ÊTRE À LA HAUTEUR

La Technologie au Service de la Sécurité des Établissements d'Enseignement

cisco Meraki

Sommaire

INTRODUCTION

Des envrionnements d'apprentissage de plus en plus numériques

Qu'ils passent un examen de mathématiques en ligne, qu'ils fassent une présentation en cours de sciences ou qu'ils participent à une sortie scolaire virtuelle, les élèves sont toujours connectés, quel que soit leur âge. Pendant qu'ils font leurs devoirs en ligne ou visionnent en streaming des vidéos éducatives, les équipes IT des établissements d'enseignement primaire, secondaire et supérieur travaillent d'arrache-pied pour concevoir et assurer la maintenance des réseaux sous-jacents.

Alors que ces établissements intègrent toujours plus la technologie numérique dans leur méthode d'enseignement, la demande pesant sur les réseaux augmente de façon exponentielle. Les élèves sont de plus en plus nombreux à apporter leurs périphériques à l'école pour écrire leurs dissertations, préparer des présentations, effectuer des recherches, passer des examens. Or, pour ce faire, ils ont besoin d'une solution d'accès à Internet fiable. Les tableaux blancs interactifs, les cours magistraux en ligne, les applications d'amélioration de la productivité en temps réel, les plates-formes vidéo, les périphériques des

programmes de déploiement, les haut-parleurs intelligents : toutes ces technologies ont permis aux enseignants de personnaliser leurs cours, de standardiser le déroulement des examens et de renforcer la collaboration entre les élèves.

Pour prendre en charge ces initiatives, les équipes IT déploient et gèrent des réseaux filaires et sans fil toujours plus sophistiqués, sans augmenter leur budget ni leurs ressources. La multiplication des technologies dans les établissements d'enseignement entraîne une augmentation des risques pour la sécurité et des vulnérabilités. Il ne s'agit plus uniquement de préserver la sécurité du réseau, ce qui est déjà extrêmement compliqué, mais il est désormais également nécessaire de protéger les périphériques des utilisateurs et d'assurer la sécurité physique des élèves et du personnel.

Pour ce faire, il est indispensable que les écoles et les universités établissent des pratiques de sécurité complètes, notamment lorsqu'elles mettent en œuvre des environnements d'apprentissage numériques. Déployer les solutions appropriées pour protéger et sécuriser les réseaux, les terminaux et les environnements physiques est primordial afin de garantir la sécurité des écoles et des universités.

CHAPITRE 1

Un nombre de menaces qui ne cesse de croître

Même si migrer des environnements d'apprentissage classiques vers des environnements numériques améliore les résultats des élèves, cette pratique expose également à de nouvelles vulnérabilités liées à la sécurité. Des objets connectés non sécurisés aux vulnérabilités sur le réseau et menaces contre la sécurité physique des élèves et des enseignants, aucun établissement n'est épargné par ces menaces.

Nombre d'entre eux abandonnent progressivement leurs montagnes de classeurs pour stocker les bulletins scolaires, les données financières et les dossiers des étudiants. Aujourd'hui, de plus en plus de systèmes, de cours et de données sont stockés en ligne, dans le cloud ou sur site, afin d'optimiser la conservation des dossiers et de faciliter l'accès aux informations. Les dossiers des élèves contiennent des informations sensibles telles que leur date de naissance, des informations médicales et sur leurs performances et leur comportement. En migrant ces données, les établissements augmentent leur niveau d'exposition aux menaces liées à la sécurité. Ces derniers sont de plus

en plus la cible des cybercriminels qui volent des informations confidentielles, telles que des recherches, pour les revendre à des tiers, bloquent des données en exigeant une rançon ou s'adonnent au vol d'identité. Les informations et les données sensibles qu'ils conservent sont très recherchées sur le dark web. De plus, un établissement d'enseignement sur 5 ayant récemment été touché par des cyberattaques, c'est l'une des menaces les plus importantes pesant sur les écoles et les universités.[1]

De nombreux risques liés à la sécurité sont involontairement générés par les élèves et les enseignants qui connectent au réseau leurs périphériques personnels, tels que des enceintes intelligentes et des consoles de jeu. EdTech a remarqué que ces derniers apportent régulièrement des objets connectés sur les campus sans consulter l'équipe IT :

