Octobre 2020 • Vol. 7 n° 9

PASSION AFFAIRES ET TECHNOLOGIES

ARS solutions affaires et technologies — 30 ans

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

« On pense trop souvent que les Ransomwares, c'est pour les autres.

Nous avons été victimes d'une cyberattaque de type Cryptolocker qui a paralysé l'ensemble de nos opérations pendant 8 jours.

On n'a pas l'expertise à l'interne pour répondre à ce genre d'attaque. J'ai donc décidé de contacter ARS pour avoir une firme expérimentée et compétente chez nous dans le but de nous aider à nous remonter plus facilement et plus rapidement.

J'aurais aimé être plus conscient de mes données critiques et de comment elles étaient protégées. On s'est rendu compte que nos copies de sécurité n'étaient pas suffisantes, même si on s'en occupait à l'interne.

Si c'était à refaire, on s'informerait plus sur les types d'attaques, comment elles fonctionnent et comment on peut se protéger et faire de la prévention. »

François-Xavier Bonneville
Directeur général
Lepage Milwork

Suivez-nous

Payer la rançon pourrait vous envoyer en justice

TEMPS DE LECTURE 4:00

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 ▼

« Aujourd'hui, on peut affirmer que 95 % des solutions de sauvegardes sur le marché ne sont plus adéquates contre les nouveaux types de cyberattaques.

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 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.**

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

Webinaire pour les dirigeants

Ce n'est pas le temps pour votre entreprise de vivre tous les problèmes qu'engendre une cyberattaque. Éliminez le stress d'en être victime et restez concentré sur la croissance de votre entreprise!

Au cours de ce webinaire, vous découvrirez :

- Comprendre le phénomène, les enjeux et évaluer les risques pour votre entreprise.
- Comme dirigeant, comment dois-je gérer la cybersécurité?
- Comment se préparer à réduire l'impact sur votre entreprise?
- Quelle stratégie est à mettre en place tout de suite?

Intéressé à y participer ? Contactez-nous pour obtenir les détails - info@ars-solutions.ca • 418 872-4744 #233

4 bénéfices d'un outil de détection des cyberattaques comme le MDR

(managed detection and response)

TEMPS DE LECTURE 3:30

Nous avons regroupé en **4 catégories les bénéfices qu'apporte le MDR aux entreprises** afin de mieux répartir l'information qui est substantielle. Vous noterez que certains éléments peuvent se retrouver dans plus d'une catégorie.

Outil de contrôle financier

Le MDR permet de limiter **les dommages financiers, le déficit d'image de marque ainsi que les impacts sur les opérations, les clients et les employés.**

Dans un contexte où **la majorité des entreprises ont d'importants défis de recrutement et doivent fonctionner à ressources réduites**, le MDR amène l'assurance d'identifier rapidement des menaces et de réduire le délai de réaction. En accélérant l'identification et l'analyse des événements de sécurité, il atténue les conséquences d'attaques et facilite la restauration qui s'ensuit.

Un MDR s'avère capable de **détecter des incidents de sécurité qui seraient passés inaperçus et d'en identifier précisément l'origine** afin de mettre en place un plan correctif et préventif plus efficace :

- Détection d'attaques de logiciels malveillants tels que virus et **Ransomware**;
- Vol d'information sensible;
- Trafic anormal sur le réseau, transfert de données non autorisé, par exemple : informations sensibles envoyées à l'extérieur vers des sites douteux en Chine, Russie, etc.;
- Destruction d'information sensible par un employé ou un externe telle qu'une liste de clients;
- Exfiltration de données, comme la copie de données sur clé USB;
- Mauvaises configurations favorisant une faille de sécurité, comme le système de caméras qui envoie des informations non autorisées à l'extérieur;
- Perte de productivité par la consommation des réseaux sociaux ou autres sites non productifs, tels que : LinkedIn, Facebook, Indeed, Jobillico.

Soutien légal, traçabilité des informations et preuves

Avec le MDR, vous avez en place des outils automatisés vous permettant de fournir sur demande les documents, lorsque demandés par les autorités légales, règlementaires ou commerciales - bureaux d'avocats, compagnies d'assurances, banques – ou requis lors d'audits:

- Capture de fichiers en vue d'analyse pour preuves légales;
- Historique des permissions de vos usagers en termes d'accès réseau;
- Qui a donné des accès non autorisés à un employé;
- Qui était et qui est toujours administrateur de vos systèmes;
- L'utilisation subversive de comptes de services et autres stratagèmes afin d'opérer incognito sur le réseau;
- Détection d'activités suspectes grâce à la corrélation de plusieurs métriques.

