Novembre 2020 • Vol. 7 n° 10

PASSION AFFAIRES *et technologies*

ARSolutions 30 ans affaires et technologies

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

ÉDITION SPÉCIALE

TOP 3

parmi les articles les plus lus en 2020

Suivez-nous

Payer la rançon pourrait vous envoyer en justice

Cette sanction ne s'applique pas seulement aux victimes, mais aussi aux sociétés de sécurité et de financement qu'elles engagent.

Les entreprises, les gouvernements et les organisations qui sont victimes d'attaques par rançongiciel doivent désormais faire face à de nouvelles inquiétudes : le ministère américain des Finances leur inflige de lourdes amendes s'ils paient pour récupérer leurs données. **Ce n'est d'ailleurs qu'une question de temps avant que le Canada suive cet exemple.**

Les fonctionnaires du département du Trésor ont officialisé cette orientation dans un avis publié récemment. Il avertit que les paiements effectués à des entités spécifiques ou à toute entité dans certains pays - en particulier, ceux ayant un "lien de sanction" désigné - pourraient soumettre le payeur à des sanctions financières prélevées par l'Office of Foreign Assets Control, ou OFAC.

L'interdiction s'applique non seulement au groupe qui est infecté, mais aussi à toutes les sociétés ou entrepreneurs avec lesquels la sécurité ou l'assurance du groupe piraté s'engage, y compris

SUITE À LA PAGE 2 ▼

ceux qui fournissent une assurance, une expertise numérique et une réponse aux incidents, ainsi que tous les services financiers qui aident à faciliter ou à traiter les paiements de rançon.

Encourager les criminels

« Faciliter le paiement d'une rançon exigée à la suite d'activités cybernétiques malveillantes peut permettre aux cybercriminels de faire progresser leurs objectifs illicites », indique l'avis. Par exemple, les paiements de rançon pourraient être utilisés pour financer des activités contraires aux objectifs de sécurité nationale et de politique étrangère des États-Unis. Les paiements de rançon peuvent également encourager les cybercriminels à s'engager dans de futures attaques.

En vertu de la loi, il est interdit de s'engager directement ou indirectement dans des transactions avec des personnes ou des organisations figurant sur la liste des ressortissants désignés et des personnes bloquées de l'OFAC.

Ces dernières années, le département du Trésor a ajouté plusieurs groupes de cybermenaces connus à sa liste de désignation comme les groupes suivants :

• Evgeniy Mikhailovich Bogachev, le développeur de **Cryptolocker**, une variante de logiciel de rançon précoce qui, selon l'OFAC, a infecté plus de 234 000 ordinateurs, dont la moitié aux États-Unis;

• Deux ressortissants iraniens derrière **SamSam**, le logiciel de rançon qui a paralysé la ville d'Atlanta en 2018;

• Des individus et des groupes liés au groupe **Lazarus**, un groupe de cybercriminels commandité par la Corée du Nord et qui serait à l'origine des attaques de WannaCry, qui a provoqué l'arrêt des ordinateurs dans le monde entier;

• "Evil Corp.", une organisation criminelle basée en Russie dont le chef a été inculpé l'année dernière pour avoir utilisé le célèbre logiciel malveillant **Dridex** pour drainer plus de 70 millions de dollars de comptes bancaires aux États-Unis, au Royaume-Uni et ailleurs.

Payer ou ne pas payer?

Les responsables de l'application des lois et les consultants en sécurité ont généralement déconseillé de payer les demandes de rançon, car ces paiements ne font que financer et encourager de nouvelles attaques. **Beaucoup trop de gens pensent que le paiement de la rançon est le moyen le plus rapide et le moins onéreux de récupérer les données. Toutefois, le paiement d'une rançon aux cybercriminels ne garantit pas que la victime retrouvera l'accès à ses données volées et celles-ci risquent quand même de se retrouver dans le Dark Web à la merci des malfaiteurs.** La ville de Baltimore a subi une perte de plus de 18 millions de dollars après que ses systèmes informatiques aient été bloqués. Les attaquants à l'origine de la demande de rançon avaient exigé 70 000 dollars. En réponse, certaines entreprises qui prétendent offrir des services de réponse aux attaques de rançon paient simplement les attaquants.

