Livre blanc

Cybersécurité : Protéger l'éducation

S'adapter à l'ère du numérique

Romain Ravon

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

Table des matières

Introduction

À l'heure où la transformation numérique redéfinit les méthodes d'apprentissage, les établissements scolaires et universitaires jouent un rôle clé dans l'acquisition des compétences numériques. Cours en ligne, plateformes éducatives, accès à des ressources en Cloud, tableaux interactifs, visioconférences : les outils connectés sont devenus indispensables au quotidien des élèves, étudiants, enseignants et personnels administratifs. Cette digitalisation de l'enseignement offre des opportunités pédagogiques majeures… mais elle s'accompagne aussi de nouvelles vulnérabilités.

Chaque jour, les réseaux Wi-Fi des établissements accueillent des centaines, voire des milliers d'appareils personnels – ordinateurs portables, tablettes, smartphones – auxquels s'ajoutent les équipements internes comme les imprimantes, les scanners, les systèmes de gestion des notes et des absences, les caméras de surveillance ou encore les serveurs pédagogiques. Cet écosystème numérique dense et hétérogène constitue une surface d'attaque particulièrement exposée.

Or, un seul appareil compromis peut suffire à désorganiser l'ensemble d'un établissement : blocage des examens, indisponibilité des plateformes d'apprentissage, fuite de données sensibles, ou encore propagation de logiciels malveillants sur l'ensemble du réseau. Ces risques ne sont plus théoriques : les cyberattaques contre les structures éducatives se multiplient, qu'il s'agisse de ransomwares, de phishing ciblé ou d'intrusions opportunistes.

Dans ce contexte, la sécurisation des infrastructures numériques n'est plus une option, mais une priorité stratégique pour les acteurs de l'éducation. Protéger les données, garantir la continuité des cours et maintenir la confiance des usagers (élèves, parents, enseignants) sont autant d'enjeux à relever pour pérenniser la mission éducative à l'ère numérique.

Ce livre blanc propose une analyse approfondie des menaces spécifiques au secteur éducatif, et présente des solutions concrètes, adaptées aux réalités de terrain, pour renforcer la résilience des établissements face aux cybermenaces.

Ce guide vise à doter les spécialistes de la sécurité, les analystes, les responsables informatiques et les membres de la direction des outils nécessaires pour naviguer dans le monde complexe de la cybersécurité.

Chapitre 1

Les menaces spécifiques au secteur éducatif

Les attaques visant le secteur de l'éducation exploitent la diversité des systèmes connectés, le volume de données sensibles et la vulnérabilité des outils numériques utilisés quotidiennement. Voici un aperçu des principales menaces auxquelles font face les écoles et universités.

PERTURBATIONS DES COURS EN LIGNE

Quand les cours en ligne sont interrompus, c'est souvent à cause d'attaques par déni de service (DDoS) qui rendent les plateformes pédagogiques inaccessibles. Les conséquences sont immédiates : retards dans les programmes, difficultés pour les enseignants, et perte de repères pour les élèves.

VOLS DE DONNÉES PERSONNELLES

Ils représentent l'une des attaques les plus fréquentes. Les dossiers des élèves, enseignants et administrateurs contiennent des informations sensibles, telles que des identités, des adresses, ou des résultats académiques, qui peuvent être exploitées pour des fraudes ou revendues sur le marché noir.

« La violation de la vie privée des élèves et enseignants entraîne des répercussions psychologiques et légales, tandis que la suspension des cours et examens perturbe gravement la continuité pédagogique. »

EXPLOITATION DES PLATEFORMES NON SÉCURISÉES

Elle constitue une autre menace majeure. Les outils numériques éducatifs, qu'il s'agisse de plateformes d'apprentissage (LMS) ou d'applications collaboratives, peuvent servir de points d'entrée aux cybercriminels si des vulnérabilités techniques ne sont pas corrigées à temps.

Un exemple concret

En août 2024, l'université Paris-Saclay a subi une attaque par rançongiciel qui a paralysé son système informatique central. Cette intrusion a perturbé la rentrée universitaire, obligeant l'administration à recourir à des méthodes traditionnelles, telles que l'affichage et le téléphone, pour communiquer avec les étudiants et le personnel. Les inscriptions ont dû être effectuées sur support papier. La reprise complète des services numériques dans ces situations peut nécessiter plusieurs mois.

