AVRIL 2020 • Vol. 7 n° 4

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies — 30 ans

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

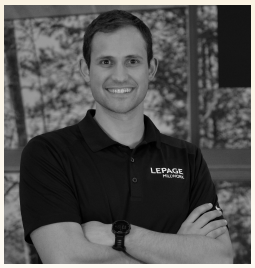
« On pense trop souvent que les Ransomwares c'est pour les autres.

Nous avons été victimes d'une cyberattaque de type Cryptolocker qui a paralysé l'ensemble de nos opérations pendant 8 jours.

On n'a pas l'expertise à l'interne pour répondre à ce genre d'attaque. J'ai donc décidé de contacter ARS pour avoir une firme expérimentée et compétente chez nous dans le but de nous aider à nous remonter plus facilement et plus rapidement.

J'aurais aimé être plus conscient de mes données critiques et de comment elles étaient protégées. **On s'est rendu compte que nos copies de sécurité n'étaient pas suffisantes, même si on s'en occupait à l'interne.**

Si c'était à refaire, on s'informerait plus sur les types d'attaques, comment elles fonctionnent et comment on peut se protéger et faire de la prévention. »



François-Xavier Bonneville
Directeur général
Lepage Millwork

Suivez-nous

La Fromagerie Bergeron

sans prétention et dans un esprit de partage

TEMPS DE LECTURE 5:00

N'oublions pas que, si un seul membre de votre équipe interne est testé positif, ***c'est 14 jours de quarantaine obligatoire pour tous les autres qui ont été en contact avec lui.*** *« On veut aussi protéger nos employés, nos clients et les opérations de l'entreprise », mentionne monsieur Bergeron.*

Tous s'entendent pour dire qu'il doit y avoir une reprise économique. Plus vite nous retournerons à nos activités, mieux ce sera pour tous. **Toutefois, la santé publique demeure un enjeu. Selon monsieur Roger Bergeron, président de la Fromagerie Bergeron, ce serait possible avec un plan approprié.**

Sans prétention et dans un esprit de partage, monsieur Bergeron favorise les échanges avec ses pairs afin de relever tous ensemble de bonnes pratiques qui pourraient conduire à une reprise plus rapide. « **Je ne prétends pas avoir les meilleures mesures de sécurité,** nous a-t-il confié en vidéoconférence, mais je suis persuadé que de partager ce que chacun a mis en place dans son entreprise pourra en aider d'autres. »

Nous avons donc rédigé cet article dans le but de poursuivre cette belle mission de partage avec la communauté d'affaires et d'aider à l'amélioration des pratiques globales au Québec. Les mesures de sécurité qui suivent sont celles mises en place par monsieur Bergeron. Peut-être vous inspireront-elles des idées pour votre propre organisation!

Pour nous partager à votre tour vos idées, écrivez-nous à partagecovid19@ars-solutions.ca et il nous fera plaisir de les transmettre à la communauté.

SUITE À LA PAGE 2 ▼

Voici les mesures de sécurité principales mises en place par la Fromagerie Bergeron en complément des mesures strictes d'hygiène déjà en place :

Contrôle des symptômes

- Prise de température à l'arrivée des employés;
- Questions sur les symptômes lors de la prise de température;
- Les employés doivent communiquer avec l'employeur avant de se présenter au travail en cas de symptômes ou de doute. Un questionnaire doit être complété pour déterminer si l'employé peut se présenter au travail ou s'il doit être mis en retrait préventif.

Désinfection

- Nettoyage et désinfection accrus des aires communes aux deux heures de jour comme de soir;
- Nettoyage de tous les équipements en fin de quart pour tous les départements;
- Ajout de bouteilles désinfectantes pour un nettoyage régulier des postes;
- Ajout d'une station de désinfection des mains obligatoire en arrivant le matin;
- Désinfection des mains obligatoire en entrant pour tous les clients;
- Ajout de plusieurs stations de désinfection des mains dans les différentes sections des bureaux;
- Désinfection des poignées de porte aux deux heures;
- Boîtes de lingettes sur les lifts et transpalettes pour désinfection régulière;
- Distribution de produits désinfectants aux livreurs pour leur permettre de désinfecter leurs mains avant et après chaque client ainsi que leur environnement plusieurs fois par quart (poignées de portes des camions, volants, etc.).

