CONSEILS DE SÉCURITÉ POUR LES ORGANISATIONS DONT LES EMPLOYÉS TRAVAILLENT À DISTANCE

Mai 2020

ITSAP.10.016

Le travail à distance pose certaines difficultés lorsqu'il s'agit de trouver un équilibre entre fonctionnalité et sécurité. Lorsqu'ils travaillent à distance, vos employés doivent avoir accès aux services, aux applications et aux informations internes dont ils se serviraient normalement s'ils travaillaient depuis le bureau. Cependant, votre organisation doit également protéger ses systèmes et ses informations, et le travail à distance comporte sa part de risques. Vous devez donc mettre en place des mesures de sécurité additionnelles visant à empêcher les auteurs malveillants d'exploiter d'éventuelles vulnérabilités de vos systèmes.

COMPRENDRE LES MENACES QUI SE POSENT POUR LES TRAVAILLEURS À DISTANCE

Le travail à distance peut accroître le risque de compromission des informations sensibles de votre organisme. Les auteurs malveillants ont recours à diverses approches pour cibler les travailleurs à distance :

- **Accès physique à un dispositif :** Lorsqu'ils sont laissés sans surveillance dans un lieu public, les dispositifs peuvent être volés ou piratés par un auteur malveillant.
- **Hameçonnage :** Un auteur malveillant se faisant passer pour le représentant d'une organisation légitime communique avec la personne ciblée au moyen de courriels, de messages textes ou d'appels téléphoniques pour lui demander de transmettre des informations sensibles (p. ex. mots de passe, numéros de cartes de crédit).
  - **Piratage psychologique :** Un auteur malveillant peut collecter de l'information portant sur votre organisation ou l'un de ses employés (p. ex. le site Web de l'organisation, les comptes de médias sociaux) dans le but de créer un message d'hameçonnage qui paraît légitime.
- **Rançongiciel** : Suivant l'utilisation d'un maliciel, un auteur malveillant empêche une victime d'accéder aux données contenues dans son propre dispositif. Ensuite, cet auteur malveillant ne permettra à la victime d'accéder à ses propres données que si elle lui verse une somme d'argent.
- **Piratage de réseau sans fil :** Un auteur crée un réseau sans fil malveillant, mais lui donne le nom d'un réseau existant et légitime (p. ex. le nom du réseau public d'une chaîne de cafés-restaurants bien connue).
- **Écoute clandestine :** Un auteur malveillant surveille le trafic de réseaux sans fil et enregistre les activités en ligne ainsi que les mots de passe employés.
- **Altération du trafic** : Lorsqu'un dispositif mobile est infecté par du code trafiqué, un auteur malveillant peut y introduire du trafic piraté dans le but de fausser des données et d'accéder au réseau de votre organisation.

GÉRER LES DISPOSITIFS MOBILES

Si possible, vos employés devraient utiliser des appareils fournis par l'organisation lorsqu'ils travaillent à distance. Rappelez à vos employés de suivre les politiques organisationnelles et d'utiliser les appareils selon les règles établies (par exemple, uniquement à des fins professionnelles).

Lorsque les employés utilisent des appareils personnels pour le travail, il faut être au courant des risques :

Omission d'installer les mises à jour de sécurité. Les dispositifs personnels peuvent ne pas être mis à jour ni corrigés régulièrement. Dans ce cas, les vulnérabilités persistent et accroissent les risques de compromission.

Utilisation de mots de passe faibles. Certains dispositifs personnels ne sont pas protégés par un NIP ni par un mot de passe. Et encore, l'emploi de NIP ou de mots de passe faibles (faciles à deviner) constitue un risque.

Perte de contrôle sur les informations. S'ils sont utilisés à des fins professionnelles, les dispositifs personnels peuvent contenir des informations commerciales sensibles que votre organisation ne peut plus gérer convenablement.

Rappelez aux employés de suivre les politiques organisationnelles (par exemple, le stockage d'informations professionnelles dans les dépôts de l'organisation) lorsqu'ils utilisent des dispositifs personnels. Le cas échéant, rappelez-leur les pratiques exemplaires qui permettent de sécuriser les dispositifs, notamment l'activation de l'authentification à plusieurs facteurs, la surveillance ininterrompue des dispositifs (surtout en public) et l'utilisation de logiciels antivirus.

PRÉPARER LES EMPLOYÉS

Pour les employés qui n'ont jamais travaillé à distance, la transition pourrait s'avérer difficile. Donnez-leur les moyens de bien s'adapter en leur communiquant clairement les mesures à prendre pour contribuer à la cybersécurité de votre organisation.

- Mettez en place des politiques et des procédures qui décrivent, par exemple, les modes acceptables d'utilisation des appareils de l'entreprise et de gestion des informations de l'entreprise.
- Veillez à ce que vos employés sachent qui contacter (les coordonnées doivent être à jour), en particulier s'ils rencontrent des problèmes de sécurité ou si leur dispositif est égaré ou volé.
- Formez vos employés sur les enjeux de cybersécurité et sur les pratiques exemplaires, notamment la détection des tentatives d'hameçonnage, la création de phrases de passe et de mots de passe forts, et l'utilisation de réseaux sans fil sécurisés.