Toutes les raisons sont bonnes pour ne pas payer la rançon. En plus des points énumérés ci-dessus, il ne faut pas oublier que **vous traitez avec des fraudeurs** en qui vous ne pouvez pas avoir confiance. **Ils peuvent d'ailleurs exiger une rançon supplémentaire** de votre part ou leur demande de rançon ne pourrait être **qu'une simple ruse pour obtenir autre chose de votre part.**

Aujourd'hui, on peut affirmer que 95 % des solutions de sauvegardes sur le marché ne sont plus adéquates contre les nouveaux types de cyberattaques. Il faut en moyenne 160 jours à une entreprise, toute région du monde confondue, pour découvrir que des données ont été compromises. Assurez-vous d'avoir la solution qu'il faut!

La meilleure option est de vous préparer et d'agir en bon père de famille en mettant en place les 3 incontournables suivants : les sauvegardes, la cybersurveillance et un programme d'hameçonnage.

N'attendez pas d'être victime d'un rançongiciel et consultez votre partenaire TI dès maintenant afin d'éviter le pire…

Source : Dan Goodin

5 CONSEILS POUR SÉCURISER VOS DONNÉES

3:45 TEMPS DE LECTURE

Si le Web n'était qu'un lieu de partage de photos de chiens en costume de dinosaure, les mots de passe ne seraient pas très utiles. Mais c'est sur Internet que vous payez vos factures, accédez aux médias sociaux, consultez votre compte bancaire et vos talons de paie. Pourquoi ne garderiez-vous pas ces objets de valeur virtuels aussi en sécurité que votre portefeuille ou vos clés?

La plupart des malfaiteurs n'ont pas besoin de compétences techniques spécialisées pour accéder à vos comptes, ils peuvent le faire en devinant vos mots de passe ou en exécutant un programme automatisé. Une fois que c'est fait, ils peuvent d'ailleurs essayer ce mot de passe compromis sur d'autres comptes, recueillir des informations sur vous et vos habitudes, reprendre des comptes que vous possédez, ou même utiliser votre identité numérique.

Voici 5 mesures pratiques pour accroître votre sécurité en ligne ▸

1. VERROUILLEZ VOTRE PORTE NUMÉRIQUE. Verrous d'écran : le mot de passe, l'empreinte digitale ou l'identification faciale que vous utilisez pour accéder à votre appareil sont quelques-uns de vos meilleurs moyens de défense contre les personnes qui pourraient vouloir y pénétrer. Mais il en existe de nombreux types et il peut être difficile de savoir lequel vous convient le mieux. Tout comme les différents types de serrures que vous pouvez poser sur vos portes, certaines serrures d'écran sont plus résistantes que d'autres.

2. LAISSEZ ENTRER LA BONNE PERSONNE. Il est facile de créer d'excellents mots de passe. Il vous suffit de suivre quelques principes de base. Vos mots de passe doivent être longs (au moins huit caractères), complexes (combinaison aléatoire difficile à deviner) et uniques (différents partout). Idéalement, vous devriez utiliser un gestionnaire de mots de passe pour générer et stocker tous vos mots de passe. Cette application permet de protéger vos identifiants de connexion et autres données sensibles. Parlez-en à votre fournisseur TI!

3. AJOUTEZ UNE DEUXIÈME CLÉ. La mise en place d'une authentification à deux facteurs (2FA) ou d'une authentification multifacteur (MFA) signifie que même si quelqu'un trouve votre mot de passe, il n'aura probablement pas le facteur supplémentaire dont il a besoin pour entrer. Consultez les paramètres de sécurité de vos sites Web et applications les plus utilisés pour voir si vous pouvez configurer cette clé supplémentaire. Commencez par les plus importants : toutes les applications financières ou les services comme le courrier électronique, que vous utilisez pour récupérer vos autres comptes.

4. PROTÉGEZ VOS OBJETS DE VALEUR VIRTUELS. Tout comme vous prenez soin des objets de valeur de votre maison, vous devriez faire de même pour les informations que vous stockez virtuellement. Cherchez des informations spécifiques qui se trouvent dans votre messagerie ou autres comptes et supprimez-les : scan de votre carte d'identité, coordonnées bancaires, assurance maladie, etc. Si vous en avez besoin plus tard, vous pouvez toujours les télécharger sur votre ordinateur ou les imprimer avant de supprimer le contenu du compte pour repartir à zéro. N'oubliez pas de vider ensuite votre poubelle et vos fichiers temporaires! Sauvegardez vos archives et vos documents sur le Cloud, un disque dur externe ou une clé USB.