Le Monde.fr

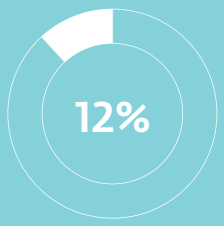
Le saviez-vous ?

En 2023,

Les établissements scolaires ont connu une **hausse de 75 %** des cyberattaques par rapport à l'année précédente.

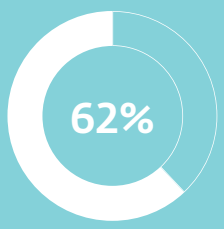
Dynamips

En 2024,



Les établissements d'enseignement supérieur représentaient **12 %** des victimes d'attaques par rançongiciel en France, égalant les entreprises stratégiques.

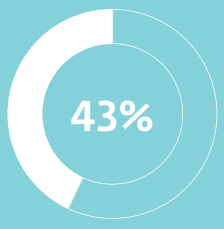
CERT-FR



62 % des établissements d'enseignement secondaire et supérieur ont payé une rançon à la suite d'une attaque par rançongiciel.

Dynamips

À noter,



43 % des cyberattaques contre les établissements scolaires via du phishing.

Dynamips

Chapitre 2

Les défis pour les établissements éducatifs

Les établissements scolaires et universitaires doivent relever des défis majeurs pour garantir leur cybersécurité. Ces défis sont particulièrement marqués par des contraintes budgétaires, la diversité des utilisateurs, et un manque de sensibilisation généralisé.

RESSOURCES LIMITÉES

Face à des priorités multiples, comme l'acquisition de matériel pédagogique ou le financement des infrastructures, la protection numérique, souvent perçue comme coûteuse, est parfois reléguée au second plan. Pourtant, des solutions accessibles et adaptées aux besoins des établissements éducatifs offrent une protection efficace à un coût maîtrisé.

DIVERSITÉ DES UTILISATEURS

Les établissements éducatifs regroupent des utilisateurs aux profils variés : élèves, enseignants, administrateurs et intervenants extérieurs. Cette diversité complique la gestion des accès et des droits. Des solutions de gestion centralisée des accès et des appareils permettent de sécuriser les réseaux tout en facilitant l'administration.

RÉSEAUX SOCIAUX

L'usage intensif des réseaux sociaux par les élèves surcharge les infrastructures Wi-Fi, perturbant les outils pédagogiques. Ces plateformes exposent également les établissements à des risques : malwares, phishing, cyberharcèlement. Sensibilisation, filtrage et outils de sécurité sont essentiels pour garantir un environnement numérique sûr.

INSOUCIANCE

Faute de sensibilisation, élèves et enseignants adoptent des comportements à risque : clics sur des liens frauduleux, mots de passe faibles, réutilisation d'identifiants. Des outils pédagogiques et des campagnes régulières peuvent renforcer la culture de la cybersécurité et réduire les risques.

