PASSION AFFAIRES et technologies

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

ARS solutions 25 ans

Vol. 3 nº 5. Mai 2016

L'aspect légal du Cloud : quoi évaluer ?

(Première partie)

TEMPS DE LECTURE 3:45

Écrit par Me Benoît Trotier, spécialiste en droit des technologies et Internet, Joli-Cœur, Lacasse, avocats

L'attrait du Cloud permettant l'accessibilité de vos données en tout temps par Internet, une solution logicielle mise à jour en continu et des frais reliés à votre consommation est bien réel et tôt ou tard vous aurez à décider si vous faites le saut avec vos données d'entreprise.

Prenez en considération les éléments suivants pour assurer la sécurité physique et légale de vos données confiées à un fournisseur Cloud :

A ÉVALUEZ OBJECTIVEMENT LA SENSIBILITÉ DES DONNÉES QUE VOUS VOUS APPRÊTEZ À FAIRE HÉBERGER SUR L'INFRASTRUCTURE INFORMATIQUE D'UN TIERS.

L'évaluation de la sensibilité des données que vous proposez de mettre dans le Cloud est un exercice absolument fondamental à la sécurité de l'opération et à une prise de décision éclairée pour l'usage du Cloud public pour votre entreprise. Pouvez-vous vous permettre la perte, l'accès illicite ou la divulgation, par exemple, de vos données stratégiques, de vos recettes industrielles, du vol de numéros de cartes de crédit de vos clients ou des numéros d'assurance sociale ou des données médicales que vous auriez pu colliger entre autres sur vos employés ?

SUITE À LA PAGE 2 ▼

SPÉCIAL SÉCURITÉ

RAPPORT SUR LA SÉCURITÉ

Saviez-vous que la moitié des cyberattaques vous sont destinées ?

Une PME sur cinq a été victime de cybercriminalité au cours de la dernière année.

La suite en page 2

Suivez-nous

SUITE DE LA PAGE 1 ▲

Considérez le Cloud public pour des données de faible à moyenne sensibilité, d'autant que les serveurs informatiques du fournisseur sont offerts en mode multi-locataires et que vous n'êtes pas à l'abri d'une divulgation inattendue de vos données à un colocataire. Sur ce point, vérifiez que votre fournisseur a des mesures concrètes de ségrégation des données entre locataires. Les données de sensibilité critiques sont encore mieux hébergées sur un serveur sécurisé à l'interne, à moins de pouvoir vous payer un Cloud privé à même votre organisation, mais les coûts ne sont plus les mêmes.

B EXIGEZ L'ENCRYPTION DE VOS DONNÉES PENDANT LE TRANSPORT ET AUSSI AU REPOS SUR LES SERVEURS DU FOURNISSEUR CLOUD.

Vérifiez que le fournisseur protège vos données pendant leur transport sur Internet via le protocole SSL et possède un certificat de haut niveau (le plus élevé étant de 2048 bits). Vérifiez que le fournisseur offre aussi l'encryption des données au repos sur ses serveurs et quelle est la norme applicable, par exemple, la norme AES-256 ou du moins, s'il vous permet d'utiliser des outils externes vous permettant d'encrypter vos données sur ses serveurs...

C VÉRIFIEZ LA RÉPUTATION ET LES CERTIFICATIONS INTERNATIONALES DU FOURNISSEUR.

« Googlez » le nom de votre fournisseur et vérifiez les derniers incidents rapportés qui le concernent. A-t-il bien réagi et supporté sa clientèle ? Est-il critiqué de toute part ou poursuivi par les autorités compétentes ?

Examinez avec le plus grand soin les accréditations internationales que possède votre fournisseur. Par exemple de type ISO 27002 sur les contrôles de sécurité des systèmes informatiques ou de type SSAE16 s'il traite pour vous des données financières. Ou mieux encore, s'il détient les toutes nouvelles normes de gestion spécialement édictées en 2014 pour les fournisseurs de services Cloud : soit la norme ISO 27017 relative aux contrôles de sécurité pour les fournisseurs Cloud ou la norme ISO 27018 visant la protection des renseignements personnels par un fournisseur Cloud et qui répond à la majorité des problématiques touchant la protection des renseignements personnels dont vous êtes responsables en tout temps malgré votre impartition dans le Cloud. À tout événement, ces certifications font l'objet d'un audit externe annuel pour être maintenues. Exigez d'en recevoir copie chaque année, quitte à signer une entente de confidentialité avec le fournisseur pour les obtenir. Vous verrez ainsi **s'il y a eu des problématiques sur son infrastructure ou sa gestion des incidents en cours d'année et si le fournisseur a su corriger la situation à la satisfaction de l'organisme certificateur**.

