Août 2019 • Vol. 6 n° 7

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies

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

« Une tranquillité d'esprit à tous les niveaux et pour tous les membres de la direction.

Avec la solution de sauvegarde d'ARS Solutions - 2B.BACK - on est maintenant sûr de la fiabilité de nos copies de sécurité.

Bravo à ARS pour sa disponibilité et sa rapidité à restaurer les fichiers qu'on lui demande. Pour nous, finies les manipulations ! Pourquoi le faire nous-mêmes ?

Nous avons deux succursales, une à Québec et une à Montréal. 2B.Back facilite notre gestion, peu importe où l'on se trouve. En plus, il occupe une position beaucoup plus stratégique en termes de plan de relève, comparativement à la solution que nous avions avant. Un souci de moins pour tous les membres de la direction. »

Maurice L'Écuyer
Responsable des TI
Orthofab Inc.

Suivez-nous

La responsabilité des entreprises DANS LA PROTECTION DES DONNÉES DE LEURS CLIENTS

TEMPS DE LECTURE 4:00

Si votre entreprise est victime d'une attaque de cybercriminalité lors de laquelle les données de vos clients ou de vos patients sont compromises, vous ferez l'objet d'une enquête et serez interrogé sur ce que vous avez fait pour éviter que cela ne se produise.

Et si la réponse n'est pas adéquate, vous pourriez être tenu responsable, faisant face à de sérieuses amendes et même à des poursuites judiciaires. Prétendre l'ignorance n'est pas une défense acceptable et ce cauchemar coûteux et destructeur de réputation tombera directement sur VOS épaules…

La cybercriminalité a grandement pris de l'ampleur depuis les dernières années. Le vol de données touche de plus en plus d'entreprises. C'est le cas notamment de **Desjardins, Equifax et Capital One qui se sont récemment fait voler les données de plusieurs millions de clients**. Il n'y a pas seulement les grandes entreprises qui sont la cible de ces attaques. Au contraire, les PME sont souvent plus vulnérables par leur faible niveau de sécurité connu des malfaiteurs, mais on en entend moins souvent parler par manque de notoriété. Il ne suffit que d'un employé malveillant pour mettre en péril vos données confidentielles ainsi que votre crédibilité.

SUITE À LA PAGE 2 ▼

LA PROTECTION DES DONNÉES POUR L'INTÉRÊT DE TOUS

Les entreprises stockent une quantité importante d'informations sensibles sur leur clientèle. La fuite ou le vol de ces données pourrait entraîner de lourdes conséquences, irréversibles. Il est donc primordial de connaître vos responsabilités en tant qu'entreprise concernant la protection des données de vos clients et d'entamer les mesures préventives bien avant qu'un tel événement ne se produise. Il est d'ailleurs dans l'intérêt de toute entreprise de protéger l'information de ses clients non seulement pour son image, mais aussi parce que cette initiative peut devenir un atout de fidélisation puisqu'une prise en charge optimale des données confidentielles va susciter la confiance des clients.

La collecte systématique d'informations personnelles auprès des consommateurs nécessite un traitement conforme à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) :

Les renseignements personnels ne peuvent être utilisés qu'aux fins auxquelles ils ont été recueillis. L'organisation qui entend les utiliser à d'autres fins doit, de nouveau, obtenir le consentement de le faire. Les renseignements personnels doivent être protégés par des mesures appropriées.

Le non-respect de cette loi pourrait entraîner la poursuite en justice de l'entreprise responsable, des recours collectifs importants, la perte de nombreux clients et parfois même la faillite. Voilà pourquoi la sécurité devrait toujours être une priorité.

COMMENT PROTÉGER LES DONNÉES DE SES CLIENTS

Il existe plusieurs façons d'éviter les fraudes et de protéger ainsi les données personnelles de votre clientèle. Tout d'abord, le respect du cadre légal est impératif. Une entreprise peut toutefois être conforme aux règlements, mais qu'en est-il de ses employés ? Il y a des dizaines

SUITE DE LA PAGE 1 ▲

de façons par lesquelles les employés volent, et cela arrive BEAUCOUP plus que ce que les entreprises croient. Selon le site Web *Statistic Brain*, 75 % des employés ont volé leurs employeurs à un moment donné. Du vol d'informations à la fraude par carte de crédit, votre argent durement gagné peut facilement être volé au fil du temps.

