PASSION AFFAIRES et technologies

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

ARS solutions 25 ans

Vol. 3 nº 7. Septembre 2016

UN GAIN EN EFFICACITÉ de près de 100 HEURES par semaine pour Les Constructions BÉ-CON Inc.

TEMPS DE LECTURE 2:30

DES OPÉRATIONS CRITIQUES

« On doit avoir un environnement informatique stable, performant et sécurisé. Pour nous, le respect des délais dans le dépôt des soumissions est très critique. Si on excède le délai, on est éliminé. On ne peut donc pas se permettre que nos systèmes soient défaillants » mentionne Yvan Deschênes, directeur de projets. Les technologies occupent donc une place importante chez Les Constructions BÉ-CON.

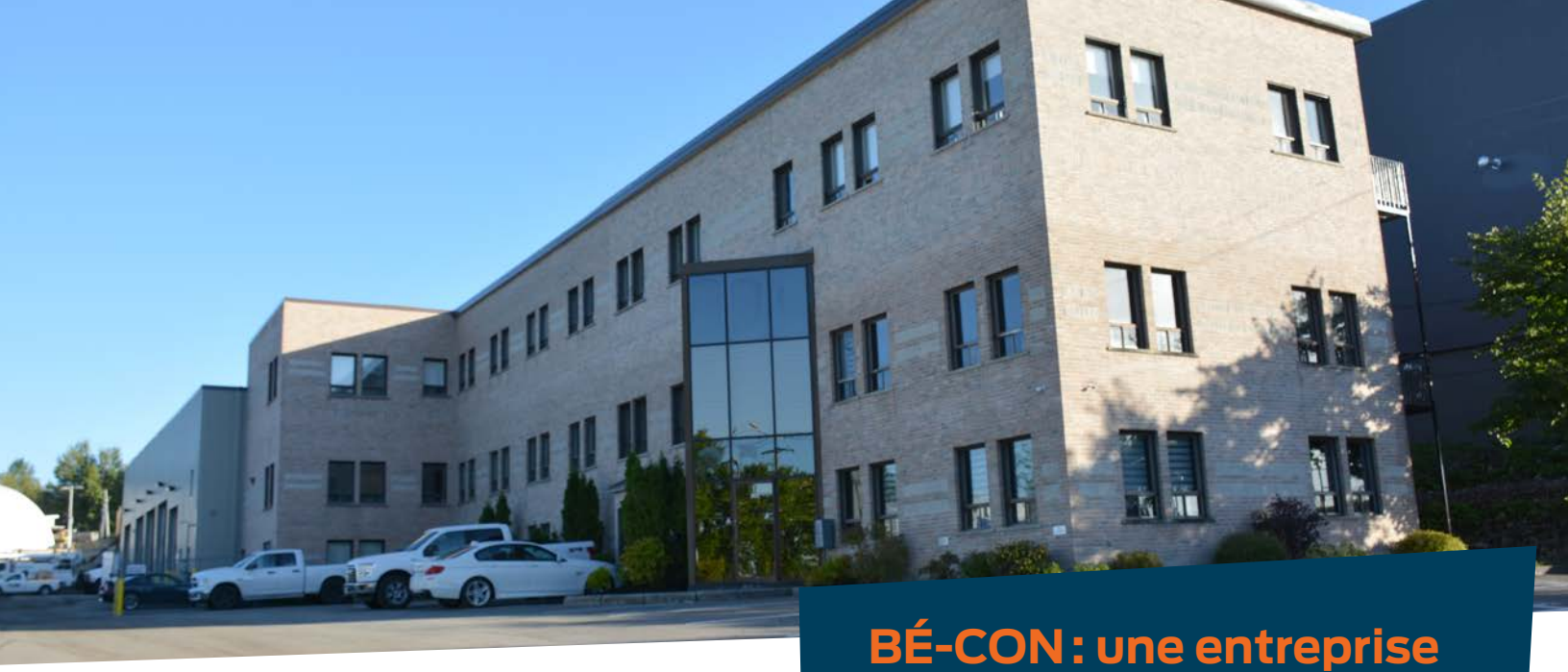
UNE NÉCESSITÉ DE CHANGER POUR ACCROÎTRE L'EFFICACITÉ

Madame Julie Pilote - administratrice et propriétaire ainsi que Monsieur Deschênes étaient fermement décidés à améliorer les TI dans l'entreprise. Les frustrations et les pertes de temps s'accumulaient.