> **L'IoT se propage sur les campus comme la plupart des nouvelles technologies : les étudiants et les enseignants connectent leurs périphériques personnels au réseau sans rien demander à personne. Il suffit de se promener dans les couloirs d'une résidence universitaire ou dans la salle des professeurs pour constater que les objets connectés y sont omniprésents.[2]**

C'est notamment lorsque ces terminaux ne sont pas protégés contre les dernières vulnérabilités de sécurité que les utilisateurs non autorisés les exploitent pour infiltrer le réseau. Par exemple, en 2017, un grand fournisseur d'accès à Internet a signalé que le réseau d'une université était tombé en panne à cause d'une attaque par déni de service distribué (DDoS) au cours de laquelle 5 000 systèmes et objets connectés envoyaient des requêtes à ses serveurs DNS toutes les 15 minutes.[3]

Par ailleurs, les cybercriminels savent que les réseaux des établissements d'enseignement sont des cibles faciles. De nombreux campus universitaires et administrations locales sont équipés de périphériques réseau obsolètes, leur budget dédié à l'achat de nouveaux points d'accès sans fil, commutateurs et appliances de sécurité étant limité. De plus, leur équipe IT est souvent surmenée et dispose de ressources limitées, ce qui complique le remplacement

---

1 https://www.telegraph.co.uk/education/2018/03/17/cyber-attacks-one-biggest-threats-schools-face-experts-warn
2 https://edtechmagazine.com/higher/article/2017/04/keep-your-campus-both-smart-and-secure-iot-expands
3 http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf

des réseaux. Toutefois, même avec une nouvelle infrastructure de réseau, il est extrêmement difficile d'assurer la mise à jour des micrologiciels, car de nombreux systèmes doivent être reconfigurés manuellement. Il est difficile de les gérer et de les mettre à jour d'un coup. Les établissements d'enseignement font donc face à des risques accrus de failles de cybersécurité.

Curieusement, ce sont les erreurs humaines qui sont l'une des principales causes des incidents. Certains enseignants et étudiants sont victimes de phishing via leur messagerie, et ainsi divulguent involontairement leurs informations d'identification ou téléchargent accidentellement un malware. Ces e-mails semblent parfois provenir de dirigeants de l'université et demandent des données financières privées des étudiants en échange d'aides ou d'activités scolaires supplémentaires.

En outre, l'équipe IT ne doit plus uniquement se limiter au réseau pour protéger les campus. En raison des progrès technologiques, il lui incombe d'assurer également la gestion et la maintenance des systèmes destinés à réduire les menaces physiques. Même si la sécurité des étudiants et du personnel est une priorité, il n'est pas simple de déployer et de maintenir des solutions qui facilitent la collaboration des équipes IT et responsable de la sécurité et qui renforcent la sécurité. Une seule université compte des résidences universitaires, des cafétérias, des bibliothèques, des installations sportives, des salles de conférence et bien plus encore, sans oublier les parents qui rendent visite aux étudiants et les invités qui se promènent sur le campus à toute heure. En raison de ces nombreuses variables, il est difficile de prévoir les incidents liés à la sécurité physique et de les réduire. En outre, comme les menaces physiques continuent à proliférer dans les établissements scolaires, une technologie adaptée aide la direction à réagir, à prendre des mesures et à empêcher ces événements de se reproduire.

Même s'il peut sembler ambitieux de chercher à relever tous ces défis liés à la sécurité en même temps, il y a trois domaines sur lesquels il convient de se concentrer pour renforcer la sécurité des environnements d'apprentissage. En évaluant les stratégies et les solutions pour la sécurité des terminaux, du réseau et de la couche physique, les équipes IT et les directeurs d'établissements scolaires créent des lieux où les élèves peuvent se concentrer sur leur apprentissage et les professeurs sur l'enseignement.

CHAPITRE 2

Protéger l'ensemble des terminaux dans un établissement

Pour renforcer la sécurité, il est crucial de commencer par protéger les périphériques de l'établissement, des étudiants et du personnel. Avec la multiplication des ordinateurs, des tablettes et des objets connectés dans les salles de classe, les bibliothèques, les laboratoires et les résidences universitaires, il est extrêmement important de s'assurer que ces terminaux ont accès au réseau en toute sécurité et sont dotés des dernières mises à jour de sécurité. De plus en plus d'écoles primaires mettent en œuvre le BYOD ou des programmes de déploiement auprès des élèves, c'est pourquoi les départements IT doivent surveiller un nombre de terminaux toujours plus important et qui augmente à un rythme inédit.

