FACTEURS À CONSIDÉRER SUR LE PLAN DE LA RECHERCHE ET DU DÉVELOPPEMENT

SEPTEMBRE 2020 **ITSAP.00.130**

L'innovation, le développement et le progrès sont les pierres angulaires de tout organisme de recherche. Vos données de recherche et votre propriété intellectuelle sont des cibles de grande valeur pour les auteurs de cybermenace et une cyberattaque fructueuse pourrait vous empêcher de mener vos activités et mettre en péril vos données. Pour protéger votre environnement de recherche et vos données, il est impératif que votre organisme comprenne les cybermenaces courantes et mette en place des mesures de sécurité de base.

LES ORGANISMES DE R ET D SONT DES CIBLES DE GRANDE VALEUR

Vos recherches peuvent viser à améliorer les fonctionnalités d'un produit ou d'un service, ou à faire progresser les connaissances dans un domaine particulier. C'est pourquoi la recherche et le développement (R et D) sont essentiels à la croissance économique, à la prospérité et à la sécurité du Canada. Les entreprises canadiennes font appel à vos données de recherche pour tirer un avantage concurrentiel sur le marché. Par exemple, le système de soins de santé compte sur la R et D pour améliorer les soins prodigués aux patients à travers le monde.

En plus de satisfaire les besoins des consommateurs, les organismes de R et D se font concurrence entre eux pour accroître la valeur pour les actionnaires. Ils ont besoin d'un soutien financier pour contribuer à la croissance économique du Canada et à l'expansion de son infrastructure.

Les auteurs de cybermenace peuvent mener des attaques en vue de perturber les activités de R et D, de voler des données aux fins de vente ou de procurer un avantage à des concurrents. Les mesures de cybersécurité protègent vos données et vous aident à conserver un avantage concurrentiel. Si votre organisme n'a encore mis en place aucune mesure de sécurité, il convient d'adopter les pratiques exemplaires décrites dans la présente. Des contrôles de sécurité efficaces aideront à protéger votre organisme contre les menaces qui pourraient avoir une incidence sur les résultats de vos activités de R et D.

LES CYBERMENACES COURANTES

Les auteurs de cybermenace peuvent avoir recours à différentes méthodes pour falsifier ou voler vos données de recherche et votre propriété intellectuelle. Les menaces ci-dessous ne sont que deux exemples, mais ces attaques peuvent rendre vos systèmes vulnérables à d'autres menaces.

Hameçonnage : Un auteur de menace vous appelle, vous envoie un texto ou un courriel, ou communique avec vous par l'entremise des médias sociaux pour vous inciter à cliquer sur un lien malveillant, à télécharger un maliciel ou à divulguer de l'information sensible. Les attaques par hameçonnage peuvent permettre à l'auteur de menace de voler les mots de passe que vous utilisez pour vous connecter à un portail de recherche ou à des comptes liés à votre travail.

Pour de plus amples renseignements, consultez l'ITSAP.00.101, *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*, sur notre site Web.

Menace interne : Quiconque a accès à l'infrastructure et aux données de votre organisme peut causer des dommages sans le vouloir ou de façon délibérée. Un membre de votre personnel pourrait, par exemple, obtenir accès aux bases de données de recherche dans le but d'en voler le contenu. Par ailleurs, un chercheur ou un collègue qui perd un dispositif de stockage portatif (p. ex. clé USB) contenant des données sensibles est un exemple de menace interne non intentionnelle. Qu'elle soit intentionnelle ou non, la menace interne peut avoir pour incidence d'entraver les progrès réalisés par l'organisme ou de mettre à risque son information.

Pour de plus amples renseignements, consultez l'ITSAP.10.003, *Comment protéger votre organisation contre les menaces internes*, sur notre site Web.

Ces deux cybermenaces mènent souvent à des attaques par **rançongiciel** contre les organismes de la R et D. Le rançongiciel est un type de maliciel qui rend vos données inaccessibles. Il peut, par exemple, verrouiller les systèmes ou chiffrer l'ensemble des fichiers jusqu'au paiement d'une rançon.

Pour de plus amples renseignements, consultez l'ITSAP.00.099, *Rançongiciels : comment les prévenir et s'en remettre*, sur notre site Web.

SÉRIE SENSIBILISATION

LA PREMIÈRE ÉTAPE : METTRE EN PRATIQUE CES MESURES DE SÉCURITÉ

Même si la cybersécurité est une nouvelle priorité pour votre organisme, vous pouvez prendre des mesures pour réduire les risques associés aux cybermenaces et aux vulnérabilités. Celles-ci ne sont que le point de départ. Pour de plus amples conseils, consultez la publication *Contrôles de cybersécurité de base pour les petites et moyennes organisations*.

ASSUREZ LA FORMATION DU PERSONNEL DE VOTRE ORGANISME

Les employés, les chercheurs, les étudiants et les entrepreneurs devraient prendre part à une formation dans le cadre de laquelle on abordera les questions de cybersécurité et les pratiques exemplaires à adopter. Ils pourront ainsi mieux comprendre le rôle qu'ils seront appelés à jouer pour protéger votre organisme des cybermenaces. Vous pourriez inclure dans la formation des sujets tels que la création de phrases de passe, des astuces sur la façon de reconnaître les courriels suspects et malveillants, et comment naviguer sur Internet en toute sécurité. Il convient également de discuter des comportements attendus et des exigences en matière de sécurité, notamment le chiffrement de l'information, le verrouillage des dispositifs et des ordinateurs lorsqu'ils sont inutilisés, et le signalement des incidents à un point de contact désigné.

