Parlons prévention

Des conseils pour vous et votre entreprise

Vos employés font du télétravail? Voici cinq raisons de mettre un réseau VPN à leur disposition.

En raison de la pandémie de COVID-19, beaucoup d'entreprises ont mis en place des mesures de télétravail. Il est donc devenu primordial d'assurer la cybersécurité de tous ces bureaux à domicile. L'une des meilleures façons de protéger les employés et les données d'une entreprise est d'avoir recours à un réseau privé virtuel (VPN en anglais).

Voici cinq façons dont un réseau privé virtuel contribue à protéger vos employés :

- **Réseau plus sûr et protection pare-feu**
  En faisant passer le trafic Internet d'un employé par le réseau de votre entreprise, vous êtes en mesure d'offrir à cet employé les mêmes pare-feu et autres solutions de protection réseau qu'il aurait dans un bureau où d'excellentes mesures de cybersécurité ont été mises en place.

- **Facteur supplémentaire d'authentification**
  L'authentification à facteurs multiples n'est pas sans faille, mais elle ajoute un degré de sécurité supplémentaire pour protéger votre réseau. Des exigences de complexité pour les mots de passe que doivent utiliser les employés pour accéder aux données de l'entreprise réduisent les risques de compromission découlant de mots de passe trop simples et prévisibles.

- **Capacité de limiter l'accès aux données de l'entreprise**
  Si vous permettez uniquement à vos employés actuels d'accéder aux données de l'entreprise, repérer une anomalie dans l'utilisation du réseau devient plus facile. Par exemple, si vous voyez 19 employés connectés à partir de Montréal et un employé connecté à partir de Moscou, vous pouvez plus facilement détecter une cyberattaque potentielle.

- **Protection des données contre le monde extérieur**
  Les détournements de données se trouvant sur des serveurs non sécurisés sont courants, et le fait d'avoir un grand nombre d'employés qui consultent les données de votre entreprise à distance à partir de nombreux endroits différents ne fait qu'accroître ce risque.
  En protégeant vos données à l'aide d'un réseau privé virtuel et en demandant aux utilisateurs de s'identifier pour les consulter, vous pouvez éviter que vos données ne soient dévoilées au grand jour.

- **Protection pour les réseaux Wi-Fi publics et partagés**
  En ce moment, beaucoup d'employés sont en isolement chez eux. Toutefois, ils n'ont pas tous accès à un service Internet fiable et rapide, et certains doivent donc utiliser un réseau Wi-Fi public ou partagé. L'utilisation d'un réseau virtuel privé bien sécurisé signifie que les données des employés sont chiffrées et donc plus difficiles à détourner lorsqu'elles passent par un réseau Internet partagé ou plus ou moins fiable.

Pour savoir comment rendre votre entreprise encore plus sécuritaire, communiquez avec le Service de prévention au **1.833.692.4112** ou rendez-vous au **www.federated.ca**.

[3584-074-ed01F | 05.2020] | © Les assurances Federated. Parlons prévention est une marque de commerce utilisée par **La Federated, Compagnie d'assurance du Canada** (émettrice des polices Les assurances Federated) avec l'autorisation de la Corporation financière Northbridge. Le présent bulletin Parlons prévention est fourni uniquement à titre informatif et ne vise pas à remplacer les conseils de professionnels. Nous ne faisons aucune assertion et n'offrons aucune garantie relativement à l'exactitude ou à l'intégralité des renseignements qu'il contient. Nous ne pourrons en aucun cas être tenus responsables des pertes pouvant découler de l'utilisation de ces renseignements.