UTILISER LES TECHNOLOGIES À DISTANCE DE MANIÈRE À PROTÉGER L'INFORMATION : CONSEILS À L'INTENTION DES ÉTABLISSEMENTS UNIVERSITAIRES

MARS 2021 ITSAP.00.140

Les établissements universitaires ont été forcés de se tourner vers les technologies d'accès à distance en raison de la pandémie. Ces dernières permettent au corps professoral, au personnel, aux chercheurs et aux étudiants de travailler et d'apprendre, peu importe où ils se trouvent. Il y a toutefois plusieurs risques à la cybersécurité dont les établissements universitaires devraient tenir compte afin de les atténuer.

RISQUES

Pour protéger l'information sensible de votre établissement, il convient de comprendre les risques associés aux technologies à distance et de mettre en place les mesures d'atténuation appropriées. Parmi les risques dont il faut tenir compte au moment de mettre en œuvre des technologies à distance dans votre organisation, citons :

- une implémentation mal configurée peut rendre vos systèmes vulnérables aux auteurs de menace qui cherchent à porter atteinte à votre information sensible ou à la voler (p. ex. propriété intellectuelle, données financières, renseignements personnels);
- l'accès, le traitement ou le stockage de données à l'extérieur du Canada peut donner lieu à une divulgation des données et à une surveillance locale (p. ex. lois en matière de respect de la vie privée);
- des points terminaux (p. ex. des dispositifs personnels) et des réseaux (p. ex. Wi-Fi public) non sécurisés peuvent offrir aux auteurs de menace l'occasion d'accéder au réseau de votre organisation.

Il est important que votre organisation mette en œuvre les technologies à distance de façon appropriée et porte une attention particulière au degré de sensibilité de l'information qui sera communiquée. Votre organisation pourrait subir de graves revers (p. ex. atteinte à la réputation, perte financière, actions potentielles en justice) si ces risques ne sont pas gérés adéquatement.

MENACES COURANTES

Voici quelques menaces courantes qui visent les établissements universitaires :

Menace interne : Quiconque a accès aux réseaux, aux systèmes et à l'information de l'établissement peut causer des dommages, que ce soit intentionnellement (p. ex. voler des données pour obtenir un gain personnel) ou involontairement (p. ex. traiter à son insu l'information de façon inappropriée).

Hameçonnage : Un auteur de menace appelle, envoie un texto ou utilise les médias sociaux de manière à inciter les utilisateurs à cliquer sur un lien malveillant, à télécharger un maliciel ou à divulguer de l'information sensible.

Logiciel malveillant : Un logiciel malveillant (ou maliciel) peut infecter les réseaux, les systèmes et les dispositifs de manière à ce que des auteurs de menace puissent accéder à l'information sensible.

Rançongiciel : Type de maliciel qui rend vos données inaccessibles (p. ex. verrouillage de système et chiffrement de fichiers) jusqu'à ce qu'une rançon soit versée.

Si l'attaque de l'auteur de menace est fructueuse, il pourra prendre le contrôle des comptes, effectuer des transactions et des modifications non autorisées, et voler de l'information sensible ou personnelle.

SÉRIE SENSIBILISATION

CONSIDÉRATIONS LIÉES À LA SÉCURITÉ

Comme il y a des risques associés à l'utilisation des technologies à distance, il est préférable que l'établissement universitaire, le corps professoral et les étudiants prennent certaines mesures pour protéger les réseaux, les systèmes et l'information sensible contre les cybermenaces les plus courantes.

POUR LES ÉTABLISSEMENTS

- Utilisez un système de gestion de l'apprentissage (SGA) pour faciliter la distribution et la soumission du matériel au corps professoral et aux étudiants;
- Utilisez des réseaux privés virtuels, des pare-feux et des antivirus pour protéger vos réseaux des menaces courantes;
- Appliquez le principe de droit d'accès minimal pour protéger l'information contre les accès non autorisés.

Pour un degré de sensibilité plus élevé, il convient d'envisager de prendre les mesures suivantes :

- Utilisez une infrastructure de postes virtuels pour accéder aux réseaux de l'établissement depuis des dispositifs personnels;
- Utilisez un fournisseur de services gérés pour ce qui est de la prise en charge et de la gestion des mesures de sécurité propres à votre établissement;
- Choisissez des fournisseurs de services basés au Canada pour veiller à ce que votre information sensible soit protégée en vertu des lois canadiennes en matière de respect de la vie privée.

POUR LE CORPS PROFESSORAL ET LES ÉTUDIANTS

- Utilisez des outils, des plateformes et des applications de sécurité pris en charge par l'établissement lorsque vous travaillez à distance;
- Sécurisez votre réseau Wi-Fi domestique en activant les fonctions de sécurité et en changeant le mot de passe par défaut;
- Connectez-vous à des réseaux Wi-Fi sécurisés lorsque vous travaillez dans des lieux publics et évitez de vous connecter à un Wi-Fi public si vous accédez à de l'information sensible;
- Utilisez des phrases de passe uniques et activez l'authentification multifacteur pour tous les comptes;
- Évitez de divulguer de l'information sensible lorsque vous utilisez des applications de vidéoconférence;
- Verrouillez les réunions par vidéoconférence au moyen d'un mot de passe qui n'est communiqué qu'aux personnes autorisées.

Si le corps professoral et les étudiants traitent des données hautement sensibles, il convient d'envisager de prendre les mesures suivantes :

- Utilisez des applications de messagerie sécurisées (c.-à-d. chiffrées) prises en charge par votre établissement si vous devez envoyer des données;
- Utilisez d'autres formes de communication pour vérifier l'identité de la personne avec qui vous échangez des données (p. ex. gestion de l'identité);
- Reconnaissez les risques qui vous entourent et mettez en place les mesures appropriées pour éviter que les données fassent l'objet d'une surveillance locale.

POUR EN SAVOIR PLUS

Consultez certaines de nos publications pour en apprendre plus sur les pratiques exemplaires en matière de cybersécurité :

- *ITSAP.10.003 – Comment protéger votre organisation contre les menaces internes*
- *ITSAP.00.101 – Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*
- *ITSAP.00.057 – Protéger l'organisme contre les maliciels*
- *ITSAP.00.099 – Rançongiciels : comment les prévenir et s'en remettre*
- *ITSAP.80.101 – Les réseaux privés virtuels*
- *ITSAP.10.216 – Vidéoconférence*
- *ITSAP.30.032 – Pratiques exemplaires de création de phrases de passe et de mots de passe*
- *ITSAP.70.111 – Utiliser un poste de travail virtuel à la maison et au bureau*
- *ITSAP.00.266 – Messagerie instantanée*
- *ITSAP.30.030 – Sécurisez vos comptes et vos appareils avec une authentification multifacteur*
- *ITSAP.80.009 – Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation*

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.