PASSION AFFAIRES et technologies

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

ARS solutions 25 ans

Vol. 3 nº 2. Février 2016

SPÉCIAL SÉCURITÉ

Vous recevez ce message en ouvrant votre ordinateur :

TEMPS DE LECTURE 4:30

Cas vécu

SAURIEZ-VOUS QUOI FAIRE ?

C'est ce qui est récemment arrivé à l'un de mes clients et croyez-moi, cela arrive plus souvent que l'on pense…

L'hameçonnage (où la fraude par courriel) n'arrive pas qu'aux autres et le fait de demander une somme d'argent en échange de vos données s'appelle le rançonnage. Selon une étude menée par l'Université de Kent en février 2014, plus de 40 % des gens qui ont été victime de CryptoLocker[1] ont payé la rançon demandée. Le rapport *SecureWorks* de Dell indique que le même malware coûte plus de 30M$ tous les 100 jours.

Mais comment savoir si la menace est sérieuse ou non ? Le contenu d'un courriel ou d'un message texte hameçon vise à déclencher une réaction impulsive de votre part. On vous demande alors une réponse immédiate sous un faux prétexte. Dans tous les cas, il n'y a pas de chance à prendre.

Les réactions sont souvent les mêmes : on s'interroge, on doute, on est fâché, on panique et voilà que le processus est amorcé…

SI CELA VOUS ARRIVE, PAR OÙ DEVEZ-VOUS COMMENCER ?

Voici ce qu'il faut faire :

- Soyez vigilant, prenez l'habitude de vérifier la barre d'adresse du site Web afin de voir si elle est différente de celle inscrite dans le courriel;
- Ne répondez pas à ces courriels ou messages textes;
- Ne cliquez jamais sur les hyperliens;
- Ne fournissez l'information demandée sous aucun prétexte.

SUITE À LA PAGE 2 ▼

Sécurité des données

SUITE DE LA PAGE 1 ▲

SI VOUS AVEZ MALENCONTREUSEMENT RÉPONDU AUX COURRIELS :
Agissez rapidement et faites vérifier votre réseau. Les programmes malveillants sont à toutes fins pratiques invisibles. Ils sont difficiles à détecter, car généralement ils n'apparaissent pas dans la liste des programmes installés et peuvent se réactiver à tout moment.

Un diagnostic révèlera s'il s'agit d'une vraie menace et vous permettra de savoir quoi faire. Vous pourrez ainsi évaluer la situation et serez en mesure de prendre la meilleure décision.

QUELS SONT LES SIGNES ?
Voici quelques exemples :

- Lenteur;
- L'ordinateur fige plus souvent;
- Pannes;
- Frais de télécommunications anormalement élevés.

L'HAMEÇONNAGE PEUT SE PRÉSENTER AINSI :

- *Nous vous prions de vérifier les renseignements de la transaction ci-dessous;*
- *Dans le cadre des efforts continus que nous déployons pour protéger votre compte et réduire les cas de fraude, nous avons remarqué que votre profil bancaire en ligne a besoin d'être mis à jour;*
- *Cher titulaire de compte en ligne;*
- *Votre compte n'est pas accessible à l'heure actuelle;*
- *Important message d'intérêt public de la part de;*
- *Vous avez 1 message relatif à la sécurité à lire;*
- *Nous avons le regret de vous informer que nous avons dû bloquer l'accès à votre compte bancaire. Pour réactiver votre compte, composez le numéro suivant...*

PRÉVENTION :

- Formez et gardez informé le personnel de votre entreprise sur les bonnes pratiques de sécurité. **N'oubliez pas que vous êtes la menace numéro un en ce qui a trait à la sécurité de votre réseau**;
- Par un simple mémo interne, faites un rappel à vos employés afin de les garder alertes. La rigueur est votre alliée;
- Assurez-vous d'avoir en place ce qu'il faut. La surveillance en continu de votre réseau doit être prise au sérieux. Cette tâche est trop souvent mise de côté pour des urgences quotidiennes...
- Faites les mises à jour des logiciels recommandés par les manufacturiers et les fournisseurs. Mettez régulièrement à jour les antivirus, les logiciels anti espions, les filtres-courrier et les pare-feu afin de protéger votre ordinateur;
- Faites auditer votre réseau annuellement.