COMMENT DÉTECTER SI UN EMPLOYÉ VOUS VOLE DES INFORMATIONS

Savez-vous ce qu'est un SIEM? C'est un système de gestion des événements de sécurité qui permet une détection plus efficace et plus rapide des incidents de sécurité qui seraient normalement passés inaperçus. Ainsi, il vous permet de prendre des mesures défensives rapidement et d'éviter les pertes de temps en recherches et diagnostics. Vous minimisez donc les dommages et avez la preuve que vous avez mis en place ce qu'il faut pour prévenir le vol d'informations. Par exemple, si le SIEM détecte un comportement anormal de la part de l'un de vos employés, vous serez notifié et pourrez immédiatement prendre les mesures nécessaires. Vous saurez aussi si une personne non autorisée tente de se connecter à vos systèmes pour extraire des informations sensibles telles que des listes de prix ou des listes de clients. Il peut également s'agir d'un virus sournois qui se manifeste silencieusement, mais progressivement sur vos systèmes dans le but de faire du dommage...

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

Séminaires sur la cybersécurité

ARS Solutions tiendra plusieurs séminaires cet automne durant lesquels vous apprendrez tout pour éviter d'être une cible de choix pour les cybercriminels et comment protéger tout ce que vous avez travaillé si fort à gagner.

Intéressé à y participer ? Appelez-nous pour obtenir les détails.

info@ars-solutions.ca • 418-872-4744 #233

Quoi faire en cas **DE VOL D'IDENTIFIANTS NUMÉRIQUES ?**

À la suite du récent vol de renseignements personnels de plus de 2,7 millions de membres du Mouvement Desjardins, il est important de savoir comment réagir à ce genre de situation qui touche beaucoup plus d'entreprises québécoises qu'on le pense.

Le vol d'identifiants personnels numériques, comme votre nom, prénom, date de naissance, numéro d'assurance sociale, n'est pourtant pas quelque chose de nouveau. Les compagnies continuent tout de même d'attendre que ça leur arrive avant d'agir. Les conséquences d'une telle attaque peuvent être très lourdes. Voilà pourquoi il faut être particulièrement prudent, et ce, bien avant de se faire avoir. Tout commence par une bonne conscientisation.

EN TANT QUE VICTIME, VOICI CE QUI POURRAIT VOUS ARRIVER :

VOTRE BANQUE SE RETIRERA DE TOUTE RESPONSABILITÉ

Si vos identifiants numériques ou ceux de vos employés se retrouvent entre les mains d'un malfaiteur, ils pourraient être utilisés pour effectuer des transactions/virements à partir du compte bancaire de votre entreprise sans que vous en soyez informé. Par exemple, on pourrait se faire passer pour vous et demander un transfert quelconque auprès de l'un de vos employés. Lorsque vous apprendrez la nouvelle, il sera déjà trop tard. **La banque ne pourra être tenue responsable des transactions non désirées à partir de votre compte puisqu'elles auront été effectuées en toute conformité avec les bons identifiants numériques** sans que ce soit considéré comme une infraction puisque l'on pensera que vous êtes à l'origine de ces transferts/paiements.

VOUS DEVREZ PAYER POUR VOTRE DÉFENSE

En cas de transactions frauduleuses à votre compte à la suite du vol de vos identifiants numériques, vous devrez prouver que ce n'était pas vous ou vos employés qui aurez fait ces transactions et ce ne sera pas aussi évident que vous le pensez. **Il vous faudra être représenté légalement devant la cour et votre requête devra être approuvée par un juge.** Nul besoin de vous spécifier que cette démarche pourrait vous coûter très cher, tant pour les frais d'avocat qu'en termes de temps.

La cybercriminalité est une réalité bien présente à laquelle on doit faire face en mettant en place les protections adéquates avant d'en devenir victime.

