PASSION AFFAIRES et technologies

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

ARS solutions 25 ans

Vol. 3 nº 6. Juin 2016

L'aspect légal du Cloud : quoi évaluer ?

(Deuxième partie)

TEMPS DE LECTURE 4:15

Écrit en collaboration avec 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.

Voici la suite des éléments à prendre en considération pour assurer la sécurité physique et légale de vos données confiées à un fournisseur Cloud.

N.B. : Les points A à C de cet article ont été abordés dans l'édition de mai 2016.

D VÉRIFIEZ ATTENTIVEMENT LES PROCESSUS DE GESTION DES INCIDENTS DE SÉCURITÉ INFORMATIQUE DU FOURNISSEUR.

Quelles sont les mesures prises par le fournisseur en cas de perte de données ou d'accès ou de communication non autorisés ? Quelles sont les mesures de signalement des incidents de sécurité à vos données ? Rappelez-vous que sous peu, la nouvelle loi fédérale sur la **« Protection des renseignements numériques »** exigera que vous mainteniez (via votre fournisseur Cloud) des registres des incidents de sécurité aux données personnelles que vous possédez et que vous divulguiez clairement l'atteinte à la sécurité des données dès que possible aux personnes susceptibles de subir un préjudice grave et à tout organisme permettant de diminuer le risque de préjudice (ex. la police), à défaut de quoi vous pourriez subir des amendes importantes allant jusqu'à 10 000 $ dans le cas d'une poursuite pénale ou à 100 000 $ dans le cas d'une poursuite pour acte criminel. Vérifiez attentivement quel est le plan de reprise du fournisseur après sinistre et quels sont les processus et délais appréhendés pour vous permettre de reprendre vos activités courantes. C'est ici que la norme ISO 2018 prend son importance alors que les engagements de divulgation des incidents aux renseignements personnels sont bien établis.

SUITE À LA PAGE 2 ▼

SPÉCIAL SÉCURITÉ

Rapport sur la sécurité

Vos employés utilisent-ils leur *smartphone* au travail ?

Cette tendance a considérablement augmenté la complexité de maintenir un réseau et vos données d'entreprise sécuritaires.

Si vous laissez vos employés utiliser des appareils personnels, vous devez vous assurer que ces dispositifs soient correctement **sécurisés, monitorés et entretenus** par un professionnel.

Et que faire en cas de départ ?

Découvrez TOUT ce que vous devez savoir à ce sujet dans notre rapport sur la sécurité.

ars-solutions.ca/protectionscritiques

Suivez-nous

SUITE DE LA PAGE 1 ▲

E GARDEZ LE CONTRÔLE DE VOS DONNÉES DANS LE CONTRAT.

Stipulez dans le contrat que vous êtes le seul et entier propriétaire de données hébergées sur les serveurs du fournisseur Cloud et que lui et ses sous-traitants n'ont droit d'accès qu'uniquement pour donner le service promis ou assurer le support ou la maintenance du système. Stipulez que le fournisseur et ses sous-traitants ne sont pas autorisés à faire aucun usage secondaire des données hébergées ou des données système générées, par exemple, par les requêtes faites par les utilisateurs, ni à les vendre à autrui. Ne permettez au besoin qu'un usage de données anonymes aux fins du fournisseur.

F ASSUREZ-VOUS DE SAVOIR DANS QUELLE JURIDICTION SONT VOS DONNÉES EN TOUT TEMPS.

Vos données peuvent être sauvegardées à l'étranger, par exemple, sur des serveurs redondants du fournisseur et il importe que vous sachiez dans quelle juridiction se trouvent vos données en tout temps. Vous devez vous informer sur la réglementation applicable en matière de protection des renseignements personnels dans ces juridictions pour répondre aux exigences de la réglementation canadienne et québécoise qui interdisent le transfert de données personnelles dans des juridictions qui n'offrent pas une protection similaire aux lois canadiennes et québécoises en cette matière. Il importe donc d'éviter des juridictions « exotiques » et que vous ayez une bonne idée des entités étrangères qui pourraient avoir accès à vos données.

G ASSUREZ-VOUS DE POUVOIR RÉCUPÉRER EFFICACEMENT VOS DONNÉES ET QUE CELLES-CI SOIENT EFFACÉES DE FAÇON PERMANENTE DE TOUTE L'INFRASTRUCTURE DU FOURNISSEUR CLOUD.