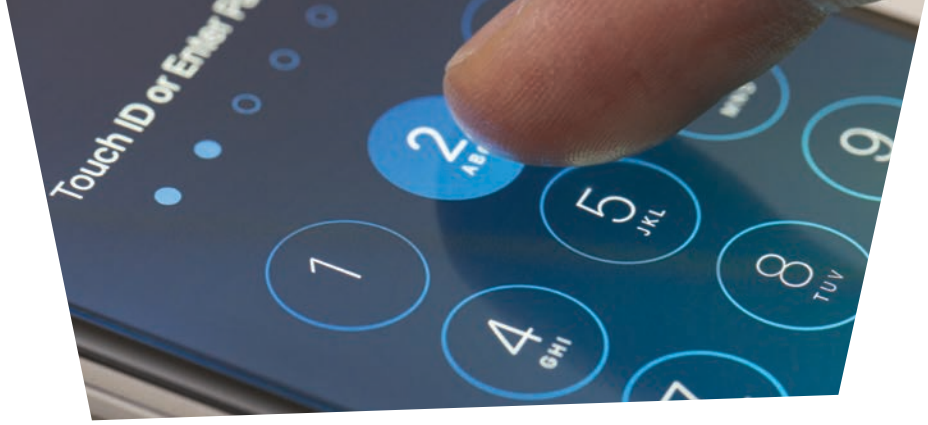
Le client qui a vécu cette situation n'a pas subi de conséquence grave puisque ses données étaient bien sécurisées. Par contre, **la vérification lors du diagnostic a révélé que la menace était bien réelle**. Les outils mis en place pour assurer la sécurité ont fait une partie du travail. Toutefois, il a quand même été nécessaire de faire une mise à niveau de la sécurité de l'environnement.

Pour en savoir plus sur la sécurité, n'hésitez pas à nous contacter.

Les programmes malveillants sont à toutes fins pratiques invisibles. Ils sont difficiles à détecter, car généralement ils n'apparaissent pas dans la liste des programmes installés et peuvent se réactiver à tout moment.

[1] CryptoLocker est un logiciel malveillant de type cheval de Troie et qui tourne sous Windows. Le programme se diffuse principalement via des mails infectés, déguisés en factures UPS, FedEx ou de banque. Une fois activé, il chiffre les données personnelles de l'utilisateur et demande une rançon pour les déverrouiller. Le message d'alerte s'accompagne d'un compte à rebours de 72 ou 100 heures, qui menace de supprimer les données si la rançon n'est pas payée. Une fois arrivé à zéro, il augmente en réalité fortement le montant de cette dernière (source : Wikipedia).

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



TEMPS DE LECTURE 2:00

La fin des mots de passe

Si le cybercrime gagne du terrain, les méthodes traditionnelles en matière de sécurité doivent être revues afin de s'en prémunir. Selon la société de recherche *Juniper Research*, le coût des violations des données à l'échelle mondiale pour les entreprises pourrait se chiffrer à 2100 G$ d'ici 2019.

Difficile de nier ceci : lorsqu'un mot de passe relève de la simplicité, il est facile à pirater, et lorsqu'il est trop complexe, il devient difficile de s'en rappeler. Vous avez peut-être, comme la plupart des gens, une *trop* longue liste de mots de passe. Et que dire des frustrations engendrées lorsque vous devez vous connecter d'urgence, mais n'avez pas ladite liste en tête… Le processus d'identification et de récupération d'un mot de passe peut s'avérer long et décourageant.

« La vision de cette entreprise : Tout dispositif avec lequel vous interagissez saura vous reconnaître. Vous n'aurez plus besoin de mémoriser tous vos mots de passe ».

Dans l'esprit de contrer ce problème, le *start-up* américain ***AimBrain*** – spécialisé en cybersécurité – a amassé plus de 700 000 $ afin de développer une technologie novatrice qui révolutionnera le mot de passe tel que nous le connaissons aujourd'hui. Vous vous demandez de quoi il s'agit ? Voyons voir de plus près leur brillante idée…

En se basant sur des **mesures comportementales** (vitesse d'écriture, pression faite sur les touches du clavier, endroit où l'écran est balayé) qui reconnaissent et évaluent comment une personne interagit avec un appareil, il est désormais possible de reconnaître si les utilisateurs sont bien ceux qu'ils prétendent être. Grâce à cette validation, l'appareil pourra décider de bloquer ou de vous donner accès à l'information.

AimBrain compte lancer la reconnaissance faciale au cours de la prochaine année, ce qui pourrait remplacer les mots de passe tel que nous les connaissons aujourd'hui. Même s'ils ne seront pas amenés à disparaître complètement, les politiques à leur sujet changeront certainement.

