



INSIGHT

Assurer une meilleure protection de votre entreprise en matière de cybersécurité

Chaque jour, les cyberattaques font la manchette. Le mois dernier, LifeLabs a été victime d'une violation de données qui a potentiellement exposé les données personnelles et les renseignements médicaux de près de 15 millions de Canadiens. Dernièrement, Facebook, Home Depot, Sony, Equifax et Marriott ont également subi de telles attaques. Visiblement, aucune organisation, quelle que soit sa taille, n'est à l'abri des atteintes à la sécurité de ses systèmes.

Les cyberatteintes ne connaissent pas de frontières géographiques; toutes les provinces du Canada sont vulnérables.

Au Québec, certaines vulnérabilités, notamment les systèmes informatiques vieillissants et non protégés, représentent une cible idéale pour les pirates informatiques, comme le démontre le nombre d'attaques en croissance depuis les dernières années. Le secteur public ni échappe pas. En effet, plusieurs ministères et organismes ont aussi subi des attaques qui ont eu des conséquences importantes sur leurs activités telles que

- ▶ Paralysie d'une partie importante du système informatique
- ▶ Paralysie de nombreux postes de travail pendant plusieurs jours,
- ▶ Fuite de données internes,
- ▶ Pannes de sites web,

- ▶ Réception d'un volume considérable de courriels potentiellement malveillants pouvant comprendre des campagnes d'hameçonnage, des virus et autres programmes malveillants.

Des cyberattaques se produisent également à l'extérieur du Québec. Par exemple, un vol de données personnelles au sein de Capital One a touché 106 millions de clients, dont 6 millions au Canada, le 29 juillet.

Il est important de mentionner que bien qu'un grand nombre d'attaques soient signalées, plus de la moitié des violations touchant les PME ne sont pas dénoncées puisque les entreprises veulent éviter d'être embarrassées ou craignent pour leur réputation. Voici quelques prédictions et faits clés intéressants sur la cybersécurité :

- ▶ Gartner prévoit que les dépenses liées à la sécurité de l'information à l'échelle mondiale dépasseront 124 milliards de dollars en 2019.
- ▶ Les pirates informatiques créent environ 230 000 programmes malveillants par jour ([Panda Security](#)).
- ▶ Jusqu'à six mois peuvent s'écouler avant qu'une brèche ne soit détectée (ZD Net).
- ▶ Selon le *2019 Official Annual Cybercrime Report (ACR)*, toutes les 14 secondes, des entreprises sont victimes d'attaques par des rançongiciels.
- ▶ Des outils de piratage informatique à faible coût sont aisément accessibles et de plus en plus faciles à utiliser.

À mesure que le cyberespace se transforme, les risques qui y sont associés augmentent. Chaque année, la cybercriminalité connaît une croissance exponentielle puisqu'il s'agit d'une activité très lucrative pour les criminels. Les risques associés aux programmes malveillants, au hameçonnage et aux attaques par rançongiciels sont bien réels. Cette réalité, qui autrefois touchait uniquement

les grandes entreprises, fait maintenant partie du quotidien de petites entreprises, d'organismes sans but lucratif, d'agences gouvernementales et de municipalités.

Les cyberattaques peuvent avoir de graves répercussions et causer des dommages importants à une organisation. Au nombre de ces répercussions et dommages, notons la perte de données confidentielles et de renseignements commerciaux, l'interruption de services de réseaux et de systèmes ou d'activités commerciales, la perte de données financières, la perte de renseignements personnels d'employés et de clients, le coût de reconstitution ou de restauration de logiciels, la perte de propriété intellectuelle et les coûts réglementaires et juridiques associés au dédommagement pour le vol d'information.

Tout ceci démontre bien l'importance de mettre en œuvre des contrôles et des sauvegardes qui sauront sensibiliser vos utilisateurs et protéger vos systèmes et vos données. Pour assurer la protection de vos données, de votre réseau et de votre personnel, il vous faut d'abord cibler et évaluer les risques liés à vos processus et actifs essentiels, puis établir une stratégie permettant de les atténuer.



Une fois les risques ciblés, votre organisation devra mettre en œuvre les contrôles et processus nécessaires en matière de cybersécurité pour se protéger des cybermenaces. Vous trouverez ci-dessous des exemples de techniques d'évaluation à utiliser pour vous aider à déterminer si le cadre de sécurité de votre entreprise est adéquat :

- ▶ **Évaluation de la cybersécurité** : Détermination du degré de maturité actuel des contrôles de sécurité de l'organisation et comparaison aux meilleures normes de sécurité du secteur.
- ▶ **Bilan de santé du réseau** : Évaluation des contrôles du réseau, y compris le flux du réseau, le trafic du réseau, les contrôles antimaliciels et les contrôles sans fil.
- ▶ **Formations en sensibilisation à la cybersécurité** : Transfert aux employés de connaissances à jour sur l'identification et l'atténuation des cybermenaces.
- ▶ **Processus de continuité de l'entreprise et reprise en cas de sinistre** : Processus permettant d'établir des stratégies pour atténuer les risques afin de permettre à votre organisation de poursuivre ses activités si elle subit une attaque.
- ▶ **Gestion des risques liés aux fournisseurs** : Évaluation de la sécurité des tiers offrant des services à votre organisation.

À partir du résultat de ces évaluations, votre organisation pourra établir une stratégie et un plan pour se protéger des menaces à la cybersécurité.

L'adoption d'une approche proactive en matière de cybersécurité misant sur des pratiques exemplaires constituera le meilleur moyen pour votre organisation de se défendre contre la cybercriminalité.

VEUILLEZ COMMUNIQUER AVEC :

Diane Fugere, FCPA, FCA

VP bureau de Québec / VP Quebec office

418-573-0738

dfugere@bdo.ca

David Daniels

Vice President Adjoint – Services Conseils

514-835-2138

ddaniels@bdo.ca

À PROPOS DE BDO

BDO est l'un des plus importants cabinets de services en certification, comptabilité, fiscalité et consultation au Canada. Profondément enracinés au sein des communautés où ils sont présents, nos professionnels offrent des services hautement personnalisés, appuyés par une excellente connaissance du secteur et près de 100 ans d'expérience sur les marchés d'un océan à l'autre. Appuyé par des ressources au Canada et à l'étranger, BDO offre une expérience continue et uniforme aux clients ayant des besoins à l'étranger.

Certification | Comptabilité | Fiscalité | Services-conseils

www.bdo.ca