« Nous avons sélectionné ARS, car un changement s'imposait pour gagner en efficacité...

Nous avions des problèmes majeurs de lenteur au niveau du réseau et des problèmes récurrents. Il fallait redémarrer le serveur régulièrement. On avait besoin de gens compétents sur qui se fier et en mesure de répondre rapidement à nos demandes » ajoute Madame Pilote.

SUITE À LA PAGE 2 ▼



SUITE DE LA PAGE 1 ▲

UN GAIN IMPORTANT EN PRODUCTIVITÉ

Après discussion avec cette dernière, on peut estimer **un gain en productivité de près de 100 heures par semaine**. L'environnement technologique de BÉ-CON avait tout à gagner à être optimisé et l'entreprise a confié ce mandat à ARS.

« Maintenant, notre environnement est performant, les problèmes qui se présentent se règlent plus vite et on a l'esprit tranquille parce que nos systèmes sont sécurisés. »

Toute l'équipe d'ARS est fière de compter Les Constructions BÉ-CON parmi sa clientèle et de s'impliquer activement dans son succès.

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

BÉ-CON : une entreprise québécoise florissante

Depuis sa fondation en 1981, Les Constructions BÉ-CON, n'a cessé d'élargir ses activités et possède une large gamme d'expertises dans les secteurs commerciaux, industriels et institutionnels publics et privés tels que routes, structures de béton, aéroports...

Elle se classe aujourd'hui parmi les plus importantes de la région.

SON IMPLICATION DANS LE PROJET DU CENTRE VIDÉOTRON

Grâce à son équipe dynamique, BÉ-CON se démarque en livrant des produits de qualité et en fournissant des solutions innovatrices sur un large éventail de projets exigeants et prestigieux contribuant au rayonnement de la Ville de Québec. **Ce qui l'a d'ailleurs amenée à être sélectionnée pour effectuer l'aménagement extérieur du Centre Vidéotron.**

RAPPORT SUR LA SÉCURITÉ

Pourquoi les PME sont actuellement dans la ligne de mire des cybercriminels ?

7 protections critiques essentielles en TI à mettre en place par les PME pour se protéger des cybercriminels.

