PASSION AFFAIRES et technologies

Nous aidons les entreprises à transformer leurs technologies en levier d'affaires

ARS solutions 25 ans

Octobre 2018
Vol. 5 n° 8.

ÉDITION SPÉCIALE

TOP 3 DES ARTICLES LES PLUS LUS EN 2018

Suivez-nous

Obligations des dirigeants et administrateurs en matière de TIC

Par Me Marie-Josée Lortie
Joli-Cœur Lacasse Avocats
418 681-7007

TEMPS DE LECTURE 3:30

Grand nombre d'activités commerciales sont affectées par les technologies de l'information et des communications (TIC). Dans les entreprises, on les retrouve notamment dans les services financiers, dans les départements des communications et des ventes ainsi qu'en R&D. Leur importance varie selon les activités de l'entreprise et sa grosseur. Mais au minimum, quelle entreprise n'a pas son site Web, aujourd'hui ?

Les TIC sont génératrices de croissance et de création de valeur pour l'entreprise, mais leur utilisation peut aussi comporter des risques et des coûts. Et pas seulement lors de leur implantation. Le rapport de 2017 de IBM Security et du Ponemon Institute sur les coûts des atteintes aux mesures de sécurité informatique estime que le coût moyen d'une faille informatique au Canada s'élève à 5,78 M$.

Ces coûts d'une cyberattaque incluent les frais rattachés au «colmatage» de la fuite, la reconstruction des systèmes attaqués et, évidemment, la perte de clients dont la confiance aura été ébranlée.

SUITE À LA PAGE 2 ▼

SUITE DE LA PAGE 1 ▲

92 % des entreprises canadiennes ont vécu au moins un cyber incident en 2017 (comparé à 85 % en 2016), *soit le plus haut taux jamais connu. Et pour la première fois de l'histoire,* ***la cybercriminalité a dépassé le vol physique,*** *selon la firme Kroll.*

Comme administrateur d'entreprise, **les questions d'ordre technologique devraient donc vous amener à vous pencher sur les stratégies de développement et d'utilisation des TIC et sur la gestion des risques qu'elles comportent**. Il s'agit d'être capable de **prévenir les risques** par la mise en place de mécanismes de protection, tout en s'assurant que l'entreprise maintienne son avantage stratégique à l'égard de ses compétiteurs par une utilisation optimale des TIC disponibles. Votre capacité à bien le faire pourrait éviter les poursuites contre l'entreprise ou, le cas échéant, vous fournir des moyens de défense plus efficaces.

Vous devez également vous préoccuper de certains aspects légaux rattachés à l'utilisation des TIC. Ainsi, lorsque votre entreprise effectue de la vente par Internet, les informations que vous obtiendrez de vos clients doivent être protégées.

Vous devez vous assurer d'obtenir les consentements adéquats à l'utilisation que vous faites des renseignements de nature personnelle. Le nouveau Règlement général sur la protection des données peut s'appliquer à votre entreprise. **Des modifications à la *Loi canadienne sur la protection des renseignements personnels et les documents électroniques* entreront en vigueur le 1er novembre 2018. Ces modifications ajoutent notamment de nouvelles exigences relatives au signalement obligatoire d'atteintes à la protection des données.**

Le défaut de respecter ces obligations peut entraîner des frais importants pour votre entreprise mais aussi, dans certains cas, pour ses administrateurs et dirigeants. Vous avez des devoirs et responsabilités à rencontrer. Vous devez, entre autres, vous tenir informé des activités de l'entreprise.

VOICI 6 SUGGESTIONS QUI VOUS PERMETTRONT DE REMPLIR VOS OBLIGATIONS D'ADMINISTRATEUR PRUDENT EN MATIÈRE DE TIC :

1. Intégrer, si possible, au conseil d'administration, une ou des personnes ayant des connaissances technologiques qui vous aideront à mieux comprendre les enjeux, les risques et les solutions;
2. À défaut d'intégration d'un administrateur au conseil, s'adjoindre des consultants fiables qui sauront vous conseiller adéquatement;
3. Ramener les questions technologiques au conseil d'administration de façon assez régulière afin d'en évaluer l'utilisation, la sécurité et prévenir les ennuis;
4. Déléguer une personne qui assurera le suivi de la sécurité informatique;
5. Réviser périodiquement les TIC utilisées par l'entreprise afin que celles-ci demeurent concurrentielles;
6. Se doter de règles de gouvernance en matière de TIC qui seront adaptées à votre entreprise.

