AYI NEDJIMI Consultants

Education : la cible cyber qu'on a laissé tomber

9 mai 2026 • Mis à jour le 17 mai 2026 • 8 min de lecture • 1148 mots • 63 vues •

L'attaque Canvas n'est pas un accident. Elle révèle un sous-investissement structurel en cybersécurité du secteur éducatif. Analyse et recommandations.

L'attaque Canvas a sorti 275 millions de dossiers d'élèves et d'enseignants en moins d'une semaine. Tout le monde fait mine d'être surpris. Personne ne devrait l'être. Le secteur éducatif est devenu en trois ans la deuxième cible la plus rentable des groupes d'extorsion, et on a regardé ailleurs.

Une accumulation de signaux ignorés

PowerSchool en janvier 2025. Illuminate Education en 2024. Finalsite en 2022. La liste des compromissions massives dans l'écosystème edtech américain est documentée depuis cinq ans. Chaque incident a généré son cycle médiatique de 72 heures, ses recommandations de la CISA, ses promesses de rotation de mots de passe. Et puis on est passés à autre chose. Le résultat : Canvas/Instructure aujourd'hui, et ce n'est pas le dernier dossier qu'on ouvrira cette année.

Ce qui distingue le secteur éducatif n'est pas un manque de compétence chez ses RSSI. C'est une équation économique simple. Une université concentre des données extrêmement sensibles : identifiants étudiants, dossiers médicaux des infirmeries, données financières des bourses, recherches en cours, brevets, propriété intellectuelle académique. Un district scolaire centralise les coordonnées de mineurs, les dossiers de protection de l'enfance, les évaluations psychologiques. Tout ça avec des budgets cybersécurité divisés par cinq comparés à ceux d'une banque de taille équivalente.

L'illusion du SaaS éducatif

Le passage massif au SaaS dans les années 2018-2022 a été vendu aux DSI éducation comme une externalisation des risques. La promesse était simple : externaliser le LMS, le SIS, l'ERP scolaire chez des éditeurs spécialisés revenait à externaliser leur cybersécurité,