EMPREINTE NUMÉRIQUE

JANVIER 2022 **ITSAP.00.133**

Votre organisation utilise Internet pour mener des activités opérationnelles, fournir des capacités de télétravail aux employés et offrir des services aux clients. À la lumière des activités que réalisent vos employés et partenaires sur différentes plateformes et applications en ligne, songez à l'empreinte numérique qu'ils laissent derrière eux.

Les empreintes numériques contiennent de l'information sensible dont peuvent tirer profit les auteurs de cybermenace. À l'aide de techniques de suivi et de surveillance, les auteurs de menace peuvent accéder à cette information sensible et l'exfiltrer, compromettant ainsi sa confidentialité et sa sécurité.

QU'EST-CE QU'UNE EMPREINTE NUMÉRIQUE?

Une empreinte numérique désigne la trace de données que vous créez lorsque vous utilisez Internet. Cette trace de données est issue des sites Web que vous consultez, des courriels que vous envoyez et de l'information que vous soumettez ou téléchargez en ligne. Vous contribuez à votre empreinte de façon active et passive.

- **Empreinte numérique active :** Données laissées à la suite d'activités intentionnelles, telles que l'affichage de contenu sur les médias sociaux, le remplissage de formulaires en ligne ou l'acceptation des témoins de navigateur.
- **Empreinte numérique passive :** Données laissées involontairement ou sans le savoir. Ces données sont souvent recueillies par la surveillance de votre adresse IP. Les sites Web et les applications peuvent installer des témoins sur les dispositifs sans vous en aviser, utiliser la géolocalisation ou consigner vos activités.

Ainsi, réfléchissez aux personnes qui contribuent à votre empreinte numérique et prenez les mesures de sécurité appropriées pour la protéger.

QUELS SONT LES RISQUES?

Il incombe à votre organisation de protéger l'information sensible (comme les noms de clients, les données financières et l'information d'identification personnelle) qu'elle recueille. Les auteurs de cybermenace sont à la recherche de vulnérabilités qu'ils peuvent exploiter pour accéder à de l'information sensible. Appliquez des mesures de protection adéquates lorsque vous traitez des données sensibles afin de prévenir les atteintes à la protection des données et à la vie privée.

Faites preuve de prudence lorsque vous communiquez de l'information au sujet d'autres personnes en ligne. Certaines personnes se préoccupent grandement de la protection de leur vie privée et de leur empreinte numérique.

Il est extrêmement important de pouvoir assurer la sécurité de l'information sensible de vos clients et ainsi de préserver la réputation de votre organisation. La compromission des empreintes numériques peut causer des problèmes lors de la vérification des antécédents, donner lieu à un vol d'identité et porter atteinte à la réputation. Mettez en place les mesures préventives nécessaires afin de protéger la confidentialité et l'intégrité de votre information sensible.

QUELLES SONT LES MENACES?

Les auteurs de menace tentent d'exploiter les vulnérabilités et d'accéder à de l'information sensible au moyen de techniques de collecte de données par l'entremise des empreintes actives et passives.

Les techniques les plus courantes comprennent les attaques par hameçonnage et la mystification de sites Web. En cliquant sur un lien, en téléchargeant une pièce jointe ou en échangeant de l'information sensible, vous facilitez l'accès des auteurs malveillants à votre empreinte numérique.

Les programmes « prenez votre appareil personnel (PAP) », les appareils intelligents et les réseaux Wi-Fi non sécurisés sont des vecteurs que peuvent employer les auteurs de menace pour recueillir des données. Avec l'augmentation du télétravail, des données sensibles sont susceptibles d'être transmises sur des appareils et des réseaux qui ne sont pas protégés par les mesures de sécurité appropriées.

Si votre entreprise gère des commandes en ligne, vous devez prendre en compte des considérations supplémentaires relatives à la protection des données sensibles. Veuillez consulter l'*ITSAP.40.016, Utiliser le chiffrement pour assurer la sécurité des données sensibles* pour obtenir des renseignements détaillés sur le chiffrement et la navigation sécurisée.

