PROTECTION DE L'INFORMATION DE GRANDE VALEUR :

CONSEILS POUR LES PETITES ET MOYENNES ORGANISATIONS

AVRIL 2019 ITSAP.40.001

Les petites et moyennes organisations détiennent de l'information importante (p. ex. des renseignements sur les clients et les employés de même que des renseignements commerciaux de nature délicate) qu'elles doivent protéger contre les menaces pour veiller au bon déroulement des activités. Les petites et moyennes organisations sont des cibles probables de cyberattaques. Comme ces organisations manquent souvent de ressources pour mettre en œuvre des mesures de sécurité, les auteurs de menace les considèrent comme des sources d'information et d'argent facilement accessibles. Il se peut que vous ne soyez pas en mesure de protéger toute votre information, mais vous pouvez à tout le moins protéger celle qui est la plus importante pour votre organisation.

CONNAÎTRE LA VALEUR DE L'INFORMATION

En sachant la valeur de l'information de votre organisation, il vous sera plus facile d'établir la priorité de l'information à protéger. Vous pouvez déterminer la valeur de l'informations en évaluant les préjudices pouvant être causés résultant de l'incapacité de protéger la confidentialité, l'intégrité et la disponibilité de l'informations, comme dans les exemples qui suivent :

- **Confidentialité :** information de nature délicate a été consulté par des personnes non autorisées.
- **Intégrité :** quand cela n'est pas censé, l'information est modifiée ou supprimée.
- **Disponibilité :** l'information est inaccessible ou perdue.

Lorsque vous déterminez la valeur de l'information, tenez compte des types d'information suivants :

- **Information opérationnelle essentielle :** information nécessaire au fonctionnement de votre organisation (p. ex. information sur les ventes, plans d'intervention en cas d'urgence).
- **Information de nature délicate :** information devant rester confidentielle ou à laquelle seules certaines personnes peuvent accéder (p. ex. données personnelles ou financières, propriété intellectuelle).
- **Documents et preuves :** devant être protégés contre toute modification non autorisée (p. ex. contrats ou reçus).

ÉTABLIR LES MENACES ET LES VULNÉRABILITÉS

En identifiant les menaces et les vulnérabilités auxquelles fait face votre organisation, vous pouvez prendre des mesures de sécurité qui répondent à vos besoins opérationnels. Une menace ou vulnérabilité courante peut toucher votre organisation d'une façon différente d'une autre organisation.

Une **menace** est définie comme étant toute cause possible d'un incident, d'un événement ou d'un acte pouvant nuire à votre organisation ainsi qu'aux systèmes et à l'information organisationnels. Les menaces peuvent être des catastrophes naturelles (p. ex. un incendie et une inondation). Elles peuvent également être d'origine humaine. Un **auteur de menace** est la personne qui déclenche une menace, intentionnellement ou non. Les auteurs de menace peuvent cibler votre organisation pour diverses raisons, notamment pour réaliser un gain financier grâce à l'information volée, pour semer le chaos ou pour se venger.

Réfléchissez aux types de menace qui pourraient toucher votre organisation en fonction de vos activités et du type d'information que vous détenez.

Une **vulnérabilité** est une lacune ou une faiblesse dans vos mesures de sécurité courantes. Différents facteurs peuvent être à la source des vulnérabilités, comme des versions périmées de logiciels, de l'information non chiffrée, des mots de passe faibles ou des logiciels infectés par un virus.

FAIRE DE LA CYBERSÉCURITÉ UNE PRIORITÉ ORGANISATIONNELLE

Lorsque vous intégrez des mesures de sécurité à vos activités, vous protégez votre information de grande valeur et votre organisation dans son ensemble. Vos clients s'attendent à ce que vous assuriez la protection de leurs renseignements personnels, et les organisations avec lesquelles vous faites affaire veulent savoir que vous n'exposerez pas leurs systèmes et leur information à des menaces.

Il n'existe pas de solution instantanée ou universelle en sécurité, et le contexte de la menace ne cesse d'évoluer. Pour protéger votre organisation, vous devez aborder la sécurité comme un processus continu de prévention, d'établissement et d'élimination des menaces. La sécurité devrait faire partie intégrante de vos processus et de vos plans d'organisation.

PROTÉGER L'INFORMATION DE GRANDE VALEUR

Les réseaux, les systèmes et l'information sécurisés de manière adéquate risquent moins d'être compromis que ceux présentant des lacunes en matière de sécurité. Protégez l'information de grande valeur de votre organisation en appliquant les conseils ci-dessous

1. **Établissement**
   - Soyez conscient de la valeur de votre information.
   - Sachez où est stockée l'information de grande valeur.
   - Dressez la liste des employés qui ont accès à l'information de grande valeur.
   - Examinez les menaces et les vulnérabilités s'appliquant à votre organisation.

2. **Protection**
   - Contrôlez l'accès aux systèmes et à l'information de nature délicate.
   - Chiffrez l'information de nature delicate.
   - Installez les mises à jour logicielles et les correctifs dès qu'ils sont offerts.
   - Utilisez des mécanismes de filtrage des courriels et du Web.
   - Avant de procéder à une disposition, effacez tout le materiel.

3. **Détection**
   - Utilisez un logiciel antivirus et antimalware.
   - Activez, gérez et surveillez les journaux d'activités pour cerner les problèmes ou les incidents.

4. **Intervention**
   - Élaborer un plan d'intervention en cas d'incident.
   - Formez les employés sur leurs rôles et responsabilités.

5. **Reprise**
   - Sauvegardez l'information régulièrement.
   - Déterminez si une cyberassurance pourrait vous convenir.

Consulter le Guide Contrôles de cybersécurité de base pour les petites et moyennes organisations pour identifier les contrôles de sécurité de base que vous pouvez implémenter pour assurer la sécurité de votre organisation et votre information de grande valeur.

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 (CCC) à cyber.gc.ca.