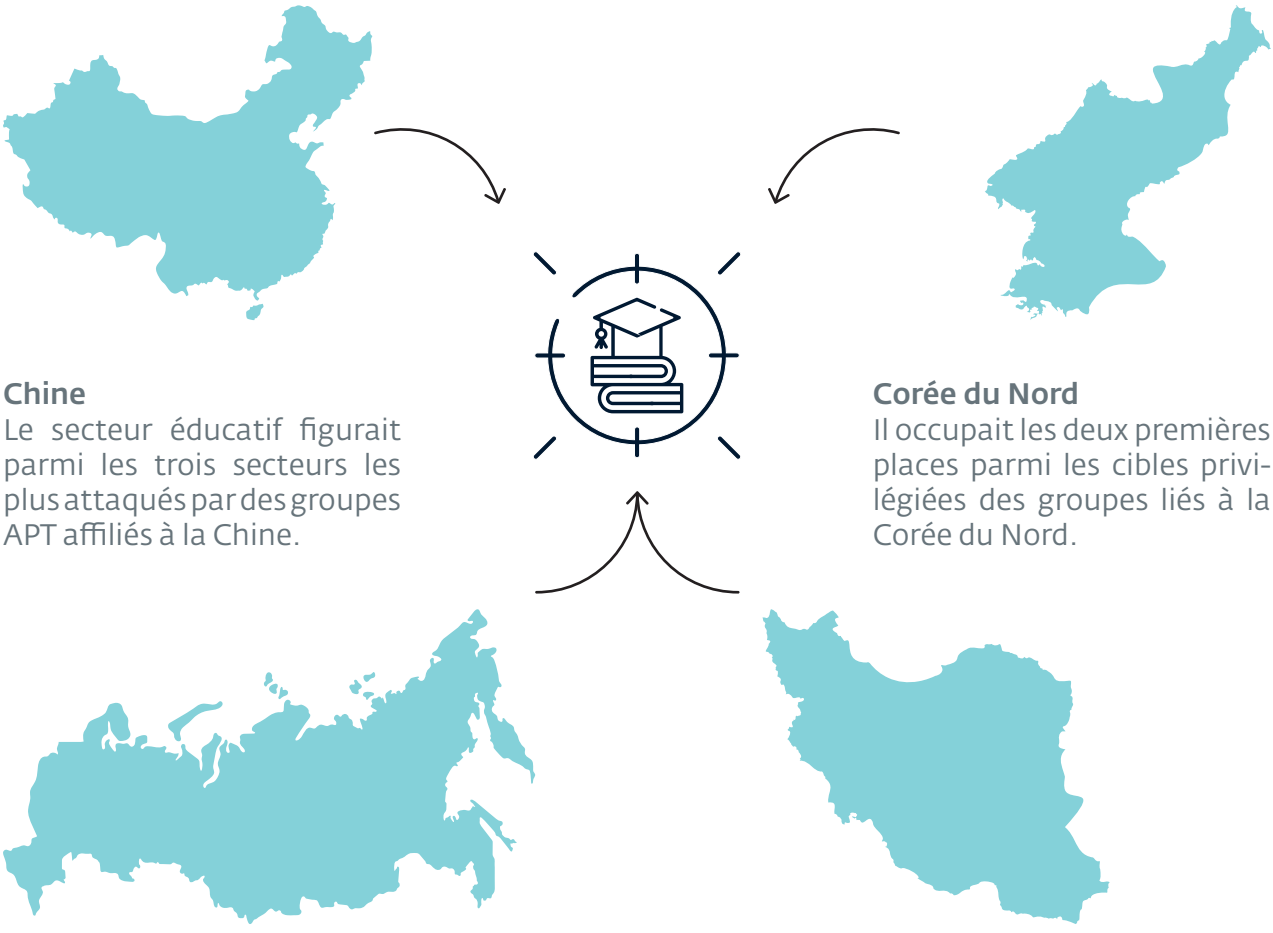
Le phishing, l'arnaque qui ne vieillit pas. Les cybercriminels misent sur la faille la plus prévisible : l'erreur humaine. Un simple e-mail promettant « un voyage scolaire de rêve » suffit à piéger sa victime.

Chapitre 3

Solutions pour sécuriser les établissements

Pour garantir un environnement numérique sûr, les établissements éducatifs doivent mettre en œuvre des mesures concrètes et adaptées à leurs besoins. Ces solutions reposent sur des politiques de sécurité claires, une protection efficace des données, l'utilisation de technologies accessibles, la sensibilisation des utilisateurs et l'appui de partenaires spécialisés.

Les chercheurs d'ESET ont remarqué une tendance préoccupante : entre avril et septembre 2024, des groupes APT (Advanced Persistent Threats) sophistiqués ont intensifié leurs attaques contre les institutions éducatives à l'échelle mondiale. Le secteur éducatif a été particulièrement ciblé par des groupes d'attaquants internationaux :



Chine
Le secteur éducatif figurait parmi les trois secteurs les plus attaqués par des groupes APT affiliés à la Chine.

Corée du Nord
Il occupait les deux premières places parmi les cibles privilégiées des groupes liés à la Corée du Nord.

Russie et Iran
Il se classait également parmi les six premiers secteurs ciblés par des acteurs associés à l'Iran et à la Russie.

PRÉVENTION

Sécuriser les infrastructures éducatives passe par une gestion stricte des droits d'accès, limités aux besoins de chaque utilisateur. Des règles claires sur le partage de fichiers, les mots de passe et l'accès aux plateformes doivent être définies et communiquées.

SENSIBILISATION

Former enseignants et élèves aux bonnes pratiques, comme l'usage de mots de passe robustes et la vigilance face aux emails frauduleux, est essentiel. Des ateliers réguliers renforcent la culture de la cybersécurité et impliquent chacun dans la protection de l'établissement.

