Mai 2019 • Vol. 6 n° 5

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies

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

5 autres études de cas d'entreprises de chez nous à venir

« Depuis ARS, je dors tranquille...

J'ai un œil externe sur la réalité et les défis auxquels nous faisons face dans notre champ d'expertise et je suis confiant que, quand je me couche le soir, quelqu'un veille sur nos opérations et prend les alertes en charge.

L'équipe d'ARS a toujours été présente, à l'écoute de nos inquiétudes et a toujours su s'adapter à notre réalité. Nous avons de moins en moins d'appels et de points à régler. Tout est stable et sous contrôle. »

Stéphane Lapierre
Directeur du développement logiciel
Signalisation Ver-Mac

Suivez-nous

Une perte de plus de 250 000 $ POUR UNE ENTREPRISE QUÉBÉCOISE VICTIME D'UNE CYBERATTAQUE

TEMPS DE LECTURE 4:00

Une entreprise de 350 employés s'est fait voler certaines informations clés importantes par une firme d'envergure internationale dont le modèle d'affaires repose sur le vol de données. La firme lui demandait un équivalent d'un quart de millions de dollars en Bitcoins !

Le problème a été détecté le samedi 9 mars vers 5 h du matin lorsqu'un employé est rentré travailler. **Tous les ordinateurs étaient bloqués et affichaient un message de rançon.** Le directeur TI a commencé à diagnostiquer le virus à distance afin de voir s'il pouvait rétablir la situation, mais en vain.

« J'ai banalisé la situation à ce moment-là, car avoir des interruptions de systèmes à cause d'un virus, c'est chose courante », avoue le vice-président de l'entreprise, qui a préféré garder l'anonymat.

SUITE À LA PAGE 2 ▼

SUITE DE LA PAGE 1 ▲

DES CONSÉQUENCES FINANCIÈRES IMPORTANTES

L'équipe en place s'est rapidement retrouvée dépassée par les événements. L'ensemble des données opérationnelles de l'entreprise était crypté : serveur Exchange, documents, copies de sécurité, etc. **Toutes les succursales étaient touchées.** Aucun employé ne pouvait recevoir ou même envoyer de courriels. Ils devaient communiquer par texto, mais n'avaient pas les coordonnées de tous.

« J'évalue nos pertes financières à au moins 250 000 $ », mentionne le vice-président qui espère obtenir un montant de 125 000 $ de sa compagnie d'assurance. « On a peut-être perdu des clients au profit de la compétition, je dois terminer mon analyse » ajoute-t-il. Heureusement, les données critiques financières n'ont pas été impactées parce qu'elles sont hébergées à l'externe et protégées par les systèmes et la sécurité du fournisseur.

NÉGOCIER OU REBÂTIR ?

Après plusieurs recherches, l'entreprise victime découvre que la firme responsable est en fait un organisme sérieux d'envergure internationale, bien organisé, et dont le modèle d'affaires repose sur le vol de données.

« On avait 2 options : embaucher un médiateur pour négocier la rançon pour nous sur le Dark Web ou rebâtir notre infrastructure à partir de nos copies de sécurité. On a fait le choix de mener les deux options en parallèle afin de se garder une porte de sortie pour récupérer les données cryptées en payant la rançon advenant le cas où la récupération des backups ne soit pas optimale », souligne le vice-président.

UN MOIS POUR SE REMETTRE EN FONCTION

« On a été en gestion de crise pendant 2 semaines. Après 5 jours, 80 % de nos opérations étaient en place pour se dépanner. **4 semaines de stress intense.** Tu ne peux pas faire ton travail de gestionnaire pendant ce temps-là » se confie le vice-président. **« On a fonctionné sur le café et mon directeur TI est parti en "burn-out". On ne peut pas tenir trop longtemps à ce rythme, surtout pour une grande organisation comme la nôtre »**, ajoute le vice-président qui n'a pas l'intention de revivre cette situation.

LA VULNÉRABILITÉ DES GESTIONNAIRES FACE AUX TI

« En tant que gestionnaire, on doit comprendre ce qui se passe dans nos TI, connaître notre infrastructure et la documenter pour savoir ce qu'on a en place. », mentionne le vice-président qui vise maintenant l'impartition.

De plus, l'entreprise n'avait rien planifié en cas de situation d'urgence et savait que les capacités de son équipe TI étaient limitées. Les informations sur lesquelles la direction s'est basée pour décider de rebâtir l'infrastructure étaient erronées. Les copies de sécurité récupérables n'avaient pas bien été gérées ni entretenues. Plusieurs mois de données ont été perdus.

IMPARTITION ET PRÉVENTION

« On doit se poser la question si ça vaut la peine d'avoir une équipe et un directeur TI à l'interne parce que, souvent, ces gens ne sont pas bien formés. Pour moi, il y a 4 volets importants : la sécurité, l'infrastructure, le support aux usagers et la stratégie. **À mon sens, ils peuvent tous être impartis pour que les gestionnaires focalisent à la bonne place.** », partage le vice-président qui considère également important de faire de la prévention auprès de ses employés. « Ils sont responsables de 99 % des failles, courriels d'hameçonnage, installation d'un logiciel malveillant, etc. ».

Ce dernier a bien l'intention de réaliser une campagne de prévention auprès de ses employés avec des tests d'hameçonnage ciblés ainsi que des tests d'intrusion.

