Décembre 2019 - Janvier 2020 • Vol. 7 n° 1

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies — 30 ans

NOUS AIDONS LES ENTREPRISES À TRANSFORMER LEURS TECHNOLOGIES EN LEVIER D'AFFAIRES

Bonne Année

À TOUS NOS CLIENTS !

Merci d'être là pour nous depuis toutes ces années et de nous aider à nous dépasser jour après jour.

Toute l'équipe d'ARS Solutions vous souhaite une bonne et heureuse année couronnée de succès !

Que cette nouvelle année soit pour vous riche en projets et moments inspirants. Qu'elle soit également une opportunité de dépassement de soi et de fierté.

Suivez-nous

NÉGLIGENCE chez Desjardins?

TEMPS DE LECTURE 4:00

Le Mouvement Desjardins prétend vouloir limiter les dégâts causés par la fuite de données personnelles de sa clientèle alors qu'il congédie deux hauts dirigeants ayant un rôle important pour la cybersécurité de la coopérative.

Le 3 décembre dernier, **Desjardins annonçait le départ du bras droit de son président, Denis Berthiaume, qui était premier vice-président exécutif et chef de l'exploitation en plus de Chadi Habib, premier vice-président des technologies de l'information**. À la suite de « vérifications internes » entourant la fuite de renseignements personnels dévoilée en juin dernier, **ces deux gestionnaires auraient perdu la confiance du président et chef de la direction de Desjardins, Guy Cormier, qui a affirmé vouloir un « leadership renouvelé »**. Ceux-ci avaient été nommés au comité de haute direction en juin 2016 par monsieur Cormier lui-même, peu de temps après son remplacement de Monique Leroux à la présidence. « La confiance que j'accorde aux membres de mon comité de direction est essentielle. Les événements des derniers mois m'amènent à la conclusion qu'il faut apporter des changements dans la composition de la haute direction. », a fait valoir M. Cormier, par voie de communiqué. En s'adressant aux employés, **M. Cormier n'a pas donner de détails sur les raisons de ces congédiements**, se limitant à prétendre que les changements permettraient d'assurer davantage la sécurité à l'interne ainsi qu'à l'externe.

SUITE À LA PAGE 2 ▼

Le premier vice-président exécutif aux finances, trésorerie, administration et chef de la direction financière, Réal Bellemare, assumera également, de façon intérimaire, la responsabilité des technologies de l'information. Difficile de se sentir soulagés par cette décision pour le moment. **Le groupe financier coopératif a également annoncé la création d'un « bureau de la sécurité »** visant à coordonner les différentes initiatives en matière de sécurité et de protection des données.

de la responsabilité de veiller sur la sécurité de plusieurs millions de clients. Avant de vouloir sauver l'image de marque, il faudrait d'abord faire preuve de proactivité et agir de manière raisonnable en s'alliant afin d'assurer une véritable protection sans équivoque aux victimes.

La cybersécurité implique tellement de conséquences pour la présidence d'une entreprise qu'elle ne peut plus être complètement déléguée sans son implication. Elle ne doit pas être confiée à leur département TI sans en assurer la gouvernance à temps plein par les membres de la haute direction. Celle-ci devrait être en mesure d'identifier ce qui est important pour l'entreprise de sécuriser et s'assurer qu'il l'est en tout temps. **Depuis trop longtemps, la sécurité des données est traitée comme s'il s'agissait exclusivement d'un enjeu technologique à confier au responsable du département TI. Il appartient à la présidence d'en assumer la gouvernance et d'élaborer sa stratégie de prévention en cybersécurité**, notamment par la formation continue des employés pour les sensibiliser et par un service de gestion d'information de sécurité et d'événements (SIEM).

Le SIEM devient un outil de gestion pour la haute direction qui doit désormais prendre pleinement part à la gouvernance de la sécurité globale de l'organisation…

Il y a définitivement un problème de gestion au sein du Mouvement Desjardins : **ce n'est que 6 mois après le dévoilement de la fuite de données que l'on apprend qu'elle n'aurait pas seulement touché 2,9 millions de membres, mais bien tous les membres particuliers en plus de 173 000 entreprises et 1,8 million de détenteurs de cartes de crédit**. On a également appris tout récemment la présence de logiciels pisteurs (trackers) qui récoltent des données personnelles sur les clients d'Equifax, dont les supposés protégés de Desjardins. Cette inquiétante nouvelle s'ajoute à celle de la cyberattaque massive dont Equifax avait été victime en 2017 en raison d'une vulnérabilité que l'agence américaine de crédit connaissait depuis plus de 2 mois, mais n'avait pas corrigée. Plus de 6 mois avaient passé suite à la brèche avant que leurs consommateurs canadiens en soient informés. **Les malfaiteurs avaient d'ailleurs manœuvré pendant 77 jours sans être détectés, ce qui leur a permis d'accéder à des renseignements personnels canadiens.**