À partir d'une console centralisant les informations, le MDR apporte une vue globale sur l'ensemble du réseau, autant pour les activités que les permissions : qui fait quoi et quand sur les serveurs, qui accède à quoi sur le réseau et particulièrement sur les serveurs, qui a modifié les configurations, **les permissions des usagers telles que l'accès aux répertoires de l'entreprise**, etc.

Le MDR amène également une assurance de traçabilité vous permettant d'extraire des rapports : journaux d'évènements en cas de litige, appui aux suivis des audits, etc. **Il vous permet de prendre des décisions fondées sur des preuves.**

Assistance aux ressources humaines

Le MDR constitue **un outil de gestion puissant qui apporte aux ressources humaines de l'information essentielle** en situation de litiges ou de résolutions de crises. Il réduit la pression et favorise ainsi **la rétention des employés.**

Grâce à l'intelligence artificielle amenant une capacité d'apprentissage constant, le MDR en vient à connaître **les comportements habituels de vos usagers et détecte les changements d'habitudes et activités suspectes.** Ceci devient encore plus intéressant dans un contexte où le travail à distance est de plus en plus fréquent.

Lors de vos rencontres de ressources humaines, vous avez donc des écrits appuyant votre démarche – avis et congédiement – et vous permettant :

- L'assainissement de la gestion de vos ressources matérielles et humaines;
- Mauvaise utilisation du matériel informatique de votre organisation : mobiles, utilisation d'Internet à des fins personnelles (recherche d'emploi, Facebook, SMS), installation de logiciels non autorisés mettant à risque l'entreprise;
- Vous savez ainsi comment vos employés utilisent les ressources matérielles et logiciels de votre réseau et pouvez intervenir au bon moment;
- Un meilleur contrôle des accès Internet : qui accède à des sites non productifs - pornographie, Facebook, Instagram, etc. - et à quelle fréquence;
- De savoir si vos télétravailleurs sont vraiment branchés comme convenu et à quels fichiers ils ont accédé.

Support à la conformité des normes

Le MDR permet de satisfaire aux exigences légales de conformité de votre entreprise. Il collecte des données et les place dans un référentiel central à des fins d'analyse de tendances. La génération de rapports de conformité est ainsi automatisée et centralisée. Les opérateurs comme les dirigeants ont accès à des vues d'indicateurs personnalisés et peuvent **alléger la charge des audits en générant eux-mêmes des rapports.**

Le MDR répond donc à plusieurs exigences de sécurité (historiques, rapports de sécurité) pouvant **générer sans effort des rapports hautement personnalisables** selon les exigences des différentes règlementations.

N'hésitez pas à nous contacter pour obtenir plus d'informations sur les bénéfices d'un outil de détection des cyberattaques au sein de votre entreprise.

10 gadgets intelligents de bureau à domicile pour stimuler votre productivité

Ce n'est plus un choix pour beaucoup d'entre nous : le travail à domicile devient peu à peu la nouvelle norme. Est-ce bien ou non? Disons qu'il y a des avantages et des inconvénients.

Il s'agit d'apprendre à concilier vie professionnelle et vie privée et de faire le lien entre les deux de la meilleure façon possible. Mais, pouvez-vous y arriver sans les meilleurs gadgets et équipements à vos côtés? Il est possible que non. C'est pourquoi ce guide présente les meilleurs gadgets et équipements de travail à distance que vous pouvez obtenir pour augmenter votre productivité dans le confort de votre foyer.

Voici donc 10 gadgets intelligents de bureau à domicile pour stimuler votre productivité :

Uhuru Minim Rise Sit/Stand Workstation

Avec le poste de travail assis/debout Uhuru Minim Rise, vous décidez si vous voulez vous asseoir ou rester debout. Ce bureau innovant comprend deux bureaux en un et est doté d'un système d'élévation électronique. Il dispose également de prises d'alimentation et de connecteurs HDMI et USB. Mieux encore, vous pouvez cacher vos fils quand vous le souhaitez grâce au flip top.