Distanciation sociale

- Réunions en conférences téléphoniques et entrevues par Skype;
- Arrêts des travaux non urgents et refus des sous-traitants non essentiels;
- Restriction des accès pour les livreurs;
- Plexiglas dans les camions des livreurs (lorsqu'ils sont 2 livreurs par camion);
- Plexiglas à la réception et dans les bureaux de services aux employés (RH, paie, etc.);
- Mise en place d'un plexiglas au comptoir des ventes;
- Modification des horaires pour avoir des équipes fixes qui ne se croisent pas;
- Espacement de 20 minutes entre le quart de jour et de soir;
- Ouverture d'une deuxième cafétéria et places attribuées par équipe dans les différentes cafétérias pour minimiser les contacts entre les équipes;
- Modifications du cheminement pour l'accès à l'usine selon les différents départements pour minimiser les croisements;
- Ajout d'un micro-onde à l'administration et d'une nouvelle section de bureau;
- Plexiglas emballage maturé et tranché;
- Port de visière pour les employés d'usine, les livreurs et les employés de maintenance pour accroître la protection lorsque la distance minimale de 2 mètres est difficile à respecter;
- Retrait de 14 jours en cas de rassemblement en dehors du travail;
- Mesures de déplacements et gestion des documents pour le service à la clientèle;
- Réaménagement des bureaux pour séparer les équipes et les gens avec des postes clés (protéger les substituts).

Mesures de protection complémentaires

- Ajout d'un contremaître pour faire respecter les mesures dans l'usine;
- Retrait des ustensiles en plastique, bâtons à café et assiettes de carton;
- Retrait des machines à bonbons;
- Paiement par carte seulement et les clients scannent eux-mêmes leurs items;
- Retrait des portes des abris à neige pour éviter d'autres contacts inutiles;
- Les portes entre les différentes sections de bureaux et les corridors sont maintenues ouvertes lorsque possible.

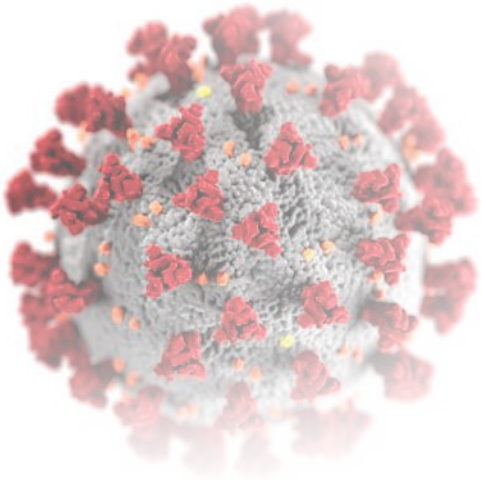
Gestion de crise

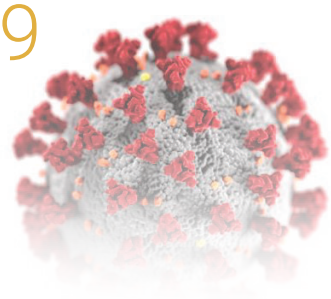
- Mise en place d'une équipe de gestion comprenant des membres de plusieurs départements;
- Rencontres quotidiennes par Skype de cette équipe pour discuter des enjeux et mesures prises ou à prendre;
- Élaboration d'un plan d'action dans l'éventualité d'un cas positif au sein de l'entreprise (identification des actions à prendre, des rôles et responsabilités de chaque membre de l'équipe);
- Communications avec les employés via plusieurs canaux (communiqués officiels affichés sur le babillard et diffusés sur le Facebook des employés, diffusion des consignes sur une télévision à la cafétéria, rappels réguliers des consignes par les superviseurs, etc.).

Écrivez-nous à partagecovid19@ars-solutions.ca.

