Principaux défis de cybersécurité dans le secteur de l'éducation

Digital Security
Progress. Protected.

Pourquoi les institutions d'enseignement sont des cibles attrayantes

Les établissements d'enseignement sont dans la ligne de mire de cybercriminels sophistiqués et d'acteurs sponsorisé par des états. Au second trimestre 2024, Microsoft a classé le secteur de l'éducation au troisième rang de ceux les plus ciblés au niveau mondial, tandis que les chercheurs d'ESET ont observé une intense activité des groupes APT (menaces persistantes avancées) dirigée contre des écoles et des universités par des groupes alignés sur la Chine, la Corée du Nord, l'Iran et la Russie.

Une véritable tempête de vulnérabilités rend le secteur particulièrement attractif : réseaux poreux, bases d'utilisateurs importantes et transitoires, budgets de sécurité limités, technologies anciennes et données de grande valeur. Rien qu'au Royaume-Uni, 71 % des écoles secondaires et la quasi-totalité des universités ont signalé des atteintes graves à la sécurité au cours de l'année écoulée, contre seulement la moitié des entreprises. Aux États-Unis, le K12 Security Information Exchange (K12 SIX) a enregistré, en moyenne, plus d'un cyberincident par jour d'école entre 2016 et 2022.

Le gain financier reste le motif dominant,
mais l'espionnage est une minorité significative.

88 %

des motifs des acteurs sont financiers et 18 % sont liés à l'espionnage.

Source : *Verizon : Rapport de Verizon sur les fuites de données en 2025.*

Sans une robuste stratégie de cybersécurité mettant l'accent sur la prévention, les établissements d'enseignement risquent non seulement de subir des dommages financiers et des atteintes à leur réputation, mais également des perturbations de leur mission principale d'enseignement, de recherche et de service à la communauté.

Pour de nombreuses institutions dont les services informatiques manquent de personnel ou sont débordés, cela signifie également qu'il faut adopter des solutions de sécurité entièrement automatisées, capables de détecter les menaces et d'y répondre en temps réel, sans attendre une intervention manuelle.

Des atteintes à la sécurité qui ont des conséquences

Les cyberattaques contre les établissements d'enseignement ne sont plus des incidents isolés : elles ont des conséquences réelles et tangibles qui perturbent l'apprentissage, la recherche et la confiance.

En 2023, l'Université de Manchester a été victime d'une importante attaque de ransomware qui a ciblé des systèmes critiques soutenant la recherche dans le domaine de la santé. Les attaquants ont exfiltré des données sensibles, ce qui a donné lieu à des enquêtes réglementaires et contraint l'université à suspendre plusieurs fonctions académiques.

Aux États-Unis, l'attaque de 2022 contre le District scolaire unifié de Los Angeles, le second plus grand système scolaire public du pays, a compromis les données de plus de 400 000 élèves et membres du personnel. Cette faille de sécurité a entraîné une perturbation généralisée, un regard critique de l'opinion publique et un effort de recouvrement prolongé.

Les acteurs extérieurs sont à l'origine de

62 %

des attaques dans le secteur des services éducatifs,

avec

59 %

d'entre elles liées au crime organisé.

Source : *Verizon : Rapport de Verizon sur les fuites de données en 2025.*

Ces cas illustrent le fait que l'éducation est une cible attrayante pour les acteurs de menaces, qu'ils soient criminels ou soutenus par un État, en raison de la richesse de son environnement de données et de ses défenses qui manquent souvent de ressources.

En l'absence d'une stratégie de cybersécurité appropriée, les institutions risquent plus qu'un simple temps d'arrêt : elles s'exposent à l'érosion de la confiance du public, une responsabilité juridique et des dommages durables pour la continuité de l'enseignement.

Principales menaces pesant sur le secteur de l'éducation

Les cinq principales catégories de menaces qui affectent le plus souvent les établissements d'enseignement aujourd'hui sont énumérées ci-dessous, avec des exemples concrets et des stratégies d'atténuation ciblées.

