jamf

LIVRE BLANC

Protéger l'enseignement supérieur des violations de données coûteuses

Les failles de sécurité font la une des quotidiens et des journaux télévisés

Quand une faille touche un grand nom du commerce de détail, de la santé ou de la finance, la presse et les journaux télévisés en font leur une. Et comment les médias savent-ils que les failles de sécurité suscitent un tel intérêt chez leur public ? Parce que tout le monde a peur d'apprendre que son numéro de sécurité sociale, ses comptes bancaires ou d'autres informations personnelles ont été dérobés par des pirates. Et les établissements d'enseignement supérieur ne font pas exception à la règle.

Dans l'enseignement supérieur, les étudiants et leurs familles ont besoin d'avoir pleinement confiance dans la réputation de leur établissement. Celui-ci devient souvent un aspect de l'identité des élèves et joue un rôle décisif pour la suite de leur carrière. La confidentialité et la sécurité des données sont le reflet de la confiance et de la responsabilité d'une institution, au-delà de sa mission et de ses activités universitaires, sportives et artistiques.

Qu'est-ce qu'une violation de données ?
Une violation est un événement au cours duquel les données sensibles, protégées ou confidentielles d'une personne sont consultées, volées ou utilisées sans son consentement.

Face aux énormes volumes d'informations à destination des étudiants et des enseignants, à la complexité des systèmes d'information et aux environnements distribués dans plusieurs départements, les établissements d'enseignement supérieur sont victimes des mêmes failles que les grandes entreprises, et à la même fréquence. Selon une **étude de l'Institut Ponemon**, le coût total moyen d'une violation de données est de 3,92 millions de dollars. Mais pour les établissements d'enseignement, le coût moyen est de 4,77 millions de dollars, avec un coût moyen par dossier perdu ou volé de plus de 150 dollars. Avec de tels montants, la moindre violation prend des allures de scénario catastrophe pour les présidents d'université et les équipes informatiques des facultés.

Pour lutter contre le risque de failles, et éviter les coûts associés, les services informatiques ont trop souvent le réflexe de verrouiller les droits d'accès et d'installation sur leurs appareils. Ce niveau de contrôle peut entraîner des frictions entre le service informatique et les utilisateurs universitaires et administratifs, qui ont évidemment besoin d'applications, de services et de ressources pour travailler. Quand ils ont l'impression que leur productivité est bridée par le service informatique, ils ont instinctivement le réflexe de contourner les règles pour faire avancer les projets et offrir la meilleure expérience d'apprentissage à leurs élèves. Sans le vouloir, et malgré leurs intentions louables, ces utilisateurs créent des vulnérabilités dans les systèmes de sécurité informatique. La réussite de la gestion de la sécurité informatique repose sur l'équilibre précaire entre l'autonomie des utilisateurs e t des contrôles informatiques bien dosés.

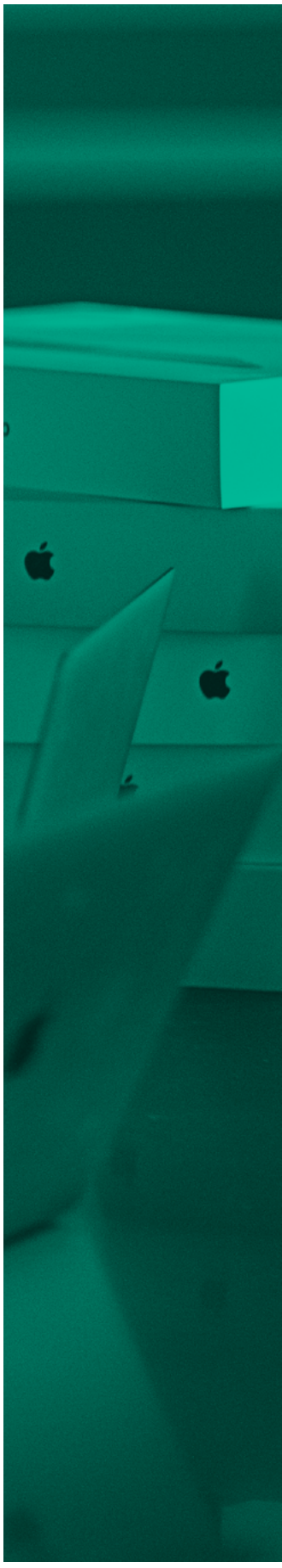
Types courants de violations de données

Les violations varient considérablement, mais on peut les classer en trois catégories : les attaques malveillantes ou criminelles, les défaillances des systèmes et les erreurs humaines. Selon une étude récente, les attaques malveillantes représentent 51 % des failles. Sans être aussi fréquents, les dysfonctionnements du système et les erreurs humaines présentent un danger tout aussi grand : bien souvent, ils passent longtemps inaperçus. Le problème tend alors à s'envenimer et à exposer davantage d'appareils et de données à des pratiques dangereuses. La même étude Ponemon note qu'il faut en moyenne 181 jours pour identifier une violation causée par une erreur humaine et 61 jours pour la contenir. Autrement, une éternité – qui laisse la porte ouverte au vol de données.