SÉRIE SENSIBILISATION

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

UTILISER LES OUTILS DE SÉCURISATION

Il existe des outils de sécurisation que votre organisation peut utiliser pour ajouter des couches de protection additionnelles à vos réseaux, systèmes et appareils. Les outils de sécurité présentés ci-dessous ne sont que quelques exemples des moyens que vous pouvez utiliser pour réduire les risques d'intrusions malveillantes causées par des maliciels ou par d'autres types de cyberattaques.

Or, les outils de sécurité peuvent réduire les risques pour votre organisation, mais il ne faut pas oublier qu'aucun outil n'est parfait. Vous ne devez jamais vous fier uniquement à un seul outil. Il faut également mettre en place des contrôles de sécurité complémentaires.

Réseau privé virtuel (RPV)

Le RPV est un tunnel de communication sécurisé et chiffré par lequel les informations sont acheminées. Vous pouvez utiliser un RPV pour établir une connexion sécurisée qui impose un mode d'authentification et protège les données. L'utilisation d'un RPV permet de créer un réseau de communication privé (pour votre organisation) qui traverse un réseau non sécurisé. Indiquez à vos employés qu'ils sont tenus d'utiliser le RPV pour se connecter aux serveurs de l'organisation.

Pare-feu

Le pare-feu est une barrière de sécurité placée entre deux réseaux. Il contrôle la quantité et les types de trafic qui peuvent circuler entre les réseaux. Un pare-feu renforce la sécurité des systèmes de l'organisation en surveillant le trafic entrant et le trafic sortant tout en filtrant le trafic indésirable que les systèmes peuvent reconnaître.

Logiciel antivirus

Vous devriez avoir recours à un antivirus et veiller à ce que celui-ci soit tenu à jour. Le logiciel antivirus protège les dispositifs contre les maliciels en balayant les fichiers et les systèmes que contiennent ces dispositifs.

Liste blanche des applications

La liste blanche des applications est une technique utilisée pour établir quelles applications peuvent fonctionner sur les appareils fournis par l'employeur. Ainsi, votre organisation peut créer une liste blanche qui définit toutes les applications approuvées et qui, par la même occasion, empêche les utilisateurs d'exécuter ou d'installer des logiciels non autorisés (ne figurant pas à la liste) sur les dispositifs de l'entreprise.

PROTÉGER LES DISPOSITIFS

Dès lors que les employés doivent travailler depuis leur domicile ou un lieu public, il devient important que les mesures énoncées ci-dessous soient rigoureusement appliquées pour protéger les dispositifs et leur information. Du coup, il conviendra également d'inciter les employés à appliquer les mêmes mesures à leurs dispositifs personnels.

- **Authentification à plusieurs facteurs**. Pour ajouter une couche de protection supplémentaire, imposez l'authentification à deux facteurs (ou plus) pour le déverrouillage des dispositifs. Par exemple, les facteurs d'authentification peuvent être un NIP et une empreinte digitale.
- **Économiseur d'écran avec mot de passe**. Lorsqu'un utilisateur est inactif, son dispositif se verrouille automatiquement après un laps de temps prédéfini.
- **Installation des mises à jour et des correctifs**. Configurer les dispositifs pour qu'ils exécutent automatiquement la mise à jour des logiciels d'exploitation, des applications principales et des logiciels de sécurité.
- **Désactivation des fonctions Bluetooth et sans fil sur les dispositifs non utilisés**. La désactivation des fonctions Bluetooth et sans fil empêche les auteurs malveillants de se connecter aux dispositifs.

PROTÉGER L'INFORMATION

Votre organisation est tenue de protéger les informations sensibles qu'elle collecte et utilise. Rappelez-vous que les informations sensibles sont des cibles très prisées par les auteurs malveillants.

- **Sauvegardez les informations**. Les informations doivent être sauvegardées régulièrement, et les copies de sauvegarde doivent être conservées en toute sécurité.
- **Chiffrez les informations**. Utilisez les fonctions de chiffrement pour protéger la confidentialité des informations sensibles. Par exemple, vous devez autoriser les utilisateurs à accéder à des sites Web compatibles HTTPS uniquement depuis des appareils fournis par l'employeur.
- **Appliquez le principe du privilège minimum**. Veillez à ce que les employés aient accès seulement aux informations dont ils ont besoin pour faire accomplir leurs tâches. Ce type de contrôle peut prévenir les accès non autorisés aux données ainsi que les violations de données.

POUR EN SAVOIR DAVANTAGE

Les conseils énoncés plus haut constituent un bon point de départ, mais il serait utile de lire les publications énumérées ci-dessous pour en savoir davantage :

- *Utiliser la technologie Bluetooth (ITSAP.00.011)*
- *Protéger l'organisme contre les maliciels (ITSAP.00.057)*
- *Reconnaître les courriels malveillants (ITSAP.00.100)*
- *Application des mises à jour sur les dispositifs (ITSAP.10.096)*
- *Conseils de cybersécurité pour le télétravail (ITSAP.10.116)*
- *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*
- *Les réseaux privés virtuels (ITSAP.80.101)*

Toutes ces publications (et bien d'autres) peuvent être consultées dans le site Web du Centre canadien pour la cybersécurité : **cyber.gc.ca.**