PROTECTION DES DONNÉES

Protéger les données sensibles passe par le chiffrement des fichiers et des échanges, ainsi que par des sauvegardes régulières, sécurisées hors ligne ou sur des serveurs protégés.

TECHNOLOGIES ABORDABLES

Il existe des solutions de sécurité pour entreprises accessibles qui permettent de sécuriser les réseaux tout en bloquant les tentatives d'intrusion, avec des fonctionnalités centralisées qui simplifient la gestion et optimisent le budget.

ACCOMPAGNEMENT

Les établissements peuvent s'appuyer sur des experts en cybersécurité pour des conseils adaptés et des solutions avancées. Des services managés comme le Managed Detection & Response (MDR) offrent une protection proactive via des technologies avancées (EDR, XDR), compensant le manque de ressources internes.

Opération Cactus

En réponse à une série d'attaques malveillantes ayant ciblé les Espaces Numériques de Travail (ENT) des établissements scolaires, le ministère a lancé en mars 2025 la campagne «Opération Cactus». Cette initiative vise à sensibiliser les élèves et le personnel aux risques liés à l'hameçonnage (phishing) et à promouvoir les bonnes pratiques en matière de cybersécurité.

Ministère de l'éducation nationale

Études de cas

Plusieurs établissements éducatifs ont récemment renforcé la sécurité de leurs plateformes numériques et collaboré avec des partenaires technologiques pour améliorer leur cybersécurité.

Après avoir subi une cyberattaque par rançongiciel en août 2024, l'université a collaboré avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour identifier et corriger les failles de sécurité. Elle a également décidé de ne pas payer la rançon et a porté plainte, tout en travaillant à la restauration sécurisée de ses services numériques.

Université Paris-Saclay

Après avoir été victime d'une cyberattaque en 2023, l'université a renforcé sa sécurité informatique en mettant en place une authentification à double facteur pour l'accès aux services en ligne, en sensibilisant les étudiants et le personnel aux bonnes pratiques de cybersécurité, et en collaborant étroitement avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour auditer et améliorer ses systèmes.

Université de Rennes 1

Les universités de technologie de Compiègne, Troyes et Belfort-Montbéliard ont mutualisé leurs efforts pour créer un centre de réponse aux incidents de sécurité informatique (CERT). Ce centre permet de détecter rapidement les menaces, de coordonner les réponses aux incidents et de partager les meilleures pratiques en matière de cybersécurité entre les établissements membres.

Réseau des Universités de Technologie (UT)

L'INSA Lyon a mis en place un programme de formation obligatoire à la cybersécurité pour tous ses étudiants en première année. Ce programme couvre les fondamentaux de la sécurité informatique, les risques liés aux cyberattaques et les mesures de protection à adopter. De plus, l'institut organise régulièrement des ateliers et des conférences pour sensibiliser l'ensemble de la communauté universitaire aux enjeux de la cybersécurité.

Institut National des Sciences Appliquées (INSA) de Lyon

Collaboration avec des partenaires technologiques pour auditer et améliorer la sécurité

En 2023, un audit réalisé par les autorités éducatives françaises a identifié 500 établissements scolaires nécessitant un renforcement des dispositifs d'alerte et de sécurisation. À la suite de cet audit, 150 établissements ont déjà vu leur sécurité renforcée. Cette initiative souligne l'importance de la collaboration entre les collectivités locales et les services académiques pour assurer un environnement sûr.

Les offres ESET

Choisir ESET comme partenaire cyber

ESET est un partenaire de choix pour le secteur éducatif, offrant des solutions robustes et adaptées aux besoins des établissements. Sa cybersécurité performante garantit un environnement numérique sécurisé, tout en respectant les contraintes budgétaires.

CONÇUES POUR LES ÉTABLISSEMENTS ÉDUCATIFS

Les solutions ESET répondent aux besoins des écoles et universités, où cohabitent une multitude d'appareils connectés et d'utilisateurs aux profils variés. Qu'il s'agisse de protéger les ordinateurs, tablettes, ou plateformes éducatives, les solutions ESET offrent une approche multicouche pour prévenir les malwares, ransomwares, et autres menaces sophistiquées. Cette protection s'étend à l'ensemble du réseau, assurant une sécurité homogène pour tous.

PERFORMANCE ET LÉGÈRETÉ

Les établissements éducatifs disposent souvent de matériel informatique varié, allant des équipements récents à des appareils plus anciens. Les solutions ESET se distinguent par leur légèreté, garantissant une performance optimale même sur des configurations modestes.

