Lussier Dale Parizeau
Cabinet de services financiers

Chronique No 2 : Les Cyberrisques…comment se protéger ?

L'équipe de responsabilité professionnelle | 3 octobre 2019

Toute entreprise peut être confrontée à des cyberrisques, qu'ils visent les renseignements personnels des employés ou les renseignements confidentiels de clients ou de fournisseurs. Les conséquences sont multiples : Pénalités pour infraction aux lois et règlements en matière de protection des renseignements ou poursuites en dommages-intérêts (divulgation ou utilisation non autorisée des renseignements) ; perte de productivité (attaque par déni de service, accès bloqué à Internet ou au réseau informatique) ; perte financière ponctuelle (rançongiciel) ; perte financière continue (interruption des affaires résultant d'un blocage d'accès ou à la destruction de données). Mais, comment peut-on se protéger ?

Évidemment, la nature et l'étendue des moyens de protection varient d'une entreprise à l'autre, selon la taille et la nature des activités. Cependant, trois volets devraient se retrouver dans toute bonne politique à cet égard :

1. Meilleures pratiques

- Former et informer les employés sur l'usage sécuritaire des courriers électroniques et des réseaux sociaux, sur les façons de détecter les courriels d'hameçonnage, les rançongiciels ou les programmes malveillants ;

- Développer un plan écrit relatif à la sécurité des renseignements ;
- Se doter d'un plan formel de continuité ;
- Établir des procédures écrites en matière d'autorisation et d'authentification visant les transferts de fonds électroniques ;
- Implanter un contrôle d'accès aux données basé sur les fonctions des employés, afin d'éviter qu'un employé puisse avoir accès inutilement à des données sensibles ;
- Modifier ou supprimer les accès immédiatement lorsqu'un employé change de fonction ou quitte l'entreprise ;
- Se doter d'une procédure formelle de gestion des mots de passe (complexité, changements fréquents);
- Faire effectuer une évaluation des risques par une firme reconnue qui pourra identifier les lacunes, formuler des recommandations sur les pratiques et effectuer un audit périodique.

2. Sécurité informatique

- Logiciel antivirus ;
- Coupe-feu ;
- Protection par mot de passe de l'accès aux réseaux sans fil ;
- Chiffrement des données sur les serveurs/sur les ordinateurs portables ;
- Sauvegarde périodique ;
- Implanter une procédure d'authentification bifactorielle (à deux niveaux, par exemple : mot de passe + carte à puce ou mot de passe + biométrie) ;

3. Protection physique

- Verrouiller les locaux en tout temps et en restreindre l'accès au moyen de cartes à puce ou d'un système d'accès par biométrie ;
- Protéger les locaux par un système d'alarme relié à une centrale de télésurveillance ;

- Munir la salle des serveurs d'un système d'extinction d'incendie à gaz ;
- Conserver les supports de sauvegarde à l'extérieur des locaux, dans un endroit protégé contre le vol et l'incendie ;
- Munir les ordinateurs portables d'un dispositif de verrouillage.

Bien sûr, il serait impossible de couvrir le sujet de façon exhaustive dans une chronique comme celle-ci. Toutefois, un consultant en sécurité informatique saura vous aider à établir un programme adapté à vos besoins.

Vous croyez ne pas être vulnérable et préférez assumer les risques ? Les lois et règlements en matière de protection des renseignements personnels pourraient vous faire changer d'avis.

Suivez-nous, ce sera le sujet de la prochaine chronique.