Vous avez également le devoir d'agir de bonne foi, avec compétence et diligence. Personne ne s'attend à ce que vous soyez un expert en technologie. Cependant, en vous référant aux connaissances réelles d'un expert vous pourrez démontrer, si besoin était, que vous avez rempli ces devoirs qui vous incombent.

Vous avez une responsabilité de comprendre et gérer les technologies qui ne cessent d'évoluer et de prendre de la place. Plus vous connaîtrez les TIC de votre entreprise, mieux vous arriverez à les contrôler.

Attention !

Votre réseau informatique est peut-être HANTÉ par des failles de sécurité et des problèmes latents qui vous prendront au dépourvu…

À moins d'effectuer un entretien régulier et structuré de vos systèmes, inévitablement vous ferez face à des problèmes de virus, de cybercriminels, de corruption de données, de panne matérielle qui pourraient causer un arrêt de vos opérations et nuire sérieusement à votre productivité.

Pour ramener votre réseau fonctionnel, il peut vous en coûter des milliers de dollars en pertes de temps, ventes, etc. Sans compter toutes les frustrations à l'interne…

Il est grand temps de capturer tous ces FANTÔMES qui circulent sur votre réseau et risquent de nuire à votre productivité!

OBTENEZ un diagnostic performance & sécurité

SANS FRAIS Valeur de 795 $

Contactez-nous avant
le 30 novembre 2018
pour bénéficier de cette offre.
info@ars-solutions.ca
418 872-4744 #233

Nous rendons les entreprises plus efficaces et performantes en transforma

TEMPS DE LECTURE 3:15

6 PRÉCAUTIONS À PRENDRE pour réduire vos risques

1 FORMATION EN SÉCURITÉ : TESTS DE *PHISHING*

La plupart des employés ne sont pas familiers avec les meilleures pratiques de base en sécurité et peuvent involontairement créer des failles. Apprenez-leur à sécuriser leurs comptes et à renforcer leurs mots de passe. Ils peuvent aussi stocker des données confidentielles de l'entreprise sur leurs appareils mobiles ou être susceptibles d'ouvrir des courriels d'hameçonnage.

Formez vos employés à détecter les courriels et fichiers frauduleux en effectuant des simulations de *phishing* sur vos employés. Des campagnes d'hameçonnage internes permettent aux employeurs d'éduquer leurs employés en toute sécurité sans risquer de perdre des informations et données précieuses. En étant bien informés, vos employés seront plus alertes et sauront comment aborder une menace.

2 GESTION DE CORRECTIFS (PATCHS)

La gestion des correctifs est une mesure préventive qui adresse et corrige les vulnérabilités découvertes dans les logiciels au fil du temps. Les pirates ciblent souvent ces faiblesses.

L'attaque WannaCry a profité d'une vulnérabilité dans les anciens systèmes d'exploitation Windows. Microsoft a déployé un correctif pour mettre à jour les ordinateurs de bureau et les serveurs quelques mois avant l'attaque, mais nombreux sont ceux qui ne l'avaient pas installé.

3 SCAN DU DARK WEB

Si les données de votre entreprise sont compromises, vous voudrez savoir où circulent vos informations. Les pirates achètent et vendent fréquemment des données volées sur le Dark Web à des fins de vols d'identité et de fraudes.

Un scan du Dark Web surveille les forums de discussion criminels, les réseaux privés et autres sites cachés pour rechercher vos informations volées. **Le système vous avertit lorsqu'il détecte que vos données sont compromises.**

Même si un scan ne peut pas supprimer vos données une fois qu'elles ont été publiées, **il vous permet de prendre des précautions pour doubler la sécurité et vous protéger contre le vol d'identité**.

4 MISE EN PLACE D'UN LOGICIEL DE MONIROTING : SIEM

Il est souvent difficile d'avoir une vision globale de la sécurité de ses systèmes. Pour pallier à ce problème, le **SIEM** (*Security Information and Event Management*) permet de collecter, analyser, surveiller les événements anormaux et corréler des données concernant la sécurité de vos systèmes, de les archiver et de réaliser des opérations de reporting. Par exemple, vous saurez si une personne non autorisée tente de se connecter à vos systèmes pour extraire des informations sensibles telles que des listes de prix ou des listes de clients. Ou si un employé accède à des informations auxquelles il n'a pas les droits.