La suite dans la prochaine édition.

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

TEMPS DE LECTURE 3:00

Conséquemment, 500 millions d'identités ont été volées ou exposées en ligne en 2015 selon le rapport de Symantec[1] – le leader mondial en sécurité informatique, soit une augmentation de 36 % comparativement à 2014.

Le Royaume-Uni est classé comme étant le pays le plus touché par les attaques de *spear phishing*[2] qui consistent à voler des données en ciblant des employés au sein d'une organisation spécifique. Ce type d'attaque a augmenté de 55 % en 2015. Et lorsqu'il est question d'escroqueries au niveau du support technique et de médias sociaux, il est le deuxième pays le plus ciblé à l'échelle mondiale.

Le logiciel Adobe Flash Player – un logiciel installé sur plus d'un milliard de postes est le logiciel le plus prisé par les pirates informatiques.

Symantec a porté une attention particulière à l'augmentation des *zero-day vulnerabilities* en 2015. Ce terme fait référence à une faiblesse ou un bogue dans une partie d'un logiciel qui est identifié et exploité par des pirates avant que le fabricant ne puisse corriger l'erreur. En 2015, la compagnie a identifié 54 *zero-day vulnerabilities*.

En moyenne, chaque faille de données expose plus de 1.3 million d'identités, mais Symantec a identifié 9 brèches majeures qui ont permis d'extraire plus de 10 millions d'enregistrements dans une seule attaque en 2015.

Lors de la célèbre attaque d'*Ashley Madison* (un site de rencontre en ligne) en juillet, les informations personnelles (nom des clients, adresse, numéro de carte de crédit, etc.) de 32 millions d'usagers ont été volées et mises en ligne en plus de 30 GB de renseignements relatifs à des courriels et documents de la compagnie. En octobre, les pirates ont volé 15 millions d'informations personnelles sur les clients de T-Mobile selon l'agence de crédit *Experian*.

Le plus grand défi des professionnels est donc d'être constamment formé et informé et d'avoir des outils à jour pour contrecarrer les attaques.

Ces chiffres permettent de mieux comprendre l'ampleur du phénomène de la cybercriminalité et nous donnent une idée du combat qui perdure entre les spécialistes en sécurité et les pirates informatiques.

L'idée d'avoir une approche globale par rapport à la sécurité ne se résume pas seulement par la mise à jour d'antivirus et la mise en place de mots de passe complexes.

Mettre sur pied un programme de maintenance quant à la sécurité rend l'entreprise moins vulnérable et améliore les chances de s'en sortir sans trop de dommage advenant le cas où l'entreprise serait victime de cybercriminalité. Cependant, même avec tous les efforts nécessaires, il est faux de prétendre qu'elle est sécurisée à 100 %, car les cybercriminels ont toujours une longueur d'avance en ce sens qu'ils sont initiateurs des attaques.

[1] **Symantec** est le leader mondial du marché en matière de sécurité des terminaux client et du courrier électronique, de prévention contre la perte de données et de certificats SSL (source : www.symantec.com/fr/ca).

[2] Le ***spear phishing*** désigne en sécurité informatique une variante de l'hameçonnage. Contrairement à l'hameçonnage traditionnel basé sur l'envoi d'un message générique à un grand nombre de destinataires, le *spear phishing* se focalise sur un nombre limité d'utilisateurs (souvent un seul) auxquels est envoyé un message fortement personnalisé (source : Wikipedia).

TEMPS DE LECTURE 2:00

La collaboration en entreprise selon Microsoft

Quand vient le temps d'utiliser les technologies pour améliorer la collaboration des individus dans l'entreprise, on fait souvent référence aux outils de productivité développés par Microsoft. **Outlook, SharePoint, Skype et Office 365 figurent parmi les applications collaboratives les plus utilisées aujourd'hui.**

Selon le directeur sénior d'Office 365 – Bryan Goode, voici la vision de l'entreprise quant à la collaboration virtuelle de demain.

Lorsqu'on parle d'outils de productivité en l'entreprise, il est maintenant question de concepts tels que les équipes dynamiques.