1. Attaques d'hameçonnage et de ransomwares

Les ransomwares restent l'une des menaces les plus répandues dans le paysage des menaces, interrompant fréquemment les activités des établissements scolaires. Un membre du personnel peut être amené à cliquer sur un faux email prétendant provenir du service informatique de l'université, ce qui entraîne un vol d'identifiants qui permet ensuite un accès latéral étendu, et peut conduire à des extorsions et des demandes de rançon.

2. Appareils personnels non sécurisés et risques liés au BYOD

La culture de l'utilisation d'appareils personnels à des fins professionnelles (BYOD) dans l'éducation élargit considérablement la surface d'attaque. Les élèves apportent régulièrement des ordinateurs portables et des smartphones à l'école et se connectent au réseau Wifi du campus pour accéder aux systèmes de gestion de l'apprentissage ou remettre des travaux.

Les élèves peuvent, sans le savoir, installer une extension de navigateur ou une application malveillante qui compromet leur appareil, permettant ainsi à des pirates de s'introduire dans le réseau de l'école. Les enseignants peuvent connecter des appareils personnels pendant les cours hybrides, contournant ainsi les contrôles institutionnels et propageant involontairement des malwares. Tout cela introduit des vulnérabilités importantes, en l'absence de surveillance de la sécurité.

3. Vulnérabilités des applications cloud

La forte dépendance à l'égard des services dans le cloud tels que la messagerie, le stockage et les plateformes de collaboration a exposé les écoles à des menaces ciblant ces environnements. Les enseignants et les professeurs, ainsi que les étudiants, utilisent régulièrement des plateformes telles que Microsoft Teams ou Google Classroom pour partager des travaux, discuter de projets et collaborer en temps réel.

Lorsqu'un compte d'étudiant compromis télécharge un fichier contenant un malware dans un dossier partagé, l'infection peut se propager rapidement. De même, un compte d'administrateur non surveillé disposant de privilèges excessifs dans un tableau de bord cloud pourrait être détourné par hameçonnage, ce qui entraînerait un blocage généralisé des comptes, un vol de données et une paralysie opérationnelle.

4. Défis de protection des données et de conformité

Les universités et les écoles gèrent de grandes quantités d'informations personnelles sensibles, de données de recherche et de dossiers financiers, qui sont tous soumis à une surveillance réglementaire stricte. Les systèmes d'information sur les étudiants stockent souvent des numéros de sécurité sociale, des relevés de notes et des informations sur les aides financières.

Une atteinte à la sécurité de ces données peut non seulement entraîner une usurpation d'identité, mais également déclencher des obligations de déclaration, des audits, des amendes réglementaires et des atteintes à la réputation en vertu de lois telles que FERPA, RGPD, ou HIPAA.

58 %

de toutes les données compromises dans le secteur des services éducatifs en 2024 étaient des données personnelles.

Source : *Verizon : Rapport de Verizon sur les fuites de données en 2025.*

En outre, les universités engagées dans des recherches sensibles ou financées par le gouvernement, telles que la biotechnologie, les soins de santé ou la défense, traitent souvent des informations non classifiées contrôlées (CUI) qui doivent répondre aux normes de conformité en matière de sécurité nationale (par ex. NIST SP 800-171). Leur compromission pourrait ébranler le financement, les partenariats et la confiance des institutions.

5. Ressources informatiques limitées et pénurie de compétences

Pour remédier à ces lacunes, les mécanismes de détection et de réponse aux menaces entièrement automatisés ne sont plus facultatifs. Ils garantissent la neutralisation des menaces en temps réel sans alourdir les équipes informatiques internes, en particulier dans les environnements manquant de ressources.