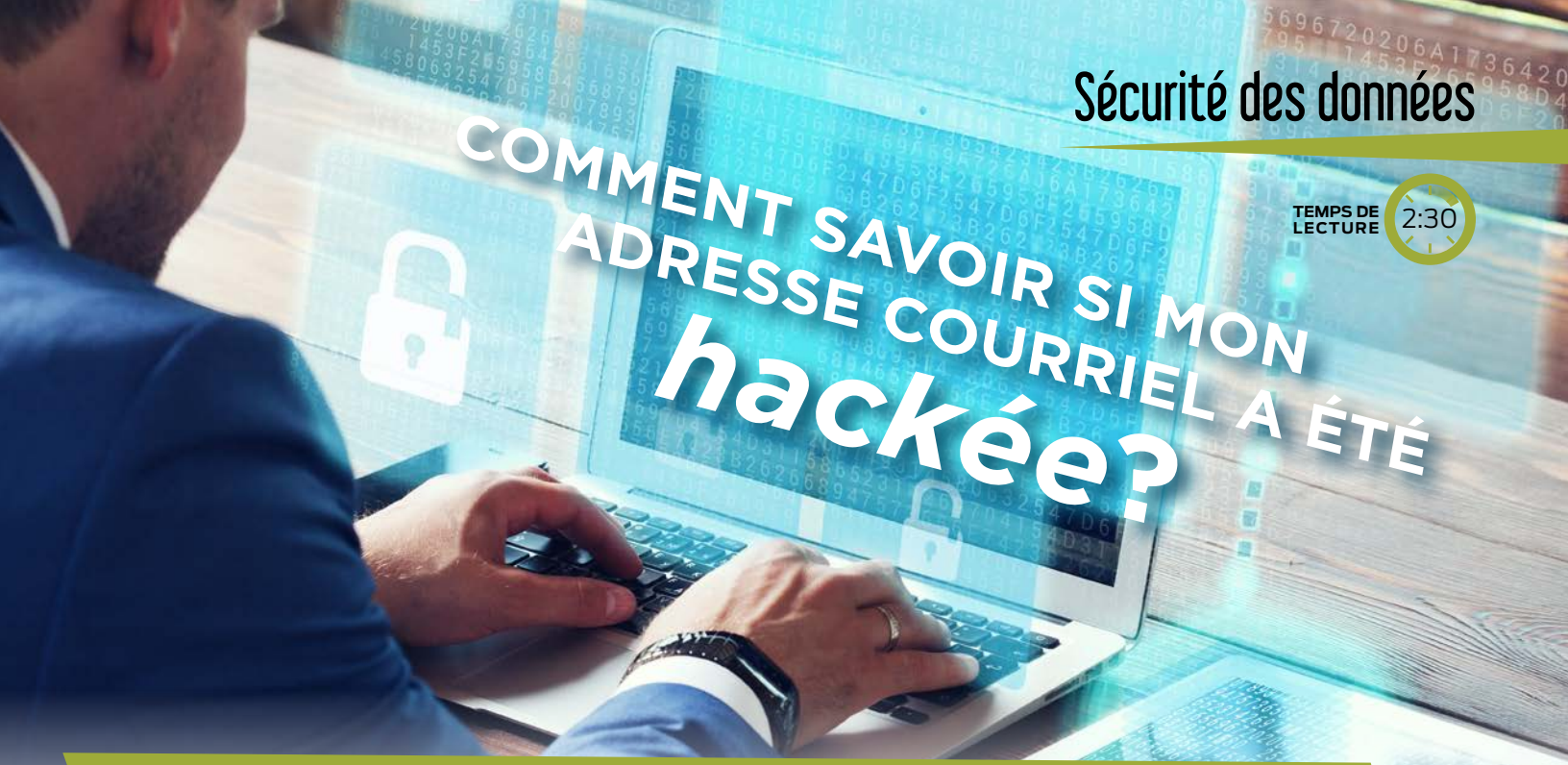
Téléchargez notre rapport GRATUIT
et passez à l'action en suivant les recommandations
www.ars-solutions.ca/protectionscritiques

En prime !
Recevez GRATUITEMENT une série d'astuces sur la sécurité

Nous rendons les entreprises plus efficaces et performantes en transforma

TEMPS DE LECTURE 2:30

COMMENT SAVOIR SI MON ADRESSE COURRIEL A ÉTÉ *hackée?*



Vérifiez auprès de 140 sites Web et plus, dont LinkedIn, Dropbox, Bell, etc.

Les arnaques, la fraude en ligne et le vol d'identité ne sont que quelques exemples d'enjeux devenus très préoccupants dans le cyberespace. Naviguer sur le Web tout en évitant ces menaces peut représenter un défi de taille. En effet, des millions de personnes sont régulièrement victimes de cyberattaques sans même le savoir. Dans cet article, vous découvrirez si vos identifiants ont été volés parmi plus de 140 sites répertoriés.

DROPBOX – L'UN DES PLUS GRANDS CAS DE CYBERATTAQUE AU MONDE

On annonçait dernièrement que Dropbox - plateforme américaine de stockage de documents en ligne - avait subi une **brèche de données en 2012 et que près de 70 millions d'identifiants (noms d'utilisateurs et mots de passe) avaient été volés. Et ce n'est qu'il y a quelques semaines, soit 4 ans plus tard, qu'elle a admis que les informations de ses clients avaient été publiées en ligne...** Dropbox a rapporté que les adresses courriel ont été rendues publiques. Elle a mis en garde ses utilisateurs que s'ils ont utilisé le même mot de passe pour d'autres services, qu'il serait préférable de le changer immédiatement.

VOS IDENTIFIANTS ONT-ILS ÉTÉ PIRATÉS ?

Rassurez-vous, il existe un outil gratuit fort simple et sécuritaire pour le savoir !

La page Web « **Have I been pwned** » (Est-ce que je me suis fait avoir ?) répertorie l'ensemble des sites piratés et dont les informations personnelles ont été divulguées.

Simplement en entrant votre adresse courriel, vous pourrez savoir si vous avez été impliqué par l'une des cyberattaques recensées par le site. **Attention ! Même si le site affiche *Good news – no pwnage found!***, cela ne veut pas dire pour autant qu'il n'y a aucun risque, puisqu'il se peut que vous ayez été impliqué dans une brèche qui n'a pas encore été révélée...