AiT Smart One App-Controlled Desk

Ce bureau de travail est tout ce dont vous avez besoin et plus encore puisque vous pouvez ajuster sa hauteur pour répondre à vos besoins directement de votre téléphone intelligent. De plus, les caractéristiques supplémentaires comprennent un tiroir de sécurité, un chargeur sans fil, un éclairage LED d'ambiance, un diffuseur d'aromathérapie et plus encore.

UPPERCASE Designs ZERO Aluminum Headphone Stand

Affichez et protégez vos écouteurs simultanément avec le support pour écouteurs en aluminium UPPERCASE Designs ZERO. Ce gadget est en aluminium de qualité aérospatiale et sa finition noir mat lui donne une touche d'élégance. Vous n'aurez plus besoin de ranger vos écouteurs dans le tiroir de votre bureau grâce à ce magnifique support.

DTEN Zoom for Home Remote Office Device

Le DTEN Zoom for Home Remote Office Device est l'un des gadgets domestiques qui vous aideront à être plus productif. Cet appareil combine une tablette et un ordinateur portable. Il dispose également de 8 microphones réducteurs de bruit et est relié au logiciel Zoom. Vous adorerez l'interface facile à utiliser pour vos contacts, notes et réunions.

Phone Toaster Multipurpose Smartphone Sanitizer

Gardez votre téléphone propre, à la manière des fantaisistes, avec le désinfectant pour téléphone portable Phone Toaster Multipurpose Smartphone Sanitizer. Ce désinfectant en forme de grille-pain élimine les germes grâce à 5 LED UV-C qui nettoient votre téléphone en 5 minutes seulement. De plus, ce gadget est également un chargeur sans fil, un réveil, un port de recharge externe, etc.

Acer ConceptD 100 Professional Creator Computer

L'ordinateur Acer ConceptD 100 est compact et puissant. Ce bureau vous permet de créer vos projets de conception en 2D en plus de la modélisation en 3D. Mieux encore, il offre 32 gigaoctets de RAM et deux téraoctets de stockage!

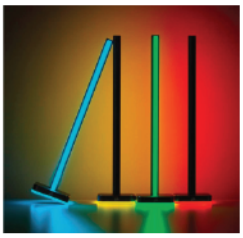
Heckler iPad Desk Stand Tablet Holder

Le support de tablette de bureau pour iPad de Heckler soutient votre tablette dans une position ergonomique afin que vous puissiez créer un espace de travail temporaire n'importe où. Parfait pour une utilisation à la maison ou au bureau, ce gadget prévient également les tensions cervicales, car il maintient votre appareil dans une position idéale.

Seagate One Touch SSD Tiny External Drive

Un autre élément formidable dans la liste des gadgets domestiques est le petit disque externe Seagate One Touch SSD. Ce disque externe a de la place pour tous vos gros fichiers. Vous pouvez choisir entre les versions de 500 gigaoctets ou d'un téraoctet, qui ont toutes deux une vitesse de 400 MBps.

CORSAIR iCue LT100 Smart Lighting Towers Ambient LED Kit



Éclairez votre espace de travail avec le kit d'ambiance CORSAIR iCue LT100. Ces tours d'éclairage intelligent vous offrent une large gamme de couleurs LED pour étendre les capacités RGB (rouge, vert, bleu) de votre PC puisque chaque tour comprend 46 LED. Choisissez l'effet d'onde ou l'effet stroboscopique pour un résultat impressionnant qui rendra le travail à domicile beaucoup plus amusant.

Netgear Nighthawk Tri-Band AX12 4K Wi-Fi Router

Le routeur Wi-Fi Tri-Band AX12 4K de Netgear Nighthawk élimine les problèmes de connexion. Et vous savez à quel point c'est important. Ce gadget augmente la vitesse d'Internet sans délai et peut prendre en charge jusqu'à 12 appareils à la fois. Il est donc idéal pour les ménages comptant plusieurs utilisateurs en télétravail.

Le travail à domicile étant la nouvelle norme, il ne s'agit pas seulement d'une tendance. Même si l'on prévoit que l'avenir ne sera peut-être pas totalement différent qu'avant la pandémie, il y aura toujours un équilibre entre le travail au bureau et le travail à domicile pour une productivité maximale. Ainsi, lorsqu'il s'agit de concevoir un bureau à domicile parfait, vous devez vous assurer que vos gadgets et votre équipement sont adaptés à un horaire de travail flexible.

Source : Lauren Wadowsky

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