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

Quels sont les risques d'utiliser DROPBOX ET AUTRES APPLICATIONS DE STOCKAGE DANS LE CLOUD ?

En utilisant des logiciels gratuits de partage de fichiers pour votre entreprise, vous augmentez de beaucoup les risques de vol d'informations, le saviez-vous ?

TEMPS DE LECTURE 2:45

Il faut faire attention aux types de données que nous stockons sur ce genre de services de partage de fichiers. Ils devraient seulement être utilisés pour héberger des informations publiques, comme celles que vous mettriez sur votre site Web par exemple. Sachez toutefois que **vous serez assujetti au profilage de données, soit le traitement automatisé de vos informations**. Celles-ci seront utilisées pour analyser ou prédire vos intérêts, votre comportement et d'autres de vos attributs à des fins de marketing.

Les logiciels gratuits de partage représentent également une porte d'entrée facile pour les pirates. Plus ils sont populaires, plus la surface d'attaque devient importante, notamment lorsqu'il est question d'espionnage industriel. Dropbox fait d'ailleurs partie de ceux qui se sont fait pirater à plusieurs reprises…

À titre d'exemple, plus de 68 millions de comptes Dropbox ont été piratés suite à un incident de sécurité survenu en 2012. Et ce n'est qu'en 2016 que Dropbox a reconnu avoir été victime de cette attaque d'envergure, soit 4 ans plus tard ! Pas très rassurant, n'est-ce pas ?

AUCUN CONTRÔLE SUR LES DONNÉES STOCKÉES

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 plateformes, elles deviennent incontrôlables. Même si vous les supprimez, elles ne le sont jamais réellement.**

Lorsqu'on veut 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**.

VOICI CE QUE VOUS POUVEZ FAIRE

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 de Google 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...

7 RAISONS D'IMPLIQUER VOTRE FOURNISSEUR TI avant de passer à la téléphonie IP

TEMPS DE LECTURE 3:15

La téléphonie IP, bien que très bénéfique pour une entreprise, peut amener des problématiques complexes à gérer en cours d'implantation. En effet, cette technologie a un impact direct sur le réseau informatique et peut nuire à sa performance. Voilà pourquoi il est important d'impliquer son fournisseur TI dès le début du projet pour évaluer les risques.

La téléphonie IP, aussi appelée VoIP, consiste à effectuer ou recevoir un appel via une connexion Internet. Comme la téléphonie IP passe par le réseau, ils ont tous les deux un impact interchangeable. L'un peut diminuer l'efficacité de l'autre et vice versa, car ils sont interdépendants. **Si vous songez à vous tourner vers cette technologie, pensez d'abord à en informer votre fournisseur TI.** Ce dernier devrait normalement être en mesure de planifier votre projet de téléphonie IP en coordination avec les impacts sur votre réseau. Vous éviterez ainsi les problèmes non planifiés qui pourraient devenir très coûteux à régler et de devenir l'intermédiaire entre deux fournisseurs qui se lancent la balle…

VOICI 7 RAISONS D'IMPLIQUER VOTRE FOURNISSEUR TI DANS LE DÉROULEMENT DE VOTRE PROJET :

1 **Vous aider à faire votre choix.** Impliquer votre partenaire TI aide à choisir la technologie IP et le fournisseur qui conviennent le mieux à vos besoins. En tant que fournisseur de services, il saura vous conseiller grâce à sa connaissance du milieu et de ses contacts.

2 **Préserver la stabilité et la performance** de votre environnement. Un projet mal planifié pourrait déstabiliser votre environnement TI et votre fournisseur de téléphonie IP ne pourrait rien y faire.

3 **Prévenir des problématiques complexes.** Il est presque impossible de revenir en arrière suite à l'implantation. Ça peut prendre de 7 à 14 jours pour autoriser un transfert de ligne d'un fournisseur à un autre. On doit toutefois corriger les problèmes immédiatement (ex. : déconnexions, lenteurs, etc.) Un centre d'appel 24/7 ne peut se permettre ce genre de situation.

4 **Fiabilité de la téléphonie** puisque tout sera bien planifié dès le départ. Ainsi, vous ne mettrez pas à risque la qualité de votre service client puisque la téléphonie sera harmonisée au réseau de votre entreprise, de sorte que les deux s'arriment parfaitement sans avoir le moindre impact négatif l'un sur l'autre.

5 **Gagner du temps** en coordination et gestion de projet. Vous évitez les désagréments de la gestion d'un projet qui implique plusieurs technologies et fournisseurs.

6 **Contrôle d'anomalies suite au projet.** Si l'on implique son fournisseur TI immédiatement, on peut facilement sauver 50 % des coûts reliés à d'éventuels problèmes après l'implantation.

7 **Sauver des coûts** en temps, en délais et en erreurs.

Il va toujours y avoir des ajustements à faire. C'est normal puisque les systèmes sont de plus en plus sophistiqués. Par exemple, avec les anciens téléphones cellulaires, on n'avait qu'à appuyer sur les boutons des numéros et c'était tout. Maintenant, sur nos téléphones intelligents, on a accès à Internet, on a le Wi-Fi, on lit nos courriels, etc. C'est un véritable ordinateur. Avec la téléphonie, c'est le même principe. C'est un projet important pour toute entreprise et il ne doit pas être pris à la légère.

N'hésitez pas à demander de l'aide. Cette démarche se doit toutefois d'être faite dès le début pour une meilleure planification ainsi que pour éviter d'éventuels problèmes.

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