Les institutions et les universités dans le viseur

Si tous les établissments du supérieur peuvent être victimes de violations, ceux qui accueillent des doctorats et des masters sont les plus vulnérables. Selon un rapport de la Commission de régulation postale (CRP), 63 % des violations ciblaient des établissements de doctorat et 21 %, des institution de niveau master. Ces institutions sont plus sensibles parce qu'elles abritent de vastes quantités de documents et de données de recherche.

Ces chiffres impressionnants ne doivent pas laisser penser que les écoles de niveau licence soient à l'abri des vulnérabilités. Comme plusieurs peuvent en témoigner, les conséquences d'une violation sont douloureuses, coûteuses, longue et pénibles.



Le 8 juillet 2015, l'Université de l'État de Washington a observé des activités suspectes sur ses systèmes. Elle a fait appel à des experts en sécurité informatique et aux forces de l'ordre fédérales, qui ont établi qu'un adversaire sophistiqué avait accédé illégalement à ses systèmes d'e-mails et d'annuaires.

L'université du Southern New Hampshire a également été victime d'une violation de sa base de données : ce sont 140 000 dossiers d'étudiants et de classes qui ont été exposés au public. Quant à l'Université d'État de l'Arkansas, elle a révélé que 50 000 personnes avaient été touchées lors de la violation de données survenue en 2014.

Comment les violations de données entrent à l'université

Logiciels malveillants et virus

Les logiciels malveillants et les virus s'introduisent dans les systèmes d'une université de façon délibérée ou accidentelle. Mais dans tous les cas, une fois dans le système d'une université, ils passent à l'action : ils suppriment des fichiers et dérobent des mots de passe, des comptes bancaires et d'autres informations sensibles. Ils peuvent cibler des appareils qui auraient dû être mis à jour, reconfigurés ou corrigés. Ces opérations peuvent d'ailleurs se faire à distance et être automatisées, sans aucune intervention physique du service informatique.

Dangers liés aux logiciels et aux applications

À l'instar des logiciels malveillants et des virus, les logiciels et applications non sécurisés qui sont installés sur des systèmes ou des appareils peuvent faciliter la fuite d'informations personnelles ou provoquer de graves pannes matérielles.

Téléchargements de services personnalisés

Tous les enseignants et les employés d'une université utilisent un compte e-mail personnel et des services comme Dropbox sur leurs appareils. Si Dropbox n'est pas nuisible en soi, les services personnels utilisés en dehors du contrôle de l'université peuvent servir de vecteurs à des violations de données. Les attaques ciblant ces services non protégés passent souvent inaperçues parce que l'équipe informatique n'est pas au courant de leur présence sur les appareils de l'établissement.

Réseaux dangereux

Les employés sont plus mobiles que jamais, et il arrive souvent que des utilisateurs se connectent au réseau de leur université chez eux ou dans un café. S'ils n'utilisent pas le réseau privé virtuel (VPN) sécurisé de l'université, ils peuvent, par inadvertance, ouvrir des vulnérabilités dans le réseau.

Appareils non chiffrés

Le corps enseignant et le personnel ne sont pas à l'abri d'une erreur – n'importe qui peut oublier son appareil ou une clé USB sur le campus ou en dehors. Un appareil perdu ou volé est une cible de choix pour les violations de données. Face à ces cinq vulnérabilités, on peut être tenté de verrouiller les accès et d'interdire l'installation de logiciels inconnus. Mais, nous l'avons vu, cette ligne de conduite peut avoir des conséquences inattendues.

Travailler avec les enseignants et le personnel pour rester en sécurité

Afin d'offrir la meilleure expérience possible aux utilisateurs, tout en veillant à ce que leur travail et leurs recherches n'affaiblissent pas les défenses de l'université, le service informatique doit suivre plusieurs lignes directrices pour les mettre à l'abri.

Faire de la protection des terminaux la norme pour lutter contre les logiciels malveillants et les virus.