Que ce soit en cas de faillite du fournisseur ou à l'expiration du contrat Cloud, vérifiez attentivement le délai qui vous est alloué pour récupérer vos données, dans quel format celles-ci vous seront remises : dans leur format original, dans une version propriétaire du fournisseur qui va exiger des frais et délais de conversion, quelle assistance sans frais le fournisseur est-il prêt à rendre ? Assurez-vous que le fournisseur s'engage à utiliser des normes reconnues de destruction de vos données après votre migration non seulement de son centre de données principal, mais dans toute son infrastructure, incluant ses centres à l'étranger.

Rappelez-vous que le Cloud public est un modèle d'affaires qui n'est pas encore arrivé à parfaite maturité. Recherchez des fournisseurs canadiens et québécois qui ont des infrastructures de qualité et des hauts standards de gouvernance. Comme pour le reste, la sécurité se paye. Privilégiez les compagnies réputées si vous êtes pour mettre vos données d'affaires dans les mains d'un tiers. Assurez-vous aussi d'un plan B au besoin et gardez une copie régulière de vos données, à jour et exploitables à l'interne, pour assurer vos arrières et la pérennité de vos activités.

Pour lire l'article intégral, téléchargez gratuitement notre rapport sur la sécurité.

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

La vulnérabilité des sites Internet intéresse les *hackers*

TEMPS DE LECTURE 3:15

De nos jours, gérer une entreprise implique d'avoir un ou plusieurs sites Internet extérieurs. Que ce soit un site de cybercommerce où les clients peuvent faire des achats, une plate-forme de médias sociaux où les gens peuvent se connecter, ou un portail Web pour les employés, il doit y avoir une interface permettant aux gens d'interagir avec votre organisation par le biais des réseaux publics. Et qui dit interface, dit accès facile à des informations sensibles et donc intéressant pour les pirates informatiques.

LES SITES INTERNET : L'UN DES MAILLONS FAIBLES DE LA CHAÎNE

Les réseaux d'entreprises peuvent être infiltrés de différentes manières. Une mauvaise configuration des équipements et/ou des logiciels et la non-application des mises à jour représentent des failles facilement exploitables par les pirates – plaçant ainsi le réseau dans un état de vulnérabilité. Et certaines de ces failles exigent un haut niveau d'expertise et de connaissances ou requièrent des ressources très spécialisées. En ce sens, le monitoring constitue un outil de défense efficace.

Selon l'Université de Pennsylvanie, **90 % des incidents de sécurité résultent de bogues dans des logiciels et à chaque 9 lignes de code, même les ingénieurs de logiciels les plus qualifiés et expérimentés font une erreur**.

Le problème est dû au fait que les bonnes pratiques en matière de sécurité concernant le développement de sites Web sont déficientes. En effet, la majorité des développeurs sont rémunérés en fonction du temps qu'ils prennent à livrer les fonctionnalités demandées et sont évalués sur la stabilité (nombre de bogues) de celles-ci et non en fonction de leur sécurité.

La majorité des cyberattaques sont effectuées sur des sites Internet et chaque jour, des milliers sont ciblés par les hackers.

Il va s'en dire que les sites et applications sont omniprésents et largement accessibles. Effectuer une **attaque sur un site Web ne nécessite qu'une connexion Internet**. Et tout ce qu'il faut à partir de là est une vulnérabilité qui peut être exploitée.

L'IMPORTANCE DE FAIRE UN AUDIT DE SÉCURITÉ

La manière traditionnelle de vérifier la sécurité d'un réseau est de le faire auditer, mais beaucoup d'entreprises négligent cette partie soit parce qu'elles n'ont pas les ressources à l'interne, soit parce qu'elles manquent de temps ou qu'elles n'ont pas les bons outils. Ne pas faire d'audit de sécurité augmente considérablement les risques d'attaques et malheureusement, les organisations peuvent parfois mettre du temps avant de réaliser qu'elles ont été piratées.

COMMENT AUGMENTER LA SÉCURITÉ DE SON SITE INTERNET ?

Il existe différentes mesures à mettre en place pour sécuriser son site, mais d'abord et avant tout, cela passe par un changement de mentalité. Les entreprises doivent **considérer la sécurité comme une préoccupation majeure et non pas comme secondaire**. Il est donc important de former et de garder les employés alertes quant aux bonnes pratiques de sécurité.