5 POLITIQUES CLAIRES

Chaque employé devrait être informé des politiques de sécurité dans votre entreprise. Créez des exigences claires en ce qui concerne la sécurité des mots de passe et des identifiants. Si vous proposez un programme **BYOD** (Bring Your Own Device), assurez-vous de l'installation obligatoire d'un logiciel de sécurité. **Clarifiez quelles informations de l'entreprise peuvent ou ne peuvent pas être consultées via des dispositifs personnels.**

6 DÉLÉGUEZ LA SÉCURITÉ

Embauchez un expert du domaine que vous ayez ou non une ressource technique à l'interne. **Vous bénéficierez d'une équipe de spécialistes possédant non seulement un ensemble de compétences, mais également des outils performants** qui sont nécessaires pour vous aider à protéger ce qui compte réellement pour votre entreprise. **La sécurité est un processus à maintenir en continu.**

TEMPS DE LECTURE 2:45

Vos données personnelles et professionnelles sont-elles en vente sur le Dark Web ?

Au-delà des plateformes de vente de drogue, d'achat d'armes, de pornographie juvénile, les voleurs d'identité utilisent aussi le Dark Web pour acheter ou vendre vos informations personnelles et les données confidentielles des entreprises.

Le **Web** : aussi appelé le Clear Web, visible et légal, possède du contenu qui peut-être trouvé par des engins de recherche comme, Google, Yahoo et Bing et il est continuellement sous surveillance.

Le **Dark Web** : aussi appelé le Web invisible, contient des sites illégaux et son contenu n'est pas accessible par les engins de recherche standards. Il est donc difficile de savoir ce qu'il contient.

Si votre adresse de courriel ou nom de domaine de votre entreprise est sur le Dark Web, les criminels ont accès à vos comptes qui y sont associés. Scanner votre adresse de courriel sur le Dark Web est la première étape pour mieux vous protéger et vous donner toute l'information nécessaire pour savoir quoi faire et agir.

COMMENT PROTÉGER MON ENTREPRISE?

Il existe aujourd'hui des technologies utilisant l'intelligence artificielle (IA) qui représentent pour vous la meilleure protection. Cela permet aux entreprises de se protéger contre le vol d'identité et contre le vol de données corporatives sensibles et offre les mêmes fonctionnalités avancées que celles utilisées par les sociétés Fortune 500. Cette approche proactive fournit en temps réel des informations d'identification compromises avant même que le vol d'identité ou les violations de données se produisent.

COMMENT LES INFORMATIONS D'IDENTIFICATION PERSONNELLE SONT TROUVÉES SUR LE DARK WEB?

À partir de votre adresse courriel ou du nom de domaine de votre entreprise, un service de surveillance scanne, détecte, recueille et analyse des informations d'identification compromises, et ce, sans risque pour des sites illégaux, de forums, de sites Web privés, logés dans le Dark Web. Plus de 10 000 requêtes sont faites par jour…

POURQUOI C'EST SI IMPORTANT?

Les informations d'identités personnelles volées telles que les mots de passe et les noms d'utilisateurs sont utilisés pour faire d'autres activités criminelles : vol de données sensibles en entreprises, vol d'identité personnelle des employés…

Les utilisateurs ont souvent le même mot de passe pour plusieurs services, tels que l'ouverture de session réseau, les médias sociaux, les boutiques en ligne et d'autres services. Ceci augmente de manière exponentielle le risque, même à partir d'un seul nom d'utilisateur et mot de passe compromis.

CERTAINES DE CES DONNÉES SONT ANCIENNES ET INCLUENT DES EMPLOYÉS QUI NE TRAVAILLENT PLUS POUR VOUS? VOUS ÊTES QUAND MÊME À RISQUE...

Bien que les employés aient quitté votre organisation, les informations d'identification peuvent toujours être actives et utilisées dans votre entreprise. Les mots de passe et les noms d'utilisateurs pour les bases de données ainsi que les accès donnés à des compagnies tierces pour effectuer de la maintenance ou des travaux sur votre réseau, sont de bons exemples. La découverte des informations d'identification volées devrait être un bon rappel de vous assurer que tous les comptes sont bien sécurisés pour éviter d'être exploités.

ARS solutions affaires et technologies
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744