Une solution de gestion des terminaux visant à protéger les périphériques appartenant à l'établissement s'avère utile de bien des manières. En gérant tous les périphériques via un seul système, les administrateurs IT peuvent déployer des correctifs de sécurité sur des centaines ou des milliers d'équipements en quelques minutes et ainsi assurer la mise à jour des

terminaux appartenant à l'établissement. Cette solution permet également, par exemple, de protéger les tablettes utilisées pour traiter les paiements contre les dernières menaces. La plupart des attaques ciblent les terminaux et de nombreuses failles actuelles exploitent des menaces ou des vulnérabilités déjà connues pour lesquelles un correctif a été publié.[4]

Conformément à sa philosophie selon laquelle on apprend non pas pour l'école, mais pour la vie, l'établissement indépendant Oswestry a décidé d'autoriser ses étudiants à utiliser des terminaux mobiles pendant les cours. Ne comptant qu'un seul technicien IT en interne, il a mis en œuvre des solutions Wi-Fi et cloud de gestion des terminaux, qui lui permettent de connecter simultanément plus de 400 clients au réseau sans fil, sans abandonner aucune instance ni provoquer de panne du réseau.

Les solutions de gestion des terminaux permettent également de suivre les équipements perdus ou d'effacer à distance les terminaux volés pour s'assurer que les données sensibles de l'établissement ne tombent pas entre de mauvaises mains. Grâce à un système qui propose le géorepérage, les équipes IT définissent les limites géographiques que des périphériques spécifiques ne doivent pas dépasser et programment le déclenchement d'une alerte si l'un d'eux quitte la zone désignée.

Avec plus de 270 écoles et plus de 200000 étudiants, un grand district scolaire canadien avait besoin d'un moyen de gérer et sécuriser 26000 iPads et 900 téléphones.

Pour mieux protéger les élèves qui utilisent leurs périphériques à l'école, les équipes IT implémentent des politiques de pare-feu et des mesures de filtrage du contenu pour bloquer le matériel inapproprié et potentiellement dangereux, et empêcher l'accès aux sites sur liste noire. Les élèves utilisent très souvent des applications de partage de fichiers peer-to-peer et des sites de jeu en ligne, qui peuvent renfermer des contenus illicites et des malwares dangereux non seulement pour leurs terminaux, mais aussi pour tout le réseau. Appliquer des mesures de sécurité aux terminaux assure également une protection contre les menaces liées au phishing. Avant que l'utilisateur clique sur un lien, le périphérique reconnaît le contenu malveillant, bloque le lien et envoie une alerte à l'utilisateur.

4 https://www.bankinfosecurity.com/blogs/do-you-have-dark-endpoint-problem-p-2576

Pour empêcher les menaces potentielles de s'infiltrer dans le réseau du campus, les équipes IT peuvent également créer des réseaux distincts : un pour les équipements fiables appartenant à l'établissement et un autre pour les équipements BYOD. Les objets connectés apportés par les étudiants n'étant pas tous dotés des derniers correctifs, isoler les équipements de l'établissement de ceux appartenant aux étudiants permet de protéger le réseau interne. De plus, en bénéficiant d'une meilleure visibilité sur ce qui se passe sur le réseau, les équipes IT peuvent rapidement identifier les terminaux non autorisés et les éteindre ou les bloquer si nécessaire. En outre, les terminaux connectés à l'IoT et autres équipements connectés doivent être évalués pour vérifier que leurs mesures de sécurité sont à jour. Par exemple, beaucoup d'établissements utilisent encore des caméras de sécurité obsolètes, points d'entrée potentiels d'attaques contre le réseau.

En assurant la mise à jour et la protection des terminaux, en isolant les réseaux pour le BYOD et en bloquant les contenus préjudiciables, les directeurs d'établissements d'enseignement mettent en place une première ligne de défense contre les menaces les plus fréquentes.

