CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Facteurs à considérer pour les organismes de recherche et de développement

Avril 2024 ITSAP.00.130

En tant qu'organisme de recherche et de développement (R et D), vous innovez et faites de nouvelles découvertes continuellement. Cela implique toutefois que vos données et votre propriété intellectuelle sont des cibles présentant un très grand intérêt. Les auteures et auteurs de cybermenace peuvent tenter d'accéder à vos serveurs et à votre information à des fins malveillantes. Une cyberattaque fructueuse peut vous empêcher de poursuivre vos activités et compromettre vos données. Pour protéger votre environnement de recherche et votre propriété intellectuelle, il est impératif que votre organisme comprenne les cybermenaces courantes et mette en place des mesures de sécurité de base.

Raisons qui font des organismes de recherche et de développement des cibles de grande valeur

La 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 travaux 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 l'équipement médical et les soins prodigués aux patientes et patients à travers le monde.

Les auteures et 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. Il s'agit d'une perte pour l'organisme et la croissance économique du Canada et l'expansion de son infrastructure.

Cybermenaces courantes

Les auteures et auteurs de cybermenace peuvent avoir recours à différentes méthodes pour falsifier ou voler vos données de recherche et votre propriété intellectuelle, et compromettre votre organisme. Voici quelques exemples des nombreuses menaces qui peuvent rendre vos systèmes vulnérables.

Hameçonnage : Une auteure ou un auteur de menace peut vous appeler, vous envoyer un texto ou un courriel, ou communiquer 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'auteure ou auteur de menace de voler les justificatifs d'identité que vous utilisez pour vous connecter à des portails de recherche et à des comptes liés à votre travail, ou de figer les réseaux et de ralentir les opérations.

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. 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.

- Menace interne intentionnelle : Un membre de votre personnel pourrait obtenir l'accès aux bases de données de recherche dans le but d'en voler le contenu
- Menace interne non intentionnelle : Une chercheuse ou un chercheur, ou une ou un collègue qui perd un dispositif de stockage portatif contenant des données sensibles (p. ex. clé USB)

Rançongiciels : L'hameçonnage et les menaces internes mènent le plus souvent à des attaques par rançongiciel contre les organismes de R et D. Un rançongiciel est un type de maliciel qui restreint l'accès à un dispositif ou à un réseau, rendant les données inaccessibles jusqu'à ce qu'une rançon soit versée. Par exemple, une auteure ou auteur de menace peut envoyer un courriel d'hameçonnage comportant un lien qui verrouillera l'accès aux systèmes et chiffrera tous les fichiers jusqu'à ce qu'un paiement soit effectué.

Pratiques exemplaires de cybersécurité

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.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-130-2024F-PDF
ISBN 978-0-660-70812-6

Former le personnel

Le personnel devrait prendre part à une formation dans le cadre de laquelle les questions de cybersécurité et les pratiques exemplaires à adopter seront abordées. Il pourra ainsi mieux comprendre le rôle qu'il sera appelé à jouer pour protéger votre organisme des cybermenaces. Votre formation relative à la cybersécurité devrait comprendre les sujets suivants :

- reconnaître les courriels suspects,
- utiliser Internet de manière sécuritaire,
- développer de bonnes habitudes en matière de mots de passe.

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 lorsqu'ils sont inutilisés,

Utilisation de l'authentification multifacteur (AMF)

L'AMF 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).

Mettez en place des contrôles d'accès

Les employées et 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 aux membres du personnel 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 des cyberattaques.

Les justificatifs d'identité servant à se connecter aux systèmes devraient être propres à chaque employée ou employé et non partagés entre plusieurs utilisatrices et utilisateurs. Il conviendra également de révoquer les privilèges accordés au moment où des employées ou 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. 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. Vos données devraient être stockées au Canada en vertu des lois canadiennes en matière de respect de la vie privée.

Installez des logiciels et des outils de sécurité

Vous pouvez installer des outils de sécurité sur vos systèmes et vos dispositifs, comme des pare-feu et des antivirus, pour protéger vos systèmes et vos réseaux contre les maliciels. Nous recommandons le recours au Bouclier canada de l'Autorité canadienne pour les enregistrements Internet (ACEI) pour protéger vos systèmes contre des cyberattaques.

Si vos employées et 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 employées et employés pourront envoyer de l'information en toute sécurité.

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, comme 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, comme 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.

Pour en savoir plus

- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Sécurité des TI : difficultés observées chez les employés (ITSAP.00.005)
- Protéger l'organisme contre les maliciels (ITSAP.00.057)
- Dispositifs mobiles et voyages d'affaires (ITSAP.00.087)
- Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)
- Ne mordez pas à l'hameçon :Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Les réseaux privés virtuels (ITSAP.80.101)
- Avantages et risques liés à l'adoption des services fondés sur l'infonuagique par votre organisation (ITSE.50.060)
- Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)

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**.