Il est donc urgent que vous vérifiiez vos comptes et rehaussiez leur sécurité.

À ce jour, ***Have I been pwned*** prend en compte plus de **140 sites et applications et 1 440 000 000 de comptes compromis**, provenant entre autres des sites suivants :

myspace	359 420 698
in	164 611 595
Adobe	152 445 165
	68 648 009
vtech	4 833 678
	4 609 615
Forbes	1 057 819
YAHOO!	453 427
	116 465
Bell	20 902
SONY	37 103

Sources : Have I been pnwed : https://haveibeenpwned.com
Times : http://time.com/4474986/dropbox-hack

VOTRE *SMARTPHONE* PEUT ÊTRE PIRATÉ FACILEMENT ET À VOTRE INSU

TEMPS DE LECTURE 2:45

« Au final, tout est piratable » mentionne Adi Sharabani - cofondateur de Skycure, une compagnie spécialisée en sécurité mobile. « Et ce qui est le plus surprenant, c'est qu'on oublie parfois à quel point c'est simple... ». Même si une personne malicieuse ne peut accéder à votre téléphone, elle peut essayer d'obtenir des informations sensibles tels vos contacts, les courriels, les places visitées, etc.

Avec l'augmentation du nombre de *smartphones* et de tablettes en milieu de travail, les pirates peuvent désormais attaquer les entreprises en exploitant les vulnérabilités présentes dans ces appareils. Les spécialistes en sécurité qui simulent des attaques informatiques pour leurs clients ont démontré qu'elles étaient habituellement non détectées par le département TI et c'est ce qui est problématique. Mais ce qui l'est encore plus, c'est qu'ils ne savent pas combien de mobiles ont été piratés.

3 FAÇONS DE PIRATER UN *SMARTPHONE*

1. WIFI NON SÉCURISÉS

Les WiFi publics des cafés ou des aéroports sont parfois non sécurisés et permettent ainsi aux pirates d'avoir accès à TOUT ce que vous faites. « Quelqu'un essaie d'accéder à vos courriels, mots de passe, contacts et ils tentent de savoir qui vous rencontrez, où et quand » mentionne Sharabani. Assez intrusif, non ?

Pour savoir si vous êtes connecté à un réseau sécuritaire, portez attention aux messages de mise en garde qui apparaissent sur vos appareils. En dépit de ces avertissements, **92 % des gens cliquent quand même sur « continuer » ou sur « j'accepte »**. Pourquoi ? **Parce que les gens sont conditionnés à cliquer sur n'importe quel message, parce qu'ils veulent le contenu**, souligne Alex McGeorge, expert en sécurité. Soyez donc vigilant quand vous vous connectez à un WiFi public et **évitez de partager des informations sensibles**.

2. FAILLES DES SYSTÈMES D'EXPLOITATION

Malgré les bonnes intentions des manufacturiers de téléphones intelligents, des vulnérabilités sont constamment trouvées et exploitées par les pirates. Sur un ratio moyen d'une vulnérabilité divulguée publiquement chaque jour, **10 % d'entre elles sont critiques** en ce sens qu'elles permettent aux pirates d'accéder à vos appareils et de les contrôler, affirme Sharabani. Les fabricants émettent régulièrement des mises à jour avec des correctifs de sécurité très importants et spécialement conçus pour vous protéger. Il est donc de votre responsabilité de les installer le plus rapidement possible.

3. APPLICATIONS MALICIEUSES

Les applications ajoutent de la fonctionnalité aux appareils mobiles, mais augmentent les risques d'attaques, particulièrement lorsqu'elles sont téléchargées à partir de sites Internet ou de messages, au lieu, par exemple, de l'*App Store* – plus sécuritaire.

COMMENT SE PROTÉGER ?

McGeorge suggère de **limiter le nombre d'applications téléchargées, de vérifier qui est le concepteur et de vous poser la question suivante : en ai-je vraiment besoin ?** Et n'oubliez pas de porter attention aux avertissements du genre : « *This app will have access to your email* » lorsque vous installez des apps. Acceptez-vous vraiment ceci ?

En résumé, selon Sharibani, il est impossible d'être 100 % sécurisé, mais il existe des façons de diminuer vos risques et de rendre l'accès à vos appareils plus difficile.

Source : NBC news

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