Il n'existe pas de défense parfaite contre les logiciels malveillants et les virus. En revanche, un bon système de protection des terminaux peut réduire considérablement le risque d'infection et fournir à l'équipe informatique les outils nécessaires pour réagir en cas de faille. Choisissez la bonne combinaison de technologies pour surveiller le trafic réseau et détecter les anomalies au niveau des appareils.
Pour maximiser la couverture, pensez à étendre la protection des terminaux à tous les appareils, qu'ils appartiennent ou non à l'institution. Un outil de gestion des appareils mobiles (MDM), capable d'installer un logiciel sur un appareil géré, vous simplifiera considérablement la tâche.

Mettez des logiciels et des applications fiables à disposition

Le service informatique peut créer un catalogue d'applications interne réunissant des logiciels et des réglages approuvés par l'université : enseignants et employés pourront librement télécharger tous les outils dont ils ont besoin. Les applications proposées ont toutes été testées et approuvées ; les utilisateurs n'ont plus besoin de contourner le service informatique, car ils accèdent facilement aux ressources utiles.
Si un enseignant a besoin d'une application qui n'est pas disponible dans le catalogue en libre-service, il lui suffit d'en faire la demande au service informatique. Une fois l'application évaluée et configurée selon les normes de l'université, elle est intégrée au catalogue et librement téléchargeable.

Connaître l'état des appareils et des logiciels

Grâce aux fonctionnalités d'inventaire de la MDM, le service informatique sait quelles applications sont utilisées et peut tester les applications les plus populaires. Si une application devient suspecte, il sait aussi qui l'a installée, et peut la mettre à jour ou la supprimer immédiatement. Résultat : l'appareil est protégé, et le logiciel non fiable ne peut pas se propager dans le système de l'université.

Qu'est-ce que la MDM ?

La MDM est le cadre mis en place par Apple pour gérer les appareils. Du déploiement et de l'inventaire des nouveaux appareils à la configuration des réglages, en passant par la gestion des applications ou l'effacement des données, MDM propose un ensemble complet d'outils pour prendre en charge les déploiements de grande envergure et garantir la sécurité des appareils.

Des services informatiques personnalisés

Quand les services d'une organisation sont aussi bons que ceux auxquels un utilisateur a accès en dehors du travail, il n'a besoin de rien d'autre. L'informatique doit miser sur les services que les utilisateurs maîtrisent le mieux, et en faire la norme. Les e-mails, les sauvegardes, le partage de fichiers et les services collaboratifs sont tous dans le cloud : à la maison ou sur le campus, les utilisateurs travaillent dans un environnement unique et centralisé. Une fois les services identifiés, il faut les gérer pour atténuer les risques et garantir le respect des règles de sécurité.

Un VPN pour sécuriser les pratiques réseau

Collaborez avec votre fournisseur de services cloud pour simplifier le VPN pour vos utilisateurs. Vous pouvez même aller au-delà de la simple identification par mot de passe et imposer une authentification Wi-Fi basée sur des certificats pour que seuls les appareils connus puissent accéder au réseau. Plutôt que de demander aux utilisateurs de saisir leur mot de passe pour accéder au VPN – ce qui pourrait les décourager, misez sur votre outil MDM et envoyez-leur un certificat lorsqu'ils s'inscrivent dans la solution de gestion. C'est leur certificat qui leur donne au réseau, sans aucun effort.

Imposer le chiffrement des données

Les universités peuvent appliquer leurs règles de chiffrement et obtenir facilement des rapports de conformité à l'échelle de l'institution. Il s'agit d'exploiter la technologie de chiffrement intégrée, pour éviter d'ajouter une sécurité tierce aux appareils des utilisateurs. Avec cette approche, le service informatique gère toutes les clés de récupération et peut rapidement réinitialiser les mots de passe, contourner le verrouillage de l'appareil et même effacer son contenu à distance.

Conclusion

En vous appuyant sur des bonnes pratiques de sécurité centrées sur l'utilisateur et sur une solution MDM, vous donnerez à l'équipe informatique les moyens de protéger les systèmes universitaires et les appareils du personnel des piratages et des logiciels malveillants. Et tout cela en offrant une excellente expérience aux utilisateurs. L'informatique est trop souvent un travail ingrat. Mais en suivant ces conseils, les universités et leur personnel informatique peuvent devenir des modèles de cybersécurité et s'épargner une mauvaise presse.

Demandez une version d'essai de Jamf dès aujourd'hui et agissez pour mieux protéger votre institution.

Demander une version d'essai

Ou contactez votre revendeur Apple.