En raison de pressions budgétaires et de la pénurie de personnel informatique, de nombreuses institutions s'efforcent de gérer des environnements de menaces de plus en plus complexes. Dans les petits districts scolaires, un seul administrateur informatique peut être responsable de la gestion de centaines d'appareils, de la sécurisation du réseau, de la

prise en charge des plateformes d'apprentissage virtuelles et de la mise en œuvre des politiques de sécurité, souvent sans formation formelle à la cybersécurité. Dans l'enseignement supérieur, les équipes de sécurité en sous-effectif peuvent manquer de temps ou d'outils pour surveiller les postes en permanence, analyser les journaux ou réagir rapidement aux menaces. Cette surcharge opérationnelle augmente le risque que les intrusions ne soient pas détectées avant que les dégâts ne soient déjà faits.

Tactiques, techniques et procédures utilisées contre les écoles

Ces attaques multivecteurs exigent des défenses automatisées capables de s'adapter en temps réel ; bien au-delà de ce que les processus manuels peuvent gérer. Les acteurs de menaces qui ciblent le secteur de l'éducation déploient fréquemment des ransomwares exploitant des vulnérabilités non corrigées, des attaques d'ingénierie sociale et d'hameçonnage contre le corps enseignant, le personnel et les administrateurs, ainsi que des campagnes d'hameçonnage par code QR diffusées via des prospectus physiques, des cartes de stationnement et des communications officielles du campus.

Des malwares sophistiqués conçus pour contourner les protections EDR (détection et réponse sur endpoint) sont de plus en plus souvent découverts, en particulier dans le cadre d'attaques sponsorisées par des États.

Les attaquants s'appuient également souvent sur des identifiants compromis récoltés via des attaques d'hameçonnage ou de bourrage d'identifiants pour obtenir un accès initial, puis se déplacent latéralement à travers des réseaux mal segmentés en utilisant des outils tels que Mimikatz. Les logiciels anciens et les systèmes non corrigés constituent des points d'entrée faciles à exploiter. En outre, les groupes de ransomwares pratiquent désormais couramment une double tactique d'extorsion, exfiltrant d'abord les données sensibles avant de les chiffrer afin de maximiser la pression exercée pour obtenir un paiement.

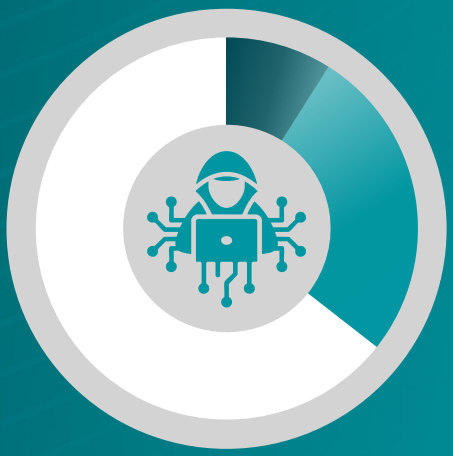
Enfin, les attaques contre la chaîne d'approvisionnement visant les fournisseurs de technologies éducatives et les prestataires de services sont une préoccupation émergente, car les compromissions en amont peuvent avoir des effets en cascade sur plusieurs institutions. Ces tactiques en constante évolution soulignent la nécessité de disposer de défenses multicouches capables de détecter et de neutraliser les menaces à plusieurs stades de la chaîne d'attaque.

À l'avenir, les établissements d'enseignement doivent se

42 %

des failles de sécurité étaient causées par des malwares ; les ransomwares étant responsables de **30 %** d'entre elles.

36 %



Les méthodes de piratage représentaient 36 % des atteintes à la sécurité, avec en tête l'utilisation d'identifiants volés (**24 %**).

29 %

Les erreurs étaient à l'origine de 29 % des failles de sécurité, principalement dues à des livraisons erronées (**17 %**).

16 %

L'ingénierie sociale, l'un des trois principaux schémas d'attaque, représentait 16 % des atteintes à la sécurité ; **77 %** d'entre elles étaient des cas d'hameçonnage et 7 % des cas de pretexting.

