LA PRESSE

Northbridge Assurance

Infonuagique, télétravail et commerce en ligne : êtes-vous protégé contre les cyberrisques ?

Une étude réalisée par la Fédération canadienne de l'entreprise indépendante (FCEI) révèle qu'en six mois, une PME canadienne sur six a été la cible d'une cyberattaque infructueuse[1]. « La question à se poser n'est plus *si*, ni même *quand* une attaque peut survenir, mais plutôt : quand l'entreprise va-t-elle s'en rendre compte ? », soulève Benoit Marc

Dufresne, spécialiste en souscription et en cyberrisques à Northbridge Assurance. Bien que divers facteurs puissent expliquer pourquoi les PME s'avèrent des proies naturelles pour les cybercriminels, quelques moyens simples et économiques peuvent suffire à décourager les attaques.

Publié le 6 octobre 2021 à 8h15

Ce qui fait des PME des cibles intéressantes

Les risques technologiques évoluent plus rapidement que la capacité pour bien des PME à s'y adapter, faisant d'elles des proies faciles.

« Beaucoup n'ont pas d'infrastructures de sécurité en place, de plan d'urgence ou de surveillance

pour détecter les brèches », explique Josée Lévesque, directrice principale, Assurances professionnelles et solutions spécialisées chez Lussier Dale Parizeau, un important courtier d'assurance indépendant au Québec.

La sécurité des systèmes et des réseaux informatiques à la maison se compare rarement à celle d'un bureau. « Le routeur peut être moins bien protégé. Les employés qui travaillent à partir de leur ordinateur personnel ne font peut-être pas les mises à jour de leur système d'exploitation et de leurs logiciels aussi assidûment, ce qui ouvre la porte aux cyberattaques potentielles », souligne M. Dufresne.

Petit lexique des cyberattaques

Faille du « Jour zéro »
Lorsque le fabricant d'un système d'exploitation découvre une faille dans son produit, il émet un correctif à tous les utilisateurs. Ce faisant, l'entreprise annonce malgré elle l'existence d'un

point faible dont les cybercriminels peuvent tirer profit auprès de ceux et celles qui n'ont pas encore téléchargé le correctif. C'est ce qu'on appelle la faille du « Jour zéro ». « Si les mises à jour automatiques ne sont pas activées, ça crée une plus grande fenêtre de vulnérabilité », poursuit M. Dufresne.

Rançongiciel et déni de service

Cliquer sur un lien malveillant, se laisser tromper par un faux courriel, insérer une clé USB trouvée à la réception, autant de gestes anodins qui servent aux cybercriminels. Les résultats les plus courants de ces actions sont le rançongiciel, un logiciel frauduleux qui verrouille l'accès aux fichiers, et le déni de service, qui paralyse le réseau. Un montant d'argent est réclamé pour mettre fin à l'attaque.

Rançons et vente de données

Aujourd'hui, les demandes de rançon sont établies avec précision. « Les cybercriminels ayant déjà infiltré les systèmes connaissent exactement les moyens de l'entreprise ; ils exigent un prix en conséquence », poursuit Josée Lévesque.

Selon une étude récente de Northbridge auprès de 400 entreprises canadiennes, près du tiers d'entre elles ont apporté des changements importants à leur modèle d'affaires, comme effectuer une transition vers le commerce électronique. Ce faisant, elles cumulent désormais de nouveaux types de données. Sur le Web caché (*dark Web*), chaque numéro de carte de crédit peut être mis en vente pour une dizaine de dollars.

Comment protéger votre entreprise des cyberrisques

Protections simples et économiques
Il est faux de croire que les PME n'ont pas les moyens d'investir en cybersécurité. M. Dufresne précise que de nombreuses précautions sont offertes gratuitement ou à coût minime, comme celles-ci :

- Activer la mise à jour automatique des logiciels et du système d'exploitation.

- Exiger des noms d'utilisateurs uniques avec des mots de passe robustes (caractères alphanumériques et longueur minimale), et les changer sur une base régulière.

- Éviter les réseaux Wi-Fi non protégés (ex. : hôtels, restaurants et lieux publics).

- Utiliser l'authentification à facteurs multiples (code de confirmation envoyé par courriel ou par texto).

- Effectuer des sauvegardes quotidiennes des systèmes, idéalement hors ligne et par itération (seuls les fichiers ayant été modifiés sont copiés).

- Offrir une formation annuelle aux employés pour réduire le risque d'erreur humaine.

L'assurance comme protection supplémentaire

Au-delà de ces précautions minimales, M. Dufresne ajoute qu'il existe une suite de logiciels de protection à prix accessible et l'assurance des cyberrisques. Celle-ci devrait couvrir les coûts que devra débourser l'entreprise

pour gérer l'incident de sécurité (expertise informatique, avis aux clients, forfait de suivi du dossier de crédit auprès des clients touchés, etc.), la perte de revenu causée par l'interruption des affaires, la responsabilité civile en cas de poursuite ou de recours collectif, ainsi que les amendes et les règlements.

La courte vidéo ci-dessous résume l'importance d'une telle assurance pour les PME de tous secteurs, tant pour prévenir les cyberattaques que pour y réagir.

L'assureur et le courtier d'assurance s'avèrent également de précieux alliés pour aider les entreprises à y voir plus clair parmi les produits et les couvertures offertes sur le marché. Ils sont aussi là pour les guider dans les clauses du contrat d'assurance en fonction de la législation applicable en matière de protection des données et de la vie privée. « Si les entreprises font affaire à l'étranger, par exemple aux États-Unis ou encore dans des pays membres de l'Union européenne, il faut aussi qu'elles se familiarisent avec la réglementation et

les exigences liées à la protection des données et de la vie privée en vigueur dans ces pays », mentionne Josée Lévesque.

« L'assurance est un outil supplémentaire pour protéger les entreprises, les accompagner en cas d'incident et absorber de potentielles pertes financières si un incident de cybersécurité se déclarait », conclut M. Dufresne. Comme l'assurance auto ou habitation pour les particuliers, l'assurance des cyberrisques pour les entreprises constitue un filet de sécurité. Mais il est de mise d'être prudent sur le Web comme dans la vie. On pourrait dire que choisir des mots de passe complexes et les changer régulièrement est aussi important que de verrouiller ses portes.

Découvrez l'Assurance des cyberrisques chez Northbridge

[1] *Les PME et la fraude informatique, février 2021,* https://content.cfib-

fcei.ca/sites/default/files/2021-02/RapportFCEI-cyberfraude-F. pdf