L'AVENIR DES SITES INTERNET

L'avenir du Web et des applications mobiles reposent sur la capacité à faire le pont entre la sécurité et le développement au sein de l'organisation.

Les sites Internet occupent une grande place dans les opérations des entreprises. Et s'ils ne sont pas bien sécurisés, ils peuvent être destructeurs pour la réputation et les opérations d'une organisation – pouvant même conduire dans certains cas, à la faillite.

LE MONITORING CONSTITUE UN OUTIL DE DÉFENSE EFFICACE

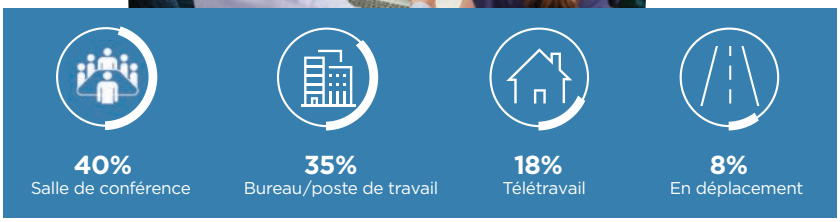
Pour plus d'informations, n'hésitez pas à télécharger notre rapport sur la sécurité au www.ars-solutions.ca/protectionscritiques ou à nous écrire à **info@ars-solutions.ca**.

Nous pouvons vous aider à **monitorer efficacement vos systèmes** et à les **sécuriser selon vos besoins d'affaires**.

TEMPS DE LECTURE 2:00

Logitech : solution de télétravail abordable pour PME

Photo : Logitech.com



Selon *WainHouse Research*, il y une augmentation de travailleurs à domicile, d'applications collaboratives et de salles de conférence plus petites.

Face à cette réalité, *Logitech* a commercialisé un dispositif intitulé *ConferenceCam Connect* qui offre une combinaison inédite de flexibilité et portabilité aux organisations en quête de réunions virtuelles évolutives et intuitives.

De plus en plus d'entreprises souhaitent investir dans des équipements permettant d'améliorer l'expérience des groupes de travail, et ce, sans se ruiner. Grâce à la performance et à la conception adaptée à la réalité des organisations, les dispositifs *ConferenceCam Connect* pourraient être une solution à considérer pour votre entreprise en matière de vidéoconférence.

Son objectif : changer la façon dont les équipes de travail coopèrent et transformer n'importe quel lieu de réunion en un espace de collaboration virtuelle.

AVANTAGES

- Son cristallin;
- Image ultra-précise;
- Simple d'utilisation et d'installation;
- Aucun logiciel, formation ou maintenance spécifique n'est requis;
- Facilement déplaçable d'une pièce à l'autre sans l'aide d'un technicien;
- Grand champ de vision : conçu pour des groupes pouvant aller jusqu'à 10 personnes.

COÛTS

Les tarifs tournent autour de 250 $ pour une caméra de base et de 1 000 $ à 1 300 $ pour un ensemble de plus haute qualité permettant des conférences entre de plus grands groupes.

Comparativement aux solutions telles que *Skype* et *Google Hangouts*, qui sont conçues pour des réunions de personne à personne (l'angle de la caméra ne permettant pas de bien filmer plusieurs personnes à la fois), *ConferenceCam Connect* convient mieux pour des groupes de plus grande taille et géographiquement éloignés. Le dispositif de *Logitech* pourrait être une option avantageuse pour votre entreprise. Renseignez-vous !

Source : Logitech.com

La solution *Cloud* d'ARS nous fait gagner en efficacité

« ARS a su nous proposer un *Cloud* privé répondant parfaitement à nos besoins d'affaires. Nous devons souvent nous déplacer et travailler à partir de différents endroits. La solution nous permet d'avoir accès à l'information facilement lors de nos déplacements. **Les coûts fixes proposés nous aident à mieux prévoir et à gérer notre budget** tout en permettant une meilleure répartition dans les états financiers. ARS prend en charge les maintenances et le support de nos usagers de manière autonome. **C'est un souci de moins** pour nous de savoir que tout se fait sans que nous ayons besoin de s'impliquer ou d'être présents au bureau.

Somme toute, l'équipe d'ARS fait preuve d'une grande disponibilité et d'une prise en charge dont nous avons besoin. Nous sommes entièrement satisfaits des services rendus. »

Sandra Bussières, Contrôleur financier
Construction GCEG

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