No de cat. D97-1/00-133-2022F-PDF
ISBN 978-0-660-41485-0

SÉRIE SENSIBILISATION

QUELLES MESURES DE PROTECTION DE LA VIE PRIVÉE PUIS-JE PRENDRE?

La protection de la vie privée est importante. Afin de réduire les risques d'exploitation des données sensibles, veuillez envisager l'adoption des mesures suivantes.

Formez et sensibilisez vos employés. Offrez de la formation à tous les employés pour les tenir au fait des enjeux relatifs à la cybersécurité et à la protection de la vie privée. La formation devrait comprendre un volet sur les mesures appropriées de protection et de traitement de l'information ainsi qu'un volet sur les pratiques exemplaires en matière de cybersécurité.

Lisez les politiques de confidentialité et les conditions d'utilisation. Avant de télécharger une application ou d'utiliser un service, il est important de lire et de bien comprendre les types d'information recueillie, les façons dont cette information peut être utilisée et les mesures de sécurité en place pour protéger les renseignements personnels.

Désactivez les témoins, dans la mesure du possible. Même si vous ne partagez pas activement de l'information sur les applications et sites Web, vos données font l'objet d'un suivi par l'entremise de votre appareil, de votre adresse IP et de votre réseau.

Configurez les paramètres par défaut. Les paramètres de certaines applications sont réglés par défaut à « accès public ». Configurez plutôt vos paramètres de sécurité et de protection de la vie privée au mode le plus sécurisé et restrictif possible.

Désactivez les paramètres de surveillance. Évitez d'utiliser les applications non nécessaires qui exigent l'accès à votre emplacement, à votre calendrier ou à vos contacts. Désactivez les paramètres qui analysent et surveillent vos activités dans le but de vous présenter de la publicité ciblée.

Restez au fait des changements apportés aux conditions d'utilisation, aux mises à jour et aux paramètres de protection de la vie privée des applications.

QUELS AUTRES FACTEURS DEVRAIS-JE PRENDRE EN CONSIDÉRATION?

Pour veiller à ce que vos activités en ligne soient à l'abri des auteurs de cybermenace, envisagez de mettre en œuvre les mesures préventives suivantes :

- installez un antivirus et un pare-feu pour réduire les risques de partage passif des données;
- imposez la création de mots de passe ou de phrases de passe robustes et uniques pour tous les comptes;
- mettez en place un système de gestion des appareils ou des applications mobiles afin de surveiller les programmes PAP;
- limitez la navigation de sites Web non chiffrés et installez des extensions de navigateur Web qui renforcent la protection de la vie privée (comme un bloqueur de publicité);
- retirez les comptes et les privilèges d'accès aux employés qui n'en ont plus besoin;
- accordez l'accès aux utilisateurs selon le principe du besoin de connaître et classifiez les données en fonction du niveau de sensibilité;
- créez une politique relative à l'utilisation des médias sociaux pour clarifier les attentes relatives au contenu pouvant être partagé sur les comptes organisationnels;
- retirez les métadonnées des photos avant de les partager et de les afficher en ligne, car ces informations sont stockées dans le fichier image et peuvent exposer des renseignements personnels tels que votre emplacement géographique.

POUR EN SAVOIR PLUS

Consultez les publications du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) sur son site Web (**cyber.gc.ca**), notamment les suivantes :

- *Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations (ITSAP.00.070)*
- *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.100)*
- *Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016)*
- *Sécurité de l'Internet des objets pour les petites et moyennes organisations (ITSAP.00.012)*
- *Est-ce que votre appareil intelligent vous écoute? (ITSAP.70.013)*
- *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)*
- *Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)*
- *Comment vous protéger du vol d'identité en ligne (ITSAP.00.033)*
- *Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)*

Consultez les cours offerts par le Carrefour de l'apprentissage du Centre pour la cybersécurité sur son site Web (**cyber.gc.ca/fr/carrefour-de-lapprentissage**), notamment les suivants :

- *Cours 110 – La cybersécurité dans le GC et la visibilité en ligne (1/2 journée)*
- *Cours 152 – Protection des renseignements personnels numériques (90 minutes)*

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**.