CHAPITRE 3

Protéger le réseau, de l'armoire jusqu'à la salle de classe

Quelle que soit leur taille, les établissements d'enseignement sont régulièrement la cible des cybercriminels. Ces hackers peuvent non seulement accéder aux données privées des élèves, mais également endommager ou détruire tout un système informatique ou un réseau, un risque majeur pour l'université ou l'école visée. Par conséquent, même s'il est crucial d'assurer une protection contre les menaces à la périphérie du réseau, les problèmes liés à la sécurité tels que les malwares, les ransomwares et les périphériques non autorisés sont mieux traités au niveau du réseau.[5]

Pour éliminer les menaces qui pèsent sur le réseau, les équipes IT peuvent créer des politiques de groupe ou d'utilisateur selon différents critères, tels que le rôle de l'utilisateur ou le département universitaire. Les étudiants qui se rendent dans le laboratoire de recherche se voient attribuer une politique,

5 https://cosn.org/sites/default/files/Top%205%20Cybersecurity%20Threats.pdf

tandis que les enseignants assistants et les professeurs qui travaillent dans le laboratoire à temps plein sont soumis à une autre politique. Ainsi, il est possible d'établir une liste de règles et de restrictions que les périphériques doivent respecter en fonction de leur type, de leur client, de leur SSID ou de leur VLAN. Selon les politiques de groupe appliquées, les équipes IT peuvent définir des règles de pare-feu de couche 3, des règles de pare-feu de couche 7, le filtrage du contenu, des règles de régulation du trafic, etc., pour que les utilisateurs n'aient accès qu'aux autorisations et aux données dont ils ont besoin sur le réseau.

Alors que de nouveaux malwares font leur apparition chaque jour, plusieurs solutions existent pour se protéger contre les cyberattaques. Les pare-feu de nouvelle génération proposent des fonctions telles que des services de prévention et de détection des intrusions (IDS/IPS) pour identifier le trafic malveillant de manière proactive et le bloquer avant qu'il pénètre dans le réseau. Même si un élève ou un membre du personnel télécharge accidentellement un fichier qui ne déclenche pas d'alerte initiale, la solution de protection avancée contre les malwares continue de surveiller et d'analyser les fichiers pour repérer les comportements malveillants de manière rétroactive, en fonction des comportements similaires détectés.

Dès qu'une cyberattaque se produit, il est rappelé aux administrateurs IT l'importance d'appliquer les correctifs pour protéger les réseaux contre les vulnérabilités. Or, la mise à jour manuelle de l'infrastructure de réseau sur site et l'application individuelle des correctifs aux systèmes IPS prend énormément de temps aux équipes IT et peut potentiellement mener à des erreurs de configuration. Grâce à une solution gérée dans le cloud, les mises à jour du micrologiciel sont lancées automatiquement pour se prémunir contre les dernières menaces pour la sécurité. Les solutions de prévention des intrusions, quant à elles, sont mises à jour quotidiennement pour une protection contre les nouvelles vulnérabilités. Les correctifs sont donc appliqués plus rapidement sur les réseaux qui sont ainsi mieux protégés. De nombreux établissements d'enseignement procèdent encore à la mise à jour manuelle du micrologiciel de leur réseau, un processus qui peut prendre plusieurs semaines. En utilisant une solution avancée gérée dans le cloud, ils pourraient facilement planifier à distance l'application des mises à jour du micrologiciel pendant la nuit ou le week-end, afin d'assurer la protection de tout le réseau en une seule fois.

