AYI NEDJIMI
Consultants

MSP : pourquoi votre prestataire est devenu votre principale faille

8 mai 2026 • Mis à jour le 17 mai 2026 • 8 min de lecture • 1401 mots • 62 vues •

Trois compromis MSP en sept jours via cPanel, SimpleHelp et Trellix : la frontière de votre cybersécurité ne s'arrête plus à votre périmètre. Analyse des leviers concrets pour reprendre la main sur les accès tiers en contexte NIS 2.

Trois compromis MSP majeurs en sept jours. cPanel, SimpleHelp, Trellix. Si votre stratégie de sécurité s'arrête à votre périmètre direct, vous êtes en train de payer pour des attaquants qui passent par la porte d'à côté — celle de votre prestataire.

Le MSP, ce point unique de défaillance qu'on refuse de regarder

Quand je rentre dans un comité de pilotage cyber d'une PME ou d'une ETI, je pose toujours la même question : « combien de prestataires ont un accès administrateur à votre infrastructure ? ». La réponse moyenne tourne autour de quatre. L'hébergeur web, l'infogérant infrastructure, l'éditeur de votre ERP qui télémaintient en VPN, le prestataire RMM qui pousse les patches sur les postes utilisateurs. Quatre identités à privilèges qui ne figurent pas dans votre IAM, qui ne respectent pas votre politique de mots de passe, qui n'envoient pas leurs logs à votre SIEM. Quatre maillons que vous n'auditez pas et qui peuvent ruiner six mois d'efforts de sécurité interne en une nuit.

Cette semaine, trois exemples concrets. Lundi 5 mai, ShinyHunters a publié les données de 275 millions d'utilisateurs Canvas — on parle d'Instructure, prestataire LMS de Harvard, MIT, Oxford et plus de 9 000 établissements. Vendredi, MuddyWater a été pris la main dans le sac à se faire passer pour le ransomware Chaos via Microsoft Teams pour exfiltrer des credentials. Mardi 6 mai, Trellix — un éditeur de cybersécurité — a annoncé la fuite d'une partie de son code source. Le point commun ? Aucun. Sauf un : dans chaque cas, c'est l'utilisateur final qui paie le prix d'une décision prise par un fournisseur en amont.