Protéger l'information au niveau organisationnel

AOUT 2022

ITSAP.10.097

À l'image des technologies qui continuent de croître, les cybermenaces (p. ex. les attaques par maliciel, par hameçonnage ou par rançongiciel) ne cessent d'évoluer et de se développer. Votre organisation doit donc constamment s'adapter pour protéger ses réseaux, ses systèmes, ses actifs de TI et son information contre les technologies et les menaces qui évoluent. Par exemple, les dispositifs connectés à Internet gagnent en popularité en milieu de travail et sont employés à des fins professionnelles. Bien que ces dispositifs soient synonymes d'efficacité et de commodité, ils peuvent aussi mettre votre organisation à risque sur le plan de la sécurité. Par conséquent, votre organisation doit prendre des mesures pour protéger l'information au niveau organisationnel.

Évaluation de votre information

En évaluant l'information que vous détenez et sa sensibilité, vous vous assurez de prendre les mesures de protection nécessaires. Vous devez tenir compte des types d'information que détient votre organisation lorsque vous en faites l'évaluation. Par exemple, votre organisation peut détenir de l'information opérationnelle essentielle (comme de l'information sur les ventes ou des plans d'intervention d'urgence), de l'information sensible qui doit demeurer confidentielle (comme des renseignements personnels ou financiers ou de la propriété intellectuelle) ou encore des dossiers et des éléments probants qui ne doivent pas être modifiés sans autorisation (comme des contrats).

Vous pouvez ainsi établir la valeur de l'information en déterminant les dommages qui pourraient se produire en cas de compromission. En accordant une valeur à l'information, vous priorisez vos efforts de protection.

Gestion de votre information

Votre organisation est tenue de gérer et de protéger l'information durant tout son cycle de vie (c.-à-d. de sa création à sa destruction). La gestion de l'information comprend des activités de traitement, de destruction et de stockage adéquats de l'information. À la fin de son cycle de vie, lorsque l'information n'est plus nécessaire sur le plan opérationnel, il faut s'assurer de la détruire correctement.

Un logiciel de prévention de la perte de données peut également aider votre organisation à ne pas perdre le contrôle de ses données. Ce type de logiciel s'appuie sur des alertes, du chiffrement et d'autres mesures de protection pour empêcher les utilisateurs de communiquer des données sensibles.

Vous devez veiller à ce que les activités de sensibilisation et de formation de votre organisation portent sur la gestion de l'information afin que le personnel, les entrepreneurs et les fournisseurs de services comprennent leurs rôles et leurs responsabilités. Il peut s'avérer intéressant d'aborder les sujets suivants :

- la bonne gestion de l'information physique et numérique;
- la conservation de l'information durant la période requise
- la destruction adéquate de l'information
- le nettoyage des supports
- le suivi des systèmes d'information et des composantes au moyen de répertoires
- la sauvegarde de l'information.

SÉRIE SENSIBILISATION

No de cat. Dnn-n/nn-nnn-2021F-PDF
ISBN nnn-n-nnn-nnnnn-n

Sécurisation de vos données à l'externe

Vous devez examiner vos pratiques de gestion de l'information lorsque vous avez recours à des dispositifs mobiles, à des fournisseurs de services ou à d'autres systèmes d'information externes (p. ex. un support de stockage portatif). Pour protéger votre information organisationnelle à l'externe, vous devez vous assurer que les systèmes externes employés sont munis de contrôles de sécurité qui respectent les politiques de sécurité de votre organisation. Pour veiller à la protection de l'information organisationnelle qui est stockée sur des systèmes d'information externes, tenez compte des recommandations suivantes :

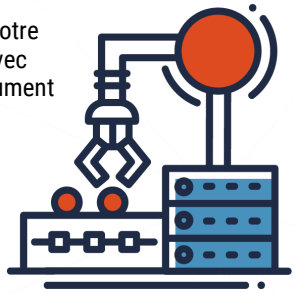
- mettre en place des contrôles de sécurité sur les dispositifs employés avant de les connecter à vos systèmes organisationnels
- restreindre l'accès des dispositifs employés à certains types d'informations, de services ou d'applications
- recourir à un environnement virtuel pour empêcher les autres composantes des systèmes de porter atteinte aux données de l'organisation
- veiller à ce que les utilisateurs et les partenaires acceptent les conditions de votre organisation (p. ex. documenter les ententes)
- surveiller continuellement tous les dispositifs d'extrémité
- vérifier les systèmes d'information externes en cas de compromissions soupçonnées (p. ex. mises à jour anormales, changements ou tentatives d'authentification).

PROTECTION DE DONNÉES PAR DES FOURNISSEURS DE SERVICES

Les données stockées à l'extérieur du Canada sont assujetties à des lois et à des règlements différents en matière de protection des renseignements personnels, de sécurité et de propriété des données. Si vous faites appel à un fournisseur de services infonuagiques ou à un fournisseur de services gérés à l'étranger, assurez-vous de comprendre les lois qui s'appliquent et les possibles répercussions quant à la confidentialité de vos données, et d'évaluer le niveau de sensibilité des données qui y seront stockées.

Protection de votre chaîne d'approvisionnement

Votre organisation peut se servir de systèmes et de services qui sont fournis par d'autres organisations. Vous devez détecter les risques et convenir de politiques de sécurité afin de bien protéger l'information. Lorsque vous collaborez avec des fournisseurs de services, nous vous recommandons de négocier un accord sur les niveaux de service (ANS) pour établir vos attentes quant aux services à recevoir. Votre ANS devrait aussi indiquer les mesures de sécurité mises en place et définir les rôles et les responsabilités quant aux audits à réaliser et aux interventions en cas d'incident.



Pour connaître les façons de protéger votre organisation lorsque vous collaborez avec d'autres fournisseurs, consultez le document *ITSAP.00.070 Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations*.

Choix d'un modèle de déploiement des dispositifs mobiles

Les dispositifs mobiles peuvent améliorer l'efficacité du travail à distance pour votre organisation, mais ils peuvent aussi mettre l'information de votre organisation à risque. En cas de compromission d'un dispositif, des auteurs de menace peuvent accéder aux réseaux, aux systèmes et à l'information de votre organisation. Les quatre modèles de déploiement des dispositifs mobiles organisationnels sont présentés ci-dessous :

- le déploiement de dispositifs réservés au travail qui appartiennent à l'organisation
- le déploiement de dispositifs pouvant servir à des fins personnelles et appartenant à l'organisation
- le déploiement de dispositifs au choix;
- le déploiement de dispositifs personnels.

Le choix d'un modèle de déploiement des dispositifs mobiles dépend du degré de propriété du dispositif par l'organisation. Il faut donc tenir compte du degré de propriété et de l'usage personnel dans le cadre de l'évaluation des menaces et des risques quand vient le temps de choisir le modèle qui convient le plus à votre organisation (p. ex. niveau de contrôle par rapport à l'information contenue dans le dispositif).

Pour en savoir plus sur les modèles, consultez le document *ITSAP.70.002, Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles*.

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**.