SUPPORT LOCAL

ESET s'engage à accompagner les établissements éducatifs avec un support technique français accessible et réactif. Les équipes d'experts d'ESET apportent des conseils personnalisés et des formations en cybersécurité.

GESTION CENTRALISÉE

La console ESET PROTECT simplifie la gestion de la sécurité grâce à une supervision centralisée, une détection proactive des menaces et des politiques adaptées aux utilisateurs.

AVANTAGES TARIFAIRES

ESET propose des tarifs adaptés aux établissements, permettant d'accéder à des solutions avancées à coût maîtrisé, optimisant ainsi la sécurité et le budget.

Conformité réglementaire

Les solutions ESET aident les établissements à se conformer aux exigences du RGPD, en offrant des outils de chiffrement et des mécanismes de protection des données. La conformité avec les réglementations européennes, telles que la directive NIS2, renforce encore davantage la résilience des infrastructures éducatives.

Une Protection Multicouche

ESET propose une gamme de produits spécifiquement adaptés aux défis du secteur éducatif :

Protection des endpoints pour sécuriser les appareils

Chiffrement des données sensibles

Authentification Multifacteur pour renforcer les accès

Extended Detection & Response (XDR) pour la détection avancée des menaces

Managed Detection & Response (MDR) pour la gestion proactive des incidents

ESET propose des tarifs adaptés au secteur éducatif, permettant d'accéder à des solutions avancées à coût maîtrisé, optimisant ainsi la sécurité et le budget.

Conclusion

La transition numérique représente un levier puissant pour moderniser l'éducation, diversifier les méthodes d'apprentissage et renforcer l'inclusion. Toutefois, cette évolution s'accompagne d'une exposition accrue aux cybermenaces : vols de données sensibles, interruption des cours, compromission des équipements connectés ou encore exploitation des failles humaines. Ces risques ne sont pas anecdotiques : ils peuvent désorganiser durablement le fonctionnement des établissements, porter atteinte à leur réputation et nuire à la continuité pédagogique.

Face à ces enjeux, garantir un environnement numérique sécurisé n'est plus une option, mais une nécessité pour permettre aux établissements de remplir pleinement leur mission éducative. Cela passe par une combinaison de trois piliers : une cybersécurité performante capable de détecter et bloquer les menaces en temps réel, une gestion centralisée des accès et des appareils pour limiter les failles, et enfin une sensibilisation active des utilisateurs – élèves, enseignants, personnel – pour faire de chacun un acteur de la sécurité.

Conscient des contraintes budgétaires et organisationnelles du secteur éducatif, ESET propose des solutions de cybersécurité à la fois robustes, accessibles et simples à déployer. De la protection des endpoints à la détection avancée des menaces, en passant par des outils de pilotage centralisé, ESET s'engage aux côtés des écoles et universités pour construire un cadre numérique de confiance. Car protéger l'éducation, c'est aussi protéger l'avenir.

À propos d'ESET

Quand la technologie permet le **progrès**, ESET est là pour le **protéger**.

ESET, entreprise européenne de cybersécurité reconnue mondialement, se positionne comme un acteur majeur dans la protection numérique grâce à une approche technologique innovante et complète. Fondée en Europe et disposant de bureaux internationaux, ESET combine la puissance de l'intelligence artificielle et l'expertise humaine pour développer des solutions de sécurité avancées, capables de prévenir et contrer efficacement les cybermenaces émergentes, connues et inconnues.

Ses technologies, entièrement conçues dans l'UE, couvrent la protection des terminaux, du cloud et des systèmes mobiles, et se distinguent par leur robustesse, leur efficacité et leur facilité d'utilisation, offrant ainsi une défense en temps réel 24/7 aux entreprises, infrastructures critiques et utilisateurs individuels. Grâce à ses centres de recherche et développement et son réseau mondial de partenaires, ESET propose des solutions de cybersécurité intégrant un chiffrement ultra-sécurisé, une authentification multifactorielle et des renseignements approfondis sur les menaces, s'adaptant constamment à l'évolution rapide du paysage numérique.

Plus de 30 ans
d'innovation continue

1er éditeur Européen
de solutions de sécurité

Focus continu
sur la technologie

Détenu par
ses fondateurs

www.eset.com/fr