[6]Les hackers peuvent aussi accéder aux données financières et personnelles des

6 https://meraki.cisco.com/customers/higher-education/illinois-college

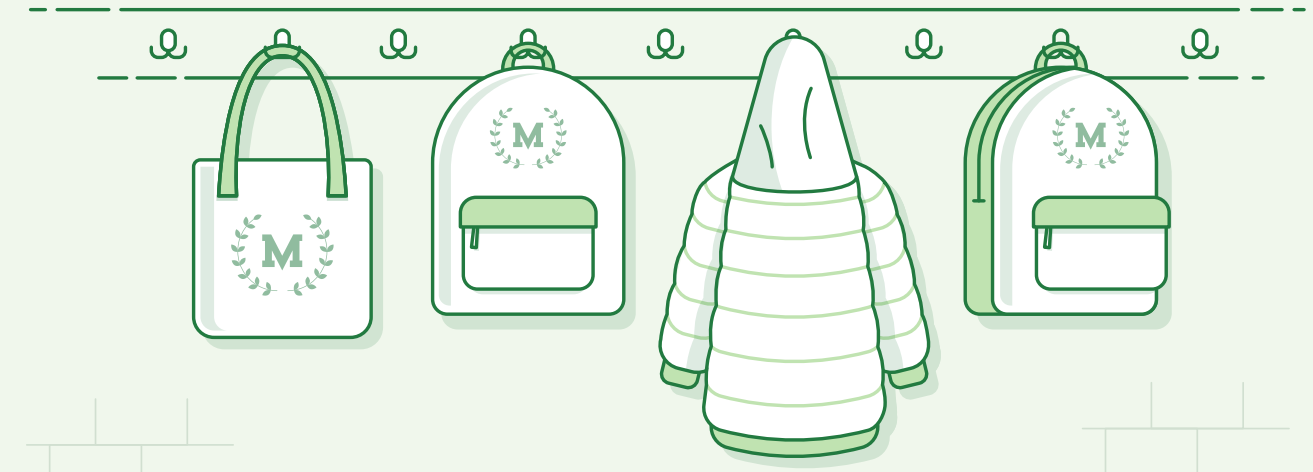
étudiants via un point d'accès et une usurpation du SSID. Toute personne qui achète un point d'accès et copie le nom du SSID principal du campus peut tromper les étudiants et les diriger vers un faux réseau. Dans les résidences universitaires en particulier, les équipes IT s'inquiètent souvent du nombre de routeurs personnels branchés par les étudiants à l'infrastructure filaire, exposant le LAN à des risques majeurs. Les technologies avancées pour la sécurité du réseau intégrées sur certains points d'accès détectent et arrêtent automatiquement les périphériques non autorisés, les SSID et les inondations de paquets à l'aide d'un module radio d'analyse dédié.

Quel que soit le nombre de mesures de sécurité implémentées par les équipes IT, il est également important de tenir compte du délai de réponse en cas d'incident sur le réseau. De nombreux systèmes réseau obsolètes n'offrent pas une visibilité suffisante sur ce qui se passe sur le réseau. Ainsi, il arrive que des incidents se produisent sans que le département IT le remarque. Le niveau de visibilité a une incidence majeure sur le délai de résolution d'un incident et sur l'importance des dommages en résultant. Les équipements réseau modernes fournissent aux équipes IT des rapports de sécurité réguliers facilement exploitables leur permettant de savoir d'où proviennent les attaques, quels clients sont concernés et comment résoudre le problème, sans devoir déchiffrer des journaux complexes. Les responsables IT peuvent également configurer des notifications automatiques par e-mail pour signaler les problèmes et neutraliser rapidement une menace dès qu'elle survient.

Le niveau de visibilité a une incidence majeure sur le délai de résolution d'un incident et sur l'importance des dommages en résultant.

Toutefois, même s'il est crucial de mettre en place les mesures de sécurité nécessaires pour garantir la sécurité du réseau, il est tout aussi important de s'assurer que les élèves et le personnel savent comment identifier les menaces et y répondre. Pour ce faire, il convient d'organiser des formations lors desquelles les étudiants apprennent à configurer des mots de passe sécurisés, à détecter les e-mails de phishing et à ne pas cliquer sur des liens suspects. Certains départements IT envoient même de fausses tentatives de phishing aux étudiants pour tester leurs connaissances et rappeler à ceux qui ont cliqué dessus les bonnes pratiques en matière d'utilisation de la messagerie.[7]

7 http://www.govtech.com/education/papers/Protecting-Students-and-Their-Data-108087.html



CHAPITRE 4

Protéger un établissement d'enseignement dans son ensemble, des couloirs aux terrains de sport

L'avènement de la technologie numérique non seulement transforme les lieux d'apprentissage, mais a aussi un impact considérable sur la sécurité dans les établissements. Les équipes IT sont de plus en plus souvent chargées de déployer et de gérer de nouvelles solutions de sécurité physique toujours plus exigeantes sur un plan technique, soit de manière indépendante, soit en partenariat avec les équipes responsables de la sécurité de l'établissement ou du campus. C'est notamment le cas lorsque ces nouvelles solutions de sécurité, notamment le contrôle d'accès par badge, les systèmes de gestion des visiteurs, les systèmes de notification groupée et les caméras de sécurité, sont conçues pour se connecter au réseau principal de l'établissement.

