Utiliser les technologies à distance de manière à protéger l'information : conseils à l'intention des établissements universitaires

Mars 2024

ITSAP.00.140

L'adoption de technologies à distance est devenue essentielle pour les établissements universitaires. Ces dernières permettent au corps professoral, au personnel, aux chercheuses et chercheurs et aux étudiantes et étudiants de travailler et d'apprendre, peu importe où ils se trouvent. Les technologies à distance comprennent l'utilisation de réseaux privés virtuels (RPV), de systèmes de gestion de l'apprentissage (SGA), et d'outils et plateformes de collaboration. Toutefois, lorsqu'on étudie ou travaille à distance, il peut arriver que l'on n'ait pas accès à toutes les mesures de sécurité mises en place par son établissement universitaire. Il est préférable de recréer ces mesures de sécurité à partir de l'endroit où vous travaillez et sur vos appareils de télétravail afin d'atténuer les risques liés aux cybermenaces les plus courantes.

Les risques liés à l'utilisation de technologies à distance

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. Tenez compte des risques suivants lorsque vous mettez en œuvre des technologies à distance dans votre organisation.

- Une mise en œuvre 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.
- 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.

Votre organisation doit mettre en œuvre les technologies à distance de manière appropriée et doit être consciente du niveau de sensibilité de toute information partagée. Si ces risques ne sont pas gérés de manière appropriée, votre organisation pourrait subir de graves répercussions telles que :

- des atteintes à sa réputation
- des pertes financières
- des poursuites judiciaires

Menaces courantes

Voici quelques menaces courantes qui visent les établissements universitaires.

Menace interne : Quiconque a accès aux réseaux, systèmes et informations institutionnels peut causer du tort. Cela peut se produire intentionnellement (p. ex. vol de données à des fins personnelles) ou involontairement (p. ex. traitement inapproprié d'information par inadvertance).

Hameçonnage : Lorsqu'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.

Maliciel : 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.

Rançongiciels : 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.

Remplacer les dispositifs en fin de vie

Les dispositifs qui ont atteint leur fin de vie représentent un risque pour la sécurité de votre organisation. La fin de vie signifie que le fournisseur cesse la commercialisation, la vente et le soutien technique ainsi que les mises à jour du dispositif. Lorsque vous utilisez des dispositifs sur lesquels les plus récentes mises à jour de progiciels n'ont pas été appliquées, vous vous exposez à des cyberattaques. Un progiciel est un logiciel qui a été installé et mis à jour par le fabricant, et qui contient d'importantes mesures de sécurité. Vous pouvez vérifier si votre dispositif est en fin de vie en consultant la liste de produits en fin de vie du fournisseur ou en accédant aux dossiers du routeur dans les journaux du système.

SÉRIE SENSIBILISATION

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

No de cat. D97-1/00-140-2024F-PDF
ISBN 978-0-660-69933-2

Mesure de sécurité

Les étapes suivantes peuvent aider à protéger les réseaux, les systèmes et les informations sensibles contre les cybermenaces courantes lors de l'utilisation de technologies à distance.

Pour les établissements

Votre institution doit s'assurer qu'elle met en œuvre des mesures de sécurité qu'elle peut surveiller et appliquer tout en offrant des possibilités de collaboration.

- 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.
- Utilisez les services d'un fournisseur de services infonuagiques (FSI) agréé et d'une agente ou d'un agent de sécurité d'accès au nuage (CASB) pour appliquer les politiques de sécurité.
- 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.
- Mettez en place un processus d'identification et d'authentification solide, y compris l'utilisation de l'authentification multifacteur (AMF).
- Assurez-vous que les administratrices et administrateurs et les utilisatrices et utilisateurs disposant de droits privilégiés utilisent des postes de travail administratifs qui leur sont réservés pour effectuer leurs tâches.

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.
- Tenez à jour vos systèmes d'exploitation et vos dispositifs électroniques.

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.
- 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.

Réseau CANARIE

Le Réseau canadien pour l'avancement de la recherche, de l'industrie et de l'enseignement (CANARIE) fournit des outils de soutien et de développement, y compris des ressources infonuagiques, aux hôpitaux de recherche, universités, collèges et installations scientifiques du Canada. CANARIE fournit également des services de gestion de l'identité et une connectivité internationale au Réseau national de recherche et d'éducation (RNRE) du Canada. De plus, CANARIE et le Canadian Shared Security Operations Centre se sont associés pour offrir des capacités de cybersécurité améliorées. Programme de cybersécurité du Canadian Shared Security Operations Centre

Pour en savoir plus…

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

- Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)
- Protéger votre organisation contre les maliciels (ITSAP.00.057)
- Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)
- Les réseaux privés virtuels (ITSAP.80.101)
- Utiliser un poste de travail virtuel à la maison et au bureau (ITSAP.70.111)
- Zones de sécurité de réseau en nuage (ITSP.80.023)
- Étapes à suivre pour déployer efficacement l'authentification multifacteur (ITSAP.00.105)
- Vidéoconférence (ITSAP.10.216)
- Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009)
- Gestion de l'identité des justificatifs d'identité et de l'accès (GIJIA) (ITSAP.30.018)