FAITES APPEL À L'AUTHENTIFICATION MULTIFACTEUR

L'authentification multifacteur est un processus qui consiste à vérifier les identités en faisant appel à deux méthodes distinctes (appelées *facteurs d'authentification*). On retrouve trois types de facteurs d'authentification : quelque chose que vous connaissez, quelque chose que vous avez et quelque chose qui vous caractérise. Vous utilisez sans doute déjà certaines formes d'authentification multifacteur comme le fait d'avoir à utiliser votre laissez-passer (quelque chose que vous avez) et à saisir un code (quelque chose que vous connaissez) pour entrer dans les installations de recherche, ou encore d'utiliser votre empreinte digitale pour déverrouiller votre téléphone (quelque chose qui vous caractérise).

INSTALLEZ DES LOGICIELS ET DES OUTILS DE SÉCURITÉ

Vous pouvez installer des outils de sécurité sur vos systèmes et vos dispositifs, comme des pare-feux et des antivirus, pour protéger vos systèmes et vos réseaux contre les maliciels. Nous vous recommandons d'utiliser le Bouclier canadien de l'Autorité canadienne pour les enregistrements Internet (ACEI) pour protéger vos systèmes contre les attaques par hameçonnage et les maliciels.

Si vos employés font du télétravail, mettez en place un réseau privé virtuel (RPV). Un RPV permet de créer un tunnel chiffré par l'entremise duquel les employés pourront envoyer de l'information en toute sécurité. Pour de plus amples renseignements, consultez l'ITSAP.80.101, *Les réseaux virtuels privés*, sur notre site Web.

Vous devriez également envisager de confier à un fournisseur de services gérés (FSG) la gestion des outils de sécurité nécessaires à la protection de vos données sécurisées. Ce dernier pourra veiller à la sécurité des points terminaux et aider votre organisme à contrôler qui accède aux données et à partir d'où (p. ex. en sécurisant les données gérées par les organisations à l'extérieur du Canada). Assurez-vous que votre FSG respecte les lois canadiennes en matière de protection de la vie privée.

APPLIQUEZ LES MISES À JOUR ET LES CORRECTIFS AUX DISPOSITIFS ET AUX LOGICIELS

Appliquez les mises à jour et les correctifs à vos dispositifs et à vos logiciels de manière à protéger vos systèmes contre les vulnérabilités de sécurité (p. ex. des bogues logiciels). L'application fréquente des mises à jour et des correctifs permettra de réduire le risque que des cybermenaces arrivent à porter atteinte aux systèmes et aux données de votre organisme.

METTEZ EN PLACE DES CONTRÔLES D'ACCÈS

Les employés de votre organisme n'ont pas tous besoin d'accéder à la même information. Votre organisme devrait appliquer le principe du droit d'accès minimal et n'accorder à ses employés que les privilèges nécessaires à l'exercice de leurs fonctions. L'octroi de privilèges excessifs fait planer de plus grands risques sur votre organisme, puisqu'il pourrait en résulter une fuite de données ou une atteinte à la vie privée.

Les justificatifs d'identité servant à se connecter aux systèmes devraient être propres à chaque employé et non partagés entre plusieurs utilisateurs. Il conviendra également de révoquer les privilèges accordés au moment où des employés changent de projet ou quittent l'organisme.

SAUVEGARDEZ VOS DONNÉES

La sauvegarde des données de votre organisme vous aidera à récupérer vos systèmes d'information en cas d'attaque, de panne ou de catastrophe naturelle. Assurez-vous de stocker vos sauvegardes sur un dispositif qui n'est pas directement connecté au réseau principal. Il sera ainsi possible de les protéger des cyberattaques visant vos systèmes principaux (p. ex. des rançongiciels) et de fournir une façon de les récupérer au besoin. Vous devriez aussi tester vos sauvegardes sur une base régulière.

Les services d'infonuagique sont un moyen courant et commode de stocker les sauvegardes de données. Assurez-vous que le fournisseur de services a recours à l'authentification multifacteur pour accéder à l'information et chiffrer les données inactives et en transit, et qu'il stocke les données au Canada (c.-à-d., qu'elles sont protégées en vertu des lois canadiennes en matière de protection de la vie privée).

POUR EN SAVOIR PLUS

Consultez certaines de nos publications connexes pour d'autres pratiques exemplaires en matière de cybersécurité :

- ITSAP.30.030, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur*;
- ITSAP.00.057, *Protéger l'organisme contre les maliciels*;
- ITSAP.10.096, *Application des mises à jour sur les dispositifs*;
- ITSAP.00.087, *Dispositifs mobiles et voyages d'affaires*;
- ITSE.50.060, *Avantages et risques liés à l'adoption des services fondés sur l'infonuagique par votre organisation*;
- ITSM.10.189, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information*.

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**.