SI VOUS ÊTES VICTIME DE VOL D'IDENTIFIANTS NUMÉRIQUES, VOICI CE QUE VOUS DEVEZ FAIRE LE PLUS RAPIDEMENT POSSIBLE :

1. Changer votre mot de passe du compte ciblé et de tous les autres comptes où les mêmes coordonnées et questions de sécurité sont utilisées.

2. Appeler votre institution bancaire pour leur demander de mettre une note à votre dossier afin d'exiger une signature pour toute demande de crédit ou de changement. N'oubliez pas de vérifier régulièrement les transactions effectuées dans vos comptes bancaires et de signaler sans tarder toute transaction douteuse. Vous pourriez aussi faire appel à Equifax ou TransUnion pour souscrire à une surveillance de votre crédit.

3. Faire une réclamation de dédommagement à l'entreprise ou la personne responsable, participer au recours collectif s'il y a lieu et vous informer à savoir si vous avez une assurance de vol d'identité.

La cybercriminalité est une réalité bien présente à laquelle on doit faire face en mettant en place les protections adéquates avant d'en devenir victime. Une cyberattaque peut rapidement se transformer en cauchemar pour l'entreprise qui la vit et son personnel.

3 choses à faire avant la fin du support de Windows 7

TEMPS DE LECTURE 2:30

*Après 10 ans de service, le support pour **Windows 7 prendra fin le 14 janvier 2020**. Après cette date, l'assistance technique et les mises à jour logicielles de Windows Update permettant de protéger votre ordinateur ne seront plus disponibles.*

Voici quelques conseils afin de bien vous préparer à la fin du support de Windows 7.

QUE SIGNIFIE LA FIN DU SUPPORT?

Le 14 janvier 2020, votre ordinateur continuera de fonctionner, mais **Microsoft ne fournira plus ce qui suit**:

- Support pour tout problème d'ordre technique
- Mises à jour des logiciels Microsoft
- Mises à jour et correctifs de sécurité

Bien que vous pourrez continuer d'utiliser votre ordinateur sous Windows 7, celui-ci sera exposé à un **plus grand risque quant aux virus et logiciels malveillants étant donné que vous ne recevrez plus de mise à jour logicielle ou de sécurité**.

VOICI 3 CHOSES À FAIRE POUR VOUS PRÉPARER À LA FIN DU SUPPORT DE WINDOWS 7:

1 Sauvegarder vos fichiers

Il se peut que vous soyez dans l'obligation de changer d'appareil en cas de problème de compatibilité. Si vous utilisez votre ordinateur depuis quelques années, vous souhaiterez probablement transférer certains fichiers vers votre nouvel appareil. **Pour déplacer vos fichiers confidentiels**, il est préférable de faire appel à un fournisseur de Cloub privé. **Pour les données publiques**, vous pouvez les sauvegarder sur OneDrive de Microsoft, Google Drive de Google ou même WeTransfer Plus qui permet de protéger vos transferts par mot de passe et de fixer la date d'expiration de ceux-ci.

2 Vous munir d'un service géré d'antivirus

Si vous utilisez un antivirus vendu par Windows 7, il ne sera plus possible de le mettre à jour. Il faudra donc vous tourner vers une solution plus sécuritaire. Ce service géré par votre partenaire TI vous assure une protection en temps réel et une gestion journalière des mises à jour dont vous n'aurez plus à vous occuper. Votre antivirus peut être entièrement pris en charge et monitoré par une équipe qui s'occupe des correctifs lorsque requis.

3 S'y prendre d'avance pour le changement

Contactez votre fournisseur TI à l'avance afin qu'il planifie la cédule pour prendre en charge votre réseau et remédier à vos prochains problèmes d'ordre technique.

ARS Solutions a 30 ans d'expérience en projets de migration et peut vous monter un plan de remplacement adapté à vos besoins. ARS offre des solutions de sauvegarde et de protection contre les virus et logiciels malveillants pour vous aider avec la fin du support de Windows 7. N'hésitez pas à nous contacter pour en savoir davantage.

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