Auparavant, un espace de collaboration commun consistait à partager des fichiers, des courriels ou à avoir un portail d'équipe. Aujourd'hui, ce temps est révolu. Avec le groupe Office 365, Microsoft a changé sa vision de la collaboration pour un modèle de type réseau en étoile (***hub and spoke***), c'est-à-dire que l'équipe devient le noyau (*hub*) et les branches (*spoke*) sont reliées à des applications, des documents et des données de l'entreprise dont les fonctions consistent en l'entreposage, la recherche, la découverte, etc.

Selon Bryan Goode, la collaboration ne se résume pas à un seul outil. Le modèle réseau en étoile de Microsoft permet une expérience plus connectée et les équipes peuvent désormais utiliser des applications qu'elles apprécient dans leur espace de travail.

VOICI LES 7 OUTILS DE COLLABORATION DÉVELOPPÉS PAR MICROSOFT

1 **Office 365 :** Éditeur et créateur de documents

2 **Skype :** Chat, vidéos, réunions, partage de fichiers

3 **Outlook :** Courriels et calendrier

4 **Sharepoint :** Intranet et créateur de sites web

5 **Yammer :** Réseau social privé pour entreprise

6 **OneDrive :** Service de stockage Cloud

7 **Delve :** Outil de statistiques et d'analyse

Dans l'ensemble, Microsoft poursuit sa quête d'avoir une collaboration virtuelle plus compréhensive et mature. Elle offre de meilleurs choix et des solutions plus adaptées à la réalité des équipes de travail d'aujourd'hui.

Référence : ZDNet

TEMPS DE LECTURE 3:00

5 vidéos hyper inspirantes pour *booster* votre productivité

Atteindre la productivité optimale est chose possible et il ne s'agit pas de travailler plus fort, mais de travailler plus intelligemment et de savoir en tirer profit chaque jour. Pour ce faire, il faut parfois penser d'une tout autre manière...

Les ***TED talks*** (Technology, Entertainment and Design) sont une série internationale de conférences organisées pour transmettre des « **idées qui valent la peine d'être diffusées** ». Les exposés couvrent un large éventail de sujets et les conférenciers – véritables sommités dans leur domaine, sont issus d'une grande variété de disciplines.

VOICI 5 *TED TALKS* QUI VOUS OFFRIRONT DES LEÇONS TRÈS INSPIRANTES ET PRÉCIEUSES À CE NIVEAU.

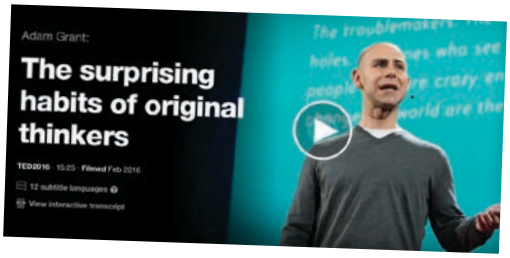
1 **Yves Morieux's**
How too many rules at work keep you from getting things done
Le marché du travail d'aujourd'hui exige d'être flexible, collaboratif et de résoudre des problèmes chaque jour. Comme le démontre Yves Morieux, trop souvent, une surcharge de règles et de processus nous empêche de faire notre travail ensemble. Dans cette vidéo, rencontrez la nouvelle frontière de la productivité : la collaboration.

2 **Arianna Huffington's**
How to succeed? Get more sleep

On dit qu'une bonne nuit de sommeil a le pouvoir d'augmenter la productivité, le bonheur et permet de prendre de meilleures décisions. Mais la cofondatrice et éditrice en chef du *Huffington Post* – Arianna Huffington, pense que cela peut conduire à de bien plus grandes choses que cela...

3 **Margaret Heffernan's**
Dare to disagree
La plupart des gens s'éloignent instinctivement des conflits, mais comme le souligne Margaret Heffernan, être en désaccord est le centre du progrès.

4 **Adam Grant's**
The surprising habits of original thinkers
Comment les gens créatifs en viennent à avoir de bonnes idées ? Adam Grant – auteur du livre *originals*, professeur et psychologue organisationnel a quelques conseils inspirants pour vous.



5 **Shawn Achor's**
The happy secret to better work
En tant que CEO de *Good Think Inc.*, psychologue et auteure du livre *The happiness Advantage*, Achor a passé beaucoup de temps à chercher où le potentiel humain, le succès et le bonheur se croisent. Nous pensons souvent qu'il faut travailler fort pour être heureux, mais qu'en est-il du contraire ?

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