Si vous avez des mesures de sécurité supplémentaires que vous aimeriez nous partager, nous nous engageons à les transmettre à notre clientèle et au reste de la communauté. ***C'est en unissant nos forces que nous passerons à travers cette crise.*** *Pour assurer une reprise économique sécuritaire, on se doit d'établir un maximum de mesures préventives adaptées à notre environnement.* ***En sécurisant nos méthodes de travail, on protège ainsi notre main d'œuvre.*** *Il faut le voir comme un investissement à plus ou moins long terme pour la continuité de nos activités.*

Les cyberattaques ont augmenté de 400 % depuis la COVID-19





TEMPS DE LECTURE 4:00

Les cybercrimes signalés au Centre de plaintes pour les crimes sur Internet (IC3) du Federal Bureau of Investigation (FBI) ont à peu près quadruplé depuis la pandémie du coronavirus, a déclaré un haut responsable de la cybersécurité lors d'un webinaire organisé par l'Institut Aspen.

Le nombre de plaintes en lien avec la cybersécurité adressées à l'IC3 au cours des quatre derniers mois est passé de **1 000 par jour avant la pandémie à pas moins de 4 000 incidents en une journée**, a déclaré Tonya Ugoretz, directrice adjointe de la branche cybernétique du FBI, selon The Hill.

Il s'agit surtout de cybercriminels qui s'en prennent aux organisations, telles que les établissements de soins de santé et les instituts de recherche qui travaillent sur les traitements contre la COVID-19, a déclaré madame Ugoretz. **« Nous avons eu plusieurs cas d'intrusion dans certaines de ces institutions, en particulier celles qui se sont publiquement identifiées comme travaillant sur la recherche liée à la COVID »**, a-t-elle déclaré. Bien qu'il ne soit pas rare que les malfaiteurs ciblent l'industrie biopharmaceutique, « cela s'est certainement intensifié pendant la crise », a déclaré la responsable du FBI.

Les organisations qui font des recherches sur des médicaments potentiels pour traiter ou vacciner les victimes du COVID-19 sont maintenant plus visibles aux yeux du public, ce qui les rendent d'ailleurs très attrayantes pour les autres états qui sont intéressés à obtenir des détails sur ce qu'ils font exactement et peut-être même à voler des informations exclusives que ces institutions ont. **« Les pays ont un très grand intérêt pour les informations sur un vaccin »**, ajoute Mme Ugoretz.

Un certain nombre de cas a fait surface au cours des deux derniers mois. **En mars dernier, des cybercriminels ont attaqué à 10 reprises Genomics, un groupe de recherche en biotechnologie basé à Pleasanton, en Californie**, qui s'efforce de comprendre la réponse immunitaire du corps humain pour accélérer le développement d'un vaccin contre la COVID-19. En état d'alerte, **Microsoft a même demandé à plusieurs douzaines d'hôpitaux de corriger immédiatement les faiblesses de leurs installations VPN** après avoir trouvé des preuves qu'une équipe de rançon cherchait des failles à exploiter.

L'Organisation mondiale de la santé (OMS) et le département de la Santé et des Services sociaux des États-Unis (HHS) n'ont pas non plus été épargnés par les malfaiteurs. Des hameçonneurs soutenus par l'Iran seraient impliqués dans une tentative de détournement des comptes de messagerie personnels d'un certain nombre de membres du personnel de l'OMS. Il s'agit d'ailleurs de la deuxième cyberattaque liée à l'OMS au cours des dernières semaines. **Une équipe de cybercriminels a tenté à plusieurs reprises de s'introduire dans le réseau de l'OMS.**

À la mi-mars, les fraudeurs du HHS ont également utilisé de faux messages textuels pour informer les gens sur le développement de la COVID-19… Cette menace est mondiale et peut toucher n'importe qui donc il est important de redoubler de vigilance. Demeurez attentif et réfléchissez avant de cliquer sur un message douteux, surtout s'il est en lien avec la pandémie, car vous pourriez rapidement vous retrouver parmi les victimes.

N'hésitez pas à nous contacter si vous souhaitez valider la légitimité d'un courriel.