Source : *Verizon : Rapport de Verizon sur les fuites de données en 2025.*

Risques futurs : une bataille qui s'intensifie

préparer à une escalade de la sophistication et de l'ampleur des cybermenaces. Comme l'ont souligné de nombreux experts, l'intelligence artificielle (IA) est de plus en plus utilisée comme arme par les adversaires, permettant des leurres d'hameçonnage hyper-personnalisés et même des attaques d'ingénierie sociale utilisant des deepfakes et ciblant les services d'admission, les bureaux d'aide financière et les dirigeants d'université.

En 2024, IBM a prédit que plus de 40 % des responsables de la sécurité s'attendent à ce que les menaces s'appuyant sur l'IA fassent parti de leurs trois principaux risques organisationnels d'ici 2026. En parallèle, la prolifération des objets connectés (IdO) sur les campus élargit considérablement la surface d'attaque numérique.

Bien que ces technologies soient souvent déployées pour améliorer les environnements d'apprentissage et la sécurité des campus, elles manquent souvent de segmentation, de visibilité et de contrôles de sécurité dédiés.

Les tendances technologiques stratégiques de Gartner pour 2025 mettent l'accent sur l'essor de ce que l'on appelle l'intelligence ambiante, à savoir des systèmes qui fonctionnent discrètement en arrière-plan, se fondant dans les environnements quotidiens. Dans l'éducation, cela reflète l'adoption discrète de l'IdO sans investissement parallèle dans des cadres de gouvernance, laissant les institutions vulnérables à des points d'entrée invisibles.

En outre, les tensions géopolitiques actuelles devraient intensifier les campagnes de cyber-espionnage contre les universités, en particulier celles qui sont impliquées dans des recherches scientifiques, médicales ou de défense sensibles.

Les acteurs sponsorisés par des États considèrent l'enseignement supérieur comme une cible douce mais stratégique dans le paysage mondial des cyberconflits ; une cible qui associe des données précieuses à une surveillance généralement limitée de la cybersécurité. Se préparer, c'est prévenir et c'est sans aucun doute essentiel de nos jours.

40 %

des responsables de la sécurité s'attendent à ce que les menaces liées à l'IA constituent l'un des trois principaux risques d'ici 2026.

Source : *Tendances de cybersécurité : Prévisions d'IBM pour 2024*.

Solutions ESET pour une cyberdéfense évolutive et préventive

Les établissements d'enseignement ont besoin de solutions de cybersécurité non seulement puissantes, mais également préventives, automatisées et pratiques, qui s'adaptent aux contraintes budgétaires, aux niveaux de personnel informatique et à l'évolution rapide du paysage des menaces. La plateforme ESET PROTECT offre un écosystème unifié et évolutif qui aide les écoles et les universités à prévenir, détecter et répondre aux menaces de manière efficace.

La plateforme comprend une protection moderne et entièrement automatisée des endpoints avec un bouclier contre les ransomwares, leur remédiation, et une détection des comportements. ESET Cloud Office Security (ECOS) ajoute une couche de défense essentielle pour les applications Microsoft 365 et Google Workspace, en minimisant les risques d'hameçonnage, de compromission de la messagerie professionnelle et de partage de fichiers malveillants au sein des outils de collaboration. Il comprend également une protection antispoofing et homoglyphe, qui identifie les menaces que les filtres traditionnels ou les utilisateurs humains peuvent souvent ne pas détecter.

Le suivi des meilleures pratiques telles que les correctifs, le chiffrement et l'application des politiques peut submerger les équipes informatiques limitées. La plateforme ESET PROTECT aide en centralisant et en automatisant les tâches principales de sécurité et de gestion des technologies de l'information, y compris la gestion des vulnérabilités et des correctifs (V&PM) pour combler rapidement les lacunes connues.

ESET Secure Authentication offre une MFA simple et évolutive, aidant à surmonter les habitudes de mots de passe faibles et empêchant l'accès non autorisé aux comptes des étudiants, du personnel et des administrateurs. Des outils de chiffrement aident à respecter les mandats de conformité en vertu du RGPD, de FERPA et de HIPAA.