Pour en savoir plus : www.telegraph.co.uk
Source : The Telegraph

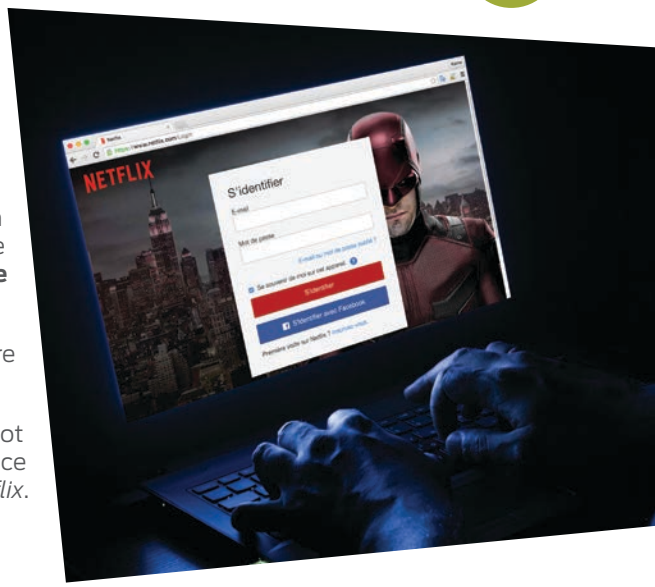
Les membres de la direction ont tous grandi dans cette expérience avec ARS…

« Nous avons vraiment apprécié l'intervention d'ARS dans notre entreprise. Après ce mandat de Planification Stratégique Affaires-TI, nous savons exactement où investir en technologies pour les trois prochaines années afin qu'elles viennent vraiment appuyer l'atteinte de nos objectifs d'affaires. Nous avons réalisé à quel point le mot « Solutions » dans le nom de cette entreprise prend tout son sens. Nous voyons clairement le retour sur investissement dans les projets que nous nous apprêtons à implanter. En plus, les membres de la direction ont tous grandi dans cette expérience. Merci à toute l'équipe ! »

Isabelle Martin
GDG Environnement
Présidente et chef de la direction

TEMPS DE LECTURE 1:00

Des pirates informatiques vendent vos mots de passe *Netflix* pour 0,25 $



LE SUCCÈS GRANDISSANT DE NETFLIX ATTIRE L'ATTENTION DES PIRATES INFORMATIQUES

Dans son blogue du 11 février dernier, l'entreprise *Symantec* – spécialisée en sécurité, rapporte qu'il y a une augmentation des mots de passe volés. Dans ce dernier, on fait mention d'un fournisseur qui possède plus de **300 000 mots de passe à vendre**.

Si vous voyez apparaître des films ou des séries télévisées à visionner dans votre compte, cela pourrait signifier que ce dernier a été piraté.

Dans ce cas, les précautions à prendre seraient de changer rapidement votre mot de passe ainsi que celui de tous les autres comptes pour lesquels vous utilisez ce même mot de passe. Assurez-vous d'en avoir un réservé exclusivement à *Netflix*. Surtout, n'utilisez pas le même mot de passe que votre compte bancaire.

Source : www.symantec.com

TEMPS DE LECTURE 1:50

3 conseils à appliquer chaque jour qui vous mèneront au succès selon le magazine *Fortune*

Il y a certaines choses à mettre en pratique en tant que dirigeant d'entreprise et qui ont énormément d'impacts. Voici un résumé de trois recommandations suggérées dans un article du magazine *Fortune*. Lorsque ces 3 principes de base sont suivis chaque jour, l'entreprise est vouée au succès.

DÉDIEZ DU TEMPS POUR APPRENDRE

Pour un dirigeant d'entreprise, lire, apprendre et expérimenter constamment a un impact très positif sur l'avenir de l'entreprise. Au final, cela donne de l'énergie et de l'inspiration pour faire avancer sa carrière. À titre d'exemple, **Mark Zuckerberg, fondateur de *Facebook*, a appris le Mandarin et a lu 2 livres par mois en 2015**.

DONNEZ PLUS DE RESPONSABILITÉS ET D'AUTONOMIE AUX PERSONNES TALENTUEUSES ET PASSIONNÉES

En s'entourant de gens passionnés et talentueux et en leur donnant les outils nécessaires afin qu'ils puissent mettre à profit leurs compétences, l'entreprise ne peut qu'en bénéficier. Il est surprenant de constater tout ce qu'une personne peut accomplir lorsqu'elle aime son travail.

SOYEZ HONNÊTE ENVERS VOUS-MÊME

Comme entrepreneur, on prend des décisions en pensant que c'est ce qu'il y a de mieux pour l'entreprise. Toutefois, il peut arriver que ces décisions soient complètement erronées. Pensez à ceci : lorsqu'on prend une décision, on croit souvent qu'il s'agit de la meilleure. Personne ne se dit : je sens que c'est une mauvaise décision, alors je vais tout de même la prendre. En résumé, l'article nous propose d'être honnête envers soi-même et de parfois repenser à son approche. Prendre du recul et baser ses décisions sur des faits et des objectifs mesurables est préférable. J'en conviens, cela peut sembler difficile à maîtriser, mais des décisions prises sur un *feeling* ne représentent pas un avantage compétitif. Votre compétiteur lui aussi pense qu'il a raison, tout comme vous.

Pour en savoir plus : fortune.com
Mots-clés : entrepreneur successful company

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