Ce n'est toutefois pas en éliminant des joueurs que la coopérative gagnera la partie. Ça risque même d'empirer la situation vu le déficit actuel de compétences pour gérer les besoins en cybersécurité de l'organisation. **Il ne s'agit pas d'un jeu de chaise musicale, mais bien** Le SIEM devient un outil de gestion pour **la haute direction qui doit désormais prendre pleinement part à la gouvernance de la sécurité globale de l'organisation, en équipe avec son département des TI**, afin d'en assurer la viabilité financière et de veiller à ce que les **intérêts des actionnaires, des clients et des employés soient protégés**. Desjardins ne démontre pas avoir pris les précautions nécessaires en ayant en place un système de surveillance comme le SIEM. On a réagi au lieu de prévenir pour **minimiser les dommages et avoir la preuve que les bonnes précautions ont été mises en place** afin d'éviter le vol d'informations, que ce soit par un employé malveillant à l'interne ou par des cybercriminels externes.

Sources : Journal Métro et Radio-Canada

Simon Fontaine, Président
simon.fontaine@ars-solutions.ca

66 % des décideurs de haut niveau des petites entreprises

CROIENT TOUJOURS QU'IL EST PEU PROBABLE QU'ELLES SOIENT LA CIBLE DE CYBERCRIMINELS

TEMPS DE LECTURE 4:15

***Avec 43 % des attaques en ligne visant désormais les petites entreprises**, cible favorite des méchants de la haute technologie, **alors que seulement 14 % d'entre elles sont prêtes à se défendre, les propriétaires doivent de plus en plus faire de la cybersécurité une priorité absolue**, selon les responsables de la sécurité des réseaux.*

« Les infrastructures informatiques modernes sont plus complexes et sophistiquées que jamais », explique Jesse Rothstein, directeur technique du fournisseur de sécurité en ligne ExtraHop. Des interactions mobiles aux interactions de bureau, les cybercriminels peuvent lancer des milliers d'attaques numériques conçues pour compromettre vos opérations à tout moment, alors qu'une seule peut être très dommageable. Par conséquent, dit-il, il est garanti que pratiquement toutes les organisations modernes finiront par être touchées. **Pour les propriétaires de petites entreprises, il ne s'agit plus de se demander si des menaces vont survenir, mais plutôt de penser au moment où elles surviendront.**

Pire encore, les conséquences des cyberattaques ne cessent de croître, **les incidents numériques coûtant maintenant aux entreprises de toutes tailles 200 000 $ en moyenne**, selon la compagnie d'assurance Hiscox. 60 % des entreprises font faillite dans les six mois qui suivent leur victimisation. La fréquence de ces attaques est également en hausse; plus de la moitié des petites entreprises ayant subi une violation au cours de la dernière année et 4 sur 10 ayant connu de multiples incidents, révèle Hiscox. En même temps, cependant, selon l'étude de Keeper Security sur la cybermenace des PME de 2019, 66 % des décideurs de haut niveau des petites entreprises croient toujours qu'il est peu probable qu'elles soient la cible de cybercriminels. De même, 6 sur 10 n'ont aucun plan de défense en place, ce qui souligne la nécessité d'une sensibilisation et d'une éducation accrues de l'industrie dans son ensemble.

De plus, étant donné que **les cybermenaces ont tendance à passer en moyenne 101 jours avant d'être détectées** par les opérateurs commerciaux, les dommages causés à une organisation par de telles attaques peuvent rapidement s'accumuler. Les dépenses supplémentaires telles que la conformité réglementaire, les honoraires d'avocats, les enquêtes techniques, la perte de revenus et de relations avec les clients peuvent rapidement s'accumuler pour une petite entreprise. **480 nouvelles menaces sont introduites chaque minute**, selon le fournisseur d'antivirus McAfee. L'erreur humaine reste l'une des plus grandes menaces pour les organisations. Avec seulement 3 employés sur 10 qui reçoivent actuellement une formation annuelle en cybersécurité, il n'est que trop facile pour les malfaiteurs de contourner même les mesures de protection numérique les plus pointues.

VOICI 10 CONSEILS POUR LUTTER CONTRE LES CYBERMENACES :

1. **Utiliser un service de gestion d'information de sécurité et d'événements (SIEM)** pour analyser les réseaux, les comptes utilisateurs et les applications afin de détecter les activités suspectes avant qu'elles ne se propagent;
2. **Faire des sauvegardes quotidiennes et des duplicatas** de données et de fichiers qui peuvent être récupérés en cas de compromission du système ou de rançon;
3. **Installer et mettre à jour régulièrement l'antivirus et le pare-feu du réseau** afin de détecter et de contrer les virus;
4. **Surveiller et analyser régulièrement tout dispositif connecté** à un système ou à un réseau;
5. **Limiter l'accès des employés** aux seuls fichiers, dossiers et applications nécessaires à l'exécution de leurs tâches respectives;
6. **Fournir une formation régulière aux employés**, au moins tous les 90 jours, sur les dernières menaces et tendances en cybercriminalité;
7. **Effectuer des exercices d'enseignement** fondés sur des scénarios réels de la vie quotidienne qui mettent à l'épreuve les employés;
8. **Enseigner au personnel les dangers** de cliquer sur les liens et les pièces jointes de courriels, et la nécessité de rester à l'affût des signes avant-coureurs de courriels frauduleux;
9. **Utiliser l'authentification multifactorielle** avant d'autoriser toute demande majeure ou irrégulière;
10. **Effectuer des tests de vulnérabilité et des évaluations des risques** sur les réseaux et applications pour rechercher et traiter les points de défaillance.