3 conseils
pour un télétravail sécuritaire

TEMPS DE LECTURE 3:00

Il est essentiel de toujours garder une longueur d'avance sur les cybercriminels, même lorsque vous travaillez à domicile pendant la pandémie. Voici 3 conseils pour protéger votre organisation lorsque votre personnel est en télétravail :

1.

Améliorez votre stratégie de mots de passe

Lors d'une crise mondiale comme une pandémie ou une catastrophe naturelle de grande ampleur, **vos mots de passe pourraient faire la différence entre investir de votre temps dans la relance et la croissance de votre entreprise OU dans la récupération de données piratées. Revoyez vos mots de passe actuels et informez votre équipe afin de créer des mots de passe plus forts et plus complexes qui ne peuvent pas être facilement devinés** (au moins 8 caractères avec des lettres majuscules et minuscules, des chiffres et des symboles). Ne rendez pas les choses faciles, en utilisant par exemple "Motdepasse123!". Bien que cela réponde techniquement aux exigences, un cybercriminel pourrait facilement le craquer. **Utilisez un gestionnaire de mots de passe pour garder tous vos mots de passe au même endroit.** Ne les conservez pas dans votre navigateur Web juste parce que c'est pratique ni dans votre cellulaire. Ils sont également faciles à pirater.

2.

Veillez à la sécurité dans le Cloud

Si vous utilisez des applications Cloud alors que vos employés travaillent à domicile, il est essentiel de vous préoccuper de la confidentialité et de la sécurité des données. **L'entreprise qui héberge vos données est responsable en dernier ressort de la protection de son réseau contre les cybercriminels, mais la plupart des violations sont dues à une ERREUR DE L'UTILISATEUR.** Il est donc de votre devoir de **veiller à la sécurité dans le Cloud. Maintenez un mot de passe FORT et assurez-vous que le dispositif que vous utilisez pour accéder à l'application est sécurisé.** Vous aurez besoin de l'aide d'un spécialiste des TI pour bien configurer le pare-feu, l'antivirus et un logiciel de filtrage du spam solides. **Important!** N'accédez pas à vos applications Cloud avec un appareil que vous utilisez également pour vérifier les sites de médias sociaux et les comptes de messagerie gratuits. **Sauvegardez vos données.** Si les données dans le Cloud sont importantes, assurez-vous que vous les téléchargez depuis l'application et que vous les sauvegardez dans un autre endroit sûr et sécurisé. Si votre compte est piraté OU si l'entreprise d'hébergement ferme votre compte, vous en aurez une copie.

3.

Faites attention aux applications de stockage comme Dropbox

Lorsque les employés travaillent à domicile, ils doivent avoir accès aux dossiers importants de l'entreprise. S'ils doivent envoyer un fichier, mais qu'il est trop volumineux pour procéder, le premier réflexe est souvent de télécharger la version gratuite de Dropbox pour y arriver. Cependant, **les applications gratuites de partage comme celle-ci viennent avec un prix : la sécurité.** De plus en plus utilisés, ces outils représentent **un risque évident pour le vol de données et d'informations personnelles,** car ces dernières se retrouvent n'importe où, et ce, avec un faible niveau de sécurité. **Une fois que vos données sont transférées sur ce genre de plateforme, elles deviennent incontrôlables.** Même si vous les supprimez, elles ne le sont jamais réellement. Si vous avez un fichier lourd à envoyer ou souhaitez continuer un travail à la maison, **le VPN (Virtual Private Network) est l'option la plus recommandée.** Il existe également des systèmes de transfert de données comme FTP (File Transfer Protocol). Si vous souhaitez absolument rester dans le Cloud, optez pour des alternatives plus sécuritaires comme **OneDrive de Microsoft, Google Drive ou même WeTransfer Plus** qui permet de protéger vos transferts par mots de passe et de fixer la date d'expiration de ceux-ci.

En résumé, même si certaines applications sont faciles d'utilisation et très abordables, ne les utilisez pas pour stocker vos données sensibles. **La sécurité est l'affaire de tous en entreprise...**

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