Même si plusieurs mesures permettent aujourd'hui de protéger les étudiants et le personnel, une technologie cruciale a récemment été mise à niveau : les caméras de sécurité. Les avancées technologiques dans ce domaine sont en train de révolutionner la réputation de la vidéosurveillance chez les leaders du secteur de l'éducation. Grâce à des caméras de sécurité plus intelligentes, les

équipes IT profitent de nombreux bénéfices et de nombreuses fonctionnalités pour mieux protéger les élèves et les enseignants, notamment une accélération des déploiements, une plus grande évolutivité, des délais de réponse plus courts et des analyses avancées.

Grâce aux fonctionnalités de recherche de mouvement, les utilisateurs peuvent identifier les personnes, les objets et les lieux concernés, ce qui permet aux équipes IT et responsable de la sécurité d'intervenir facilement, de gérer des situations stressantes et de résoudre rapidement les conflits.

À mesure que les campus s'étendent et que des bâtiments sont construits ou rénovés, il est primordial d'utiliser des caméras de sécurité flexibles et évolutives pour assurer une couverture continue dans tous l'établissement. Les caméras de sécurité IP ou analogiques classiques sont, en général, difficiles à installer, car elles doivent se connecter à un serveur sur site. De plus, si plusieurs caméras sont branchées sur un enregistreur vidéo sur réseau (NVR) ou sur un enregistreur vidéo numérique (DVR), lorsqu'une caméra tombe en panne, il arrive que toutes les caméras s'arrêtent sans que le département IT le remarque. Si des zones du campus ne sont pas protégées en raison de difficultés d'installation ou de pannes des caméras, la sécurité de l'établissement risque d'en souffrir. En revanche, en mettant en œuvre un système qui stocke les vidéos au niveau de la caméra, les établissements accélèrent le déploiement et ils sont sûrs de filmer les scènes importantes. Un incident s'est produit dans les dortoirs de l'université d'Ashland, mais le système de sécurité analogique n'a pas permis d'identifier le coupable. Les équipes IT et responsable de la sécurité savaient qu'elles devaient rapidement mettre à niveau leur solution de sécurité. Elles ont donc déployé une solution gérée dans le cloud, permettant de stocker la vidéo au niveau de la caméra. Elles ont ainsi mis à niveau et déployé plus de 150 caméras intérieures et extérieures sur le campus en quelques mois.

Il est important de pouvoir identifier facilement les incidents dès qu'ils se produisent ou de visionner rapidement les images d'événements spécifiques. Pourtant, c'est un souci majeur pour les établissements d'enseignement, qui disposent de systèmes vidéo de mauvaise qualité et doivent analyser les images manuellement, ou se rendre sur site et exécuter un logiciel spécialisé. Après avoir déployé des caméras de sécurité gérées dans le cloud, l'université d'Ashland a utilisé les fonctions de recherche de mouvement et de recherche par heure des caméras pour identifier, en quelques minutes, l'étudiant qui a vandalisé un dortoir. L'équipe de sécurité peut visionner les vidéos où qu'elle se

trouve ; les étudiants se sentent donc toujours protégés. Grâce aux fonctionnalités de recherche de mouvement, les utilisateurs peuvent identifier les personnes, les objets et les lieux concernés, ce qui permet aux équipes IT et responsable de la sécurité d'intervenir facilement, de gérer des situations stressantes et de résoudre rapidement les conflits.

Les établissements d'enseignement accueillant des milliers d'étudiants chaque jour, il peut être fastidieux de trouver des moyens efficaces d'exploiter et d'analyser les images des caméras. Toutefois, les nouvelles caméras étant équipées des mêmes processeurs que les smartphones, des méthodes d'analytique avancée permettent d'exploiter les images collectées pour protéger les étudiants. Grâce à la technologie de détection de personnes, les équipes IT et responsable de la sécurité savent combien de personnes entrent dans le champ à un moment donné et ainsi détectent facilement des tendances et des anomalies en matière de trafic et de comportements. Par exemple, le département IT détecte qui entre sur le campus, quand des étudiants circulent dans les couloirs pendant les heures de classe et où les étudiants se réunissent en dehors des heures de classe, puis apporte les ajustements nécessaires. Les équipes IT peuvent planifier des alertes par e-mail lorsqu'une personne entre dans le champ à une heure spécifique et réagir en conséquence.