5. PASSEZ LE MOT. Le Web ne s'appelle pas "toile" pour rien. Nous sommes tous connectés en ligne par le biais de différents réseaux, non seulement en tant qu'"amis" sur les médias sociaux, mais aussi par les contacts de nos comptes de messagerie. Lorsque vous sécurisez vos données, tous ceux avec qui vous êtes connecté sont un peu plus en sécurité grâce à vos efforts. Pensez à ce que vous pouvez supprimer pour aider vos amis ou collègues : les coordonnées bancaires de votre sœur, le code d'accès à votre bureau ou le scan du passeport de votre fils sont des exemples de documents qui pourraient vous donner mal à la tête s'ils tombaient entre de mauvaises mains. Partagez cette procédure de nettoyage de données avec votre entourage afin de les aider à conserver ce qui leur appartient.

Source : https://datadetoxkit.org/en/security/essentials

Le travail à distance

5 applications pour être plus productif

3:45 TEMPS DE LECTURE

Il n'est pas toujours facile d'être productif en ce moment, mais certains outils peuvent vous aider à tout faire, qu'il s'agisse de rester concentré ou de générer de nouvelles idées.

Le travail à domicile est soudainement devenu la norme depuis la pandémie. Cela entraîne beaucoup plus d'appels Zoom et de chats Slack, et ouvre de nouvelles façons de travailler que vous n'auriez peut-être pas envisagées en travaillant au bureau. **C'est pourquoi les applications de productivité ci-dessous mettent l'accent sur la suppression des distractions, l'élimination des inefficacités et le renforcement de l'organisation.**

Dynamisez vos communications

Comme on ne peut pas se tourner vers l'ordinateur d'un collègue en travaillant à la maison, **Screens est un substitut puissant pour partager votre écran.** L'outil de bureau à distance permet à plusieurs collègues de contrôler un seul ordinateur tout en discutant par la voix ou la vidéo. Il est également doté d'un outil de dessin qui permet aux gens de marquer ce qu'ils regardent sur l'écran partagé. Utilisez-le pour tout ce qui n'est pas déjà intégré à la collaboration en direct de type Google Documents.

Le calendrier des motivations

Lightpad

Vous en avez assez des vieilles grilles ennuyeuses de votre calendrier? **Lightpad adopte une approche différente, en repensant le calendrier comme une sorte d'escalier en spirale que vous pouvez faire défiler**, avec des points qui signifient les tâches de l'agenda de chaque jour et des dégradés de couleurs apaisantes en arrière-plan. C'est une façon intelligente et esthétique de visualiser votre semaine de travail.

Retrouvez un peu de temps

Alors que votre journée se remplit de réunions Zoom successives, il est trop facile de négliger le temps dont vous avez besoin pour d'autres choses, comme vous concentrer sur le travail et vous nourrir. **Reclaim est un assistant de planification pour Google Agenda qui vous permet de gagner un temps précieux.** Une fois que vous avez spécifié la durée et la fenêtre de temps pour les différentes "habitudes", Reclaim va automatiquement mélanger ces blocs de temps personnels au fur et à mesure que les réunions sont ajoutées à votre calendrier. Et si vous partagez votre calendrier avec d'autres personnes, elles verront que vous êtes occupé pendant les périodes que Reclaim vous réserve.

Pour les conservateurs de l'agenda papier

Pour les propriétaires d'iPad qui n'ont jamais été capables d'abandonner leur agenda en papier, **le Pencil Planner peut vous aider à combler le vide.** L'application prend les événements de votre calendrier numérique et les affiche à l'intérieur de surfaces de dessin semblables à du papier. Vous pouvez ainsi noter vos notes de réunion, vos objectifs, les faits marquants de la journée et les éléments de votre liste de tâches avec un Apple Pencil. Ce n'est pas la seule application qui tente d'imiter les planificateurs sur papier, mais c'est la mieux exécutée.

Maîtrisez le multimédia

Vous avez besoin d'**enregistrer l'écran de votre ordinateur à des fins de démonstration ou de tutorat?** Vous pouvez utiliser **Screen Recorder**, un site Web gratuit qui rend la tâche très simple. Il vous suffit de cliquer sur le bouton "Sélectionner l'écran", de choisir le bureau ou la fenêtre d'application que vous souhaitez capturer, puis de cliquer sur le bouton "Enregistrer". Le site prend également en charge l'entrée micro pour que vous puissiez également narrer vos captures d'écran de façon hors ligne pour des raisons de confidentialité.

N'hésitez pas à communiquer avec nous si vous souhaitez obtenir d'autres astuces pour optimiser votre productivité.

Source : Jared Newmanlong

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