
identités d'application désactivées
le 17/10/2026, service suspendu (ConnectWise)

7 / 30 jours
conservation des journaux de connexion
Entra ID sans ou avec licence P1/P2 (heise)

Les sauvegardes doivent sauver la mise quand quelque chose tourne mal. En octobre 2026, c'est pourtant un service de sauvegarde qui est devenu la porte d'entrée : des attaquants ont utilisé les accès de **ConnectWise Cloud Backup** (anciennement SkyKick) pour se connecter aux environnements Microsoft 365 de clients. Le site spécialisé allemand heise a parlé d'une attaque de la chaîne d'approvisionnement touchant des centaines de tenants.

// Que s'est-il passé ?

Le **16 octobre 2026**, ConnectWise a indiqué sur sa page de sécurité enquêter sur des tentatives d'accès non autorisé. Le 17 octobre, l'éditeur dit avoir désactivé **sept identités d'application** et suspendu Cloud Backup en révoquant les certificats des connexions concernées ; d'autres services ont été mis en pause par précaution. Le 20 octobre, ConnectWise a confirmé un **accès non autorisé à des identités d'application** de Cloud Backup.

Selon heise, les tentatives de connexion ont commencé le 13 octobre, et les premières connexions non autorisées ont eu lieu le **15 octobre**. D'après l'article de heise, la société de sécurité Huntress a d'abord trouvé des connexions non autorisées dans 162 tenants, puis une activité suspecte dans environ **1 000 tenants**, dont plus de **300 réussies** ; quelque 10 000 tenants Microsoft 365 dotés d'applications ConnectWise ont été examinés. Fin octobre, ConnectWise a lancé une reprise progressive via une nouvelle application.

// Comment fonctionne l'attaque ?

Un service de sauvegarde pour Microsoft 365 a besoin de droits étendus : il doit pouvoir lire boîtes mail, fichiers et données Teams. Le client installe pour cela dans son tenant une application qui se connecte avec des certificats ou secrets de l'éditeur. Quiconque obtient ces accès peut, selon heise, se connecter aux tenants des clients – avec les droits du service de sauvegarde. heise évoque comme voie probable une assertion d'authentification de l'application volée, sans que cela ait été confirmé.

ConnectWise souligne que ses archives de sauvegarde restent chiffrées, isolées et préservées, sans indice de compromission. L'éditeur indique en même temps ne pas pouvoir déterminer pour chaque client si son tenant Microsoft 365 a été touché – chaque tenant doit le vérifier lui-même. Une connexion réussie ne prouve pas à elle seule que des données ont été copiées.

// Qui est concerné ?

Les clients de ConnectWise Cloud Backup étaient concernés, souvent via des prestataires informatiques exploitant le service pour de nombreuses entreprises. Le cas est typique des attaques de la chaîne d'approvisionnement : un fournisseur ayant accès à de nombreux clients vaut plus pour un attaquant que n'importe quel client isolé.

Le schéma concerne toute entreprise utilisant Microsoft 365 ou un autre cloud. Outils de sauvegarde, solutions de sécurité, archivage, connecteurs CRM : de nombreuses applications disposent de droits dans le tenant que personne ne vérifie. Et qui conserve trop peu de temps ses journaux de connexion ne peut guère reconstituer après coup ce qui s'est passé. Selon heise, Entra ID supprime ces journaux après sept jours sans licence supplémentaire et après 30 jours avec une licence P1/P2.

// Que faire maintenant ?

Les administrateurs doivent savoir quelles applications tierces opèrent dans leur tenant et avec quels droits, supprimer celles qui sont inutiles et surveiller les connexions des principaux de service. Après une alerte d'un fournisseur : bloquer les accès, renouveler les secrets, sécuriser et analyser ses propres journaux. Et prévoir des sauvegardes qui fonctionnent même si le service de sauvegarde tombe. La check-list ci-dessous résume les étapes.

// Comment Airnite vous aide-t-il ?

En **conseil**, Airnite examine votre tenant Microsoft 365 à la recherche d'applications tierces et d'autorisations, et met en place surveillance et conservation des journaux. Avec des **tests d'intrusion**, nous montrons jusqu'où un attaquant irait avec l'accès d'un prestataire. En **formation**, les administrateurs apprennent à repérer les connexions d'applications suspectes.

> Remarque : nous n'avons pas vérifié dans l'original les informations sur les auteurs et ne les reprenons donc pas. Les chiffres sur les tenants touchés proviennent de Huntress via heise. État de la recherche : 21 novembre 2026.

Check-list : ce qu'il faut faire maintenant

[+] Lister toutes les applications d'entreprise et applications tierces du tenant Microsoft 365 et vérifier leurs autorisations.

[+] Supprimer les applications inutiles et réduire les autorisations au strict nécessaire.

[+] Analyser régulièrement les journaux de connexion des principaux de service – et les conserver assez longtemps pour retracer un incident.

[+] Après une alerte d'un fournisseur, bloquer immédiatement ses accès, renouveler secrets et certificats et contrôler la réactivation.

[+] Prévoir des sauvegardes utilisables même si le service de sauvegarde lui-même tombe.

[+] Obliger contractuellement les prestataires à notifier, à être transparents et à coopérer en cas d'incident.

Comment Airnite vous aide

- Conseil – Un regard extérieur sur vos projets.
- Tests d'intrusion et sécurité – Attaques contrôlées avec rapport clair et plan d'action.
- Formations – Votre équipe apprend nos outils et méthodes.

Quelles applications ont accès à votre Microsoft 365 ?

Airnite examine votre tenant Microsoft 365 à la recherche d'applications d'entreprise, de principaux de service et d'autorisations tierces, analyse les journaux de connexion et met en place des alertes. Vous voyez qui se trouve dans votre cloud et avec quels droits – avant un attaquant.

Demander un premier échange · Écrire un e-mail · Par WhatsApp

Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/connectwise-cloud-backup-m365-chaine-approvisionnement/

Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.

1. **ConnectWise Trust Center · Advisories: Cloud Backup (formerly known as SkyKick) Service Interruption** · à partir du 16/10/2026, mises à jour continues · SOURCE PRIMAIRE
   Source primaire (éditeur) : accès non autorisé aux identités d'application, coupure, état des sauvegardes, reprise
   https://www.connectwise.com/company/trust/advisories
2. **heise online · Lieferkettenangriff auf Backup-Dienst trifft Hunderte M365-Tenants** · 21/10/2026
   Presse spécialisée : déroulé, chiffres de Huntress, conseils aux administrateurs
   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 spécialisé : contexte des incidents d'octobre 2026
   https://borncity.com/blog/2026/10/22/black-october-2026-it-katastrophen-der-letzten-tage/

Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.

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