Outre ces fonctionnalités puissantes, des intégrations et des options de personnalisation uniques contribuent à créer des solutions de sécurité complètes. En connectant des systèmes de notification groupée, des applications d'identification par badge, des programmes d'alerte d'urgence, des voyants et d'autres périphériques équipés de fonctions d'analyse des caméras de sécurité, les établissements d'enseignement améliorent les alertes et les réponses, et automatisent leurs processus, ce qui était impossible auparavant. Par exemple, en cas d'incendie dans un bâtiment, les caméras de sécurité signalent aux équipes d'intervention si des personnes sont détectées dans certaines pièces pour les aider à cibler leurs efforts. Ou si un étudiant retourne à sa voiture seul la nuit, la caméra de sécurité déclenche l'allumage des lumières du parking pour qu'il soit plus en sécurité.

Pour mieux protéger les étudiants dans les établissements, il est indispensable que les équipes de direction déploient des technologies modernes. En investissant dans des solutions de sécurité physique appropriées, le département IT consacre moins de temps à la maintenance et au dépannage de la technologie et peut ainsi se concentrer sur la réduction du nombre d'incidents sur le campus.

CONCLUSION

Protéger les étudiants avec la sécurité des données de bout en bout

Les technologies numériques transforment rapidement le secteur de l'éducation. Il y a quelques dizaines d'années, les salles de classe commençaient tout juste à être équipées d'ordinateurs. Aujourd'hui, de plus en plus d'établissements scolaires fournissent des terminaux, comme des iPad et des Chromebook à leurs élèves dans le cadre de programmes de déploiement. Autrefois, la sécurité du réseau se limitait à bloquer l'accès aux sites inappropriés.[8] Maintenant, elle consiste aussi à protéger d'énormes quantités de données stockées numériquement à l'aide de pare-feu sophistiqués. Auparavant , les établissements utilisaient des journaux papier pour consigner l'arrivée et le départ des invités dans un bâtiment ou sur un campus. Aujourd'hui, nombre d'entre eux les inscrivent numériquement et provisionnent automatiquement des badges d'accès qui déterminent les lieux où ils sont autorisés à se rendre.

---

8 https://searchnetworking.techtarget.com/feature/How-the-basics-of-network-security-have-evolved

Les équipes IT reconnaissent rapidement que la technologie a non seulement un impact considérable sur les résultats des élèves, mais qu'elle a également un impact majeur sur les problématiques liées à la sécurité. À bien des égards, les menaces auxquelles les établissements doivent faire face évoluent beaucoup plus rapidement que leurs ressources financières et humaines. C'est pourquoi les écoles et les universités doivent déployer des technologies faciles à gérer, capables d'évoluer efficacement pour les protéger contre les dernières menaces liées à la sécurité.

En offrant une combinaison parfaite de terminaux, de solutions pour le réseau et de solutions de sécurité physique, Cisco Meraki renforce la sécurité des établissements d'enseignement primaire, secondaire et supérieur. Les solutions de sécurité complètes Meraki, notamment les points d'accès, la gestion des terminaux, les appliances de sécurité et les caméras de sécurité, fonctionnent ensemble en toute transparence pour assurer la sécurité des établissements d'enseignement. Grâce à Meraki, les équipes IT détectent et bloquent un large éventail de menaces, telles que les périphériques non autorisés, les malwares, le phishing et les virus, tout en réduisant les coûts d'exploitation, en simplifiant les déploiements multisites et en optimisant l'utilisation de la bande passante afin d'améliorer les performances sans sacrifier la sécurité ou la confidentialité des données. Les caméras de sécurité MV Meraki aident les départements IT à assurer la sécurité physique des élèves sur tout le campus. Elles sont faciles à déployer et à gérer, et fournissent des analyses poussées pour mieux prévenir, résoudre et éliminer les incidents dans les établissements d'enseignement.

Tous les produits Meraki sont intégralement gérés via un tableau de bord intuitif en ligne et sont mis à jour automatiquement via le cloud, pour un plus grand niveau d'évolutivité et de contrôle pour s'adapter aux nouvelles problématiques liées à la sécurité.

cisco Meraki