Pourquoi la sauvegarde et la restauration ne suffisent-elles pas à contrer les rançongiciels ?

Réponse courte : Les sauvegardes ne traitent que la dernière étape d'une attaque par rançongiciel — le chiffrement. Au moment où le chiffrement commence, les attaquants ont généralement déjà volé des identifiants et exfiltré vos données. La restauration à partir d'une sauvegarde permet de récupérer vos fichiers ; elle ne fait rien concernant les données déjà entre les mains de l'attaquant.

Le rançongiciel est la dernière étape, pas la première

Une intrusion typique se déroule en trois étapes :

1. **Vol d'identité** — des identifiants sont compromis pour obtenir un accès.
2. **Vol de données** — la propriété intellectuelle, les dossiers clients et d'autres données sensibles sont exfiltrés.
3. **Chiffrement** — les fichiers sont verrouillés et une rançon est exigée.

Les stratégies de récupération n'interviennent qu'à la troisième étape. La violation de confidentialité et la perte de contrôle opérationnel ont déjà eu lieu.

Le coût réel

Le risque commercial le plus important lié aux rançongiciels n'est généralement pas la rançon elle-même — c'est la perte de revenus due à une interruption prolongée et les dommages réputationnels qui en découlent. Prévenir la compromission initiale protège les deux, c'est pourquoi la prévention doit précéder la planification de la récupération plutôt que s'y substituer.

Revision #1
Created 2026-07-24 06:55:19 UTC by Dennis Underwood
Updated 2026-07-24 06:55:19 UTC by Dennis Underwood