Prendre note que les menaces peuvent provenir aussi bien du personnel interne que de sources externes, et que les entreprises modernes doivent jongler avec un volume croissant d'informations sensibles. Les experts avertissent que les meilleures cyberdéfenses actuelles sont désormais multidimensionnelles.

Source : Scott Steinberg

Voici quoi faire pour augmenter votre productivité de manière super simple

TEMPS DE LECTURE 3:45

Dans la chasse à la productivité accrue, nous recherchons presque instinctivement les coups de pouce simples par définition. Le temps qu'il faut pour apprendre et mettre en œuvre une méthode complexe pour améliorer la productivité combat l'idée même de productivité. Ainsi, lorsque je tombe sur un truc efficace et simple, je me sens obligé de le partager avec mes lecteurs.

Le hack de productivité qui double sa productivité, selon Richard Branson, fondateur de Virgin, est le fait qu'il prend du temps pour faire de l'exercice - au moins 60 minutes par jour, tous les jours. Tout le monde sait que l'on devrait faire de l'exercice, mais le lien avec la productivité est un peu contre-intuitif (étant donné le temps qu'il faut pour faire l'exercice lui-même). La logique de Branson est pourtant très simple (comme il le partage sur son blogue). Si vous vous sentez au mieux de votre forme, vous vous sentirez encore mieux. Il s'entraîne pour se donner de l'énergie, pour combattre la léthargie et pour stimuler son humeur.

« Beaucoup de gens disent qu'ils n'ont pas le temps de faire de l'exercice, et vous avez raison, vous n'avez pas le temps si vous ne prenez pas le temps. Vous établissez vos priorités, et à moins que votre santé n'en fasse partie, il peut être facile de trouver quelque chose d'autre à faire qui semble plus important. La réalité est qu'il n'y a rien de plus important que de prendre soin de soi-même. », dit Branson qui en fait une priorité absolue. Celui-ci n'est pas la seule personne à placer l'exercice sur un tel piédestal et à le considérer comme un facteur d'amélioration de la productivité, par opposition à un facteur de détérioration. **Oprah Winfrey, Mark Cuban et Mark Zuckerberg sont tous connus pour prioriser l'exercice malgré la multitude d'autres choses qu'ils pourraient passer leur temps à faire pour bâtir un empire.** La science conspire avec ces milliardaires pour faire avancer le dossier, car des études de Harvard montrent que l'exercice améliore la mémoire, la concentration et la vivacité d'esprit - toutes choses nécessaires à la productivité et à l'accroissement général de la réussite professionnelle.

Lorsque je travaillais dans le monde des affaires, je faisais de l'exercice, mais je le considérais toujours comme quelque chose qui m'empêchait d'être productif. Mais quelque chose d'étonnant s'est produit lorsque j'ai quitté le monde des affaires pour devenir entrepreneur. J'ai eu l'occasion de tout remettre en question et de redéfinir mes priorités dans ma vie, y compris l'exercice. **J'ai fait de l'exercice la base de ma vie et je l'ai fait fructifier (au lieu de faire de ma vie professionnelle la base de ma vie et d'essayer de faire de l'exercice là où je le pouvais).** J'ai doublé le nombre de fois où je fais de l'exercice, passant de deux à trois à six fois par semaine (et j'ai prolongé mes séances d'entraînement). **Pour ce faire, j'ai établi un horaire où je me lève et je travaille à temps plein au plus tard à 8 h pour profiter de mon temps de réflexion. Je travaille pendant 7 bonnes heures, en ne faisant que de brèves pauses pour le déjeuner et la salle de bain. Ensuite, je vais au gym, je prends une douche et je retourne au travail jusqu'à 18h30.**

Voici la magie pour moi quand il s'agit de faire de l'exercice dans ma vie maintenant : **L'exercice n'enlève pas le temps productif, il le crée.** Je suis beaucoup plus énergique pour la deuxième ronde de travail de la journée, et je laisse derrière moi l'étirement improductif, qui était souvent entre 15 h à 17 h. Je m'entraîne durant cette plage horaire maintenant. **Alors, pensez à prendre le temps de faire de l'exercice comme si vous preniez littéralement du temps pour vous. Votre productivité et le succès qui en découlent seront certainement plus rentables.**

Source : Scott Mautz

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