Pour les institutions dont les services informatiques sont débordés ou dont l'expertise interne est limitée, la solution Managed Detection and Response (MDR) d'ESET offre une protection 24x7 entièrement gérée ainsi qu'une recherche de menaces experte. Elle prend en charge le back-end technique afin que les équipes internes puissent se concentrer sur des tâches stratégiques et de grande valeur plutôt que d'être noyées dans des alertes de sécurité.

Le MDR répond directement aux défis du paysage actuel des menaces liées à l'éducation — vastes surfaces d'attaque, divers points d'entrée et campagnes ciblées persistantes — tout en offrant l'avantage d'une protection permanente à une fraction du coût de la mise en place de moyens internes. Qu'il s'agisse d'un petit district ou d'une grande université de recherche, les solutions d'ESET s'adaptent de manière intelligente et abordable à la taille de l'institution, à sa maturité et à l'évolution de ses besoins opérationnels.

SOUTENIR L'ÉDUCATION EN RENFORÇANT LA CYBERSÉCURITÉ

Un district scolaire public avec 4 800 postes Windows 10 a été confronté à des défis importants dans la protection des postes de travail contre les menaces web. Leur solution antivirus existante (datant de 2009) était inefficace pour empêcher les cyberinfections, ce qui entraînait des temps d'arrêt considérables car les ordinateurs devaient être réimagés. La solution ne disposait également pas d'une console d'administration, ce qui empêchait le contrôle global des paramètres et la détection des infections.

À la recherche d'une protection plus robuste et d'une gestion améliorée, le district scolaire central s'est tourné vers ESET. En 2009, le district a effectué une transition transparente de son ancienne solution antivirus avec l'aide de l'équipe de services professionnels d'ESET. En tant que client du secteur de l'éducation, le district apprécie la légèreté et la facilité d'utilisation d'ESET. Le district a continué à renforcer son dispositif de sécurité avec ESET au fil des ans et protège désormais 7 800 postes avec ESET PROTECT Enterprise, qui comprend le XDR et le chiffrement complet des disques

AVANTAGES CLÉS

- Déploiement transparent et configuration rapide grâce à la console d'administration centrale et à la configuration des politiques
- La solution fonctionne en arrière-plan, ce qui la rend invisible pour l'utilisateur final.
- Empreinte légère avec un impact minimal sur les performances du système
- Protection fiable sécurisant l'environnement grâce à une défense efficace contre les malwares

« ESET nous permet d'améliorer la disponibilité et la fiabilité de nos postes de travail, tout en protégeant le réseau informatique du district contre les menaces. »

TECHNICIEN RÉSEAU SENIOR

Conclusion

Alors que les cybermenaces contre l'éducation gagnent en ampleur et en sophistication, les institutions doivent accorder la priorité à la prévention plutôt qu'à la réaction. La sécurité réactive n'est plus viable à une époque où des atteintes à la sécurité peuvent se produire en quelques minutes. L'automatisation, la visibilité et les principes zero trust doivent être intégrés à chaque couche de l'infrastructure de sécurité.

Avec les outils et l'état d'esprit adéquats, en particulier des solutions entièrement automatisées et axées sur la prévention, les écoles et les universités peuvent passer de la vulnérabilité à la résilience, en protégeant à la fois leur mission et leurs actifs numériques les plus précieux.

Grâce aux solutions de cybersécurité d'ESET, complètes et adaptées à l'enseignement, l'implémentation de cette résilience devient nettement plus facile et plus efficace.

EN SAVOIR PLUS

À propos d'ESET

Défense proactive. Minimisez les risques par la prévention.

Conservez une longueur d'avance sur les cybermenaces connues et émergentes **grâce à notre approche axée sur l'IA et la prévention.** Nous combinons la puissance de l'IA et l'expertise humaine pour améliorer l'efficacité et la facilité d'utilisation de la protection.

Bénéficiez d'une protection **de haut niveau** grâce à notre Threat Intelligence interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des chercheurs reconnus.

ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie. Progress. Protected.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat intelligence de renommée mondiale

Support hyperlocal et personnalisé

eset®
Digital Security
Progress. Protected.