Janvier 2021 • Vol. 8 n° 1

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies

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

BONNE ANNÉE 2021

À TOUS NOS CLIENTS

Merci d'être là pour nous depuis toutes ces années et de nous permettre de faire la différence en contribuant à votre succès d'affaires.

Toute l'équipe d'ARS Solutions vous souhaite une bonne et heureuse année couronnée de succès !

Que cette nouvelle année soit pour vous riche en projets et moments inspirants. Qu'elle soit également une opportunité de dépassement de soi et de fierté.

Suivez-nous

Microsoft Teams

Un outil d'amélioration du rendement de vos employés

TEMPS DE LECTURE 4:00

Cet outil de collaboration n'est pas seulement là pour faciliter la vie des employés. Il permet aussi de fournir aux gestionnaires de nombreuses données sur leurs usagers.

Il y a quelques semaines, le PDG de Microsoft, Satya Nadella, a déclaré, dans une interview au Financial Times, que **Teams pourrait bientôt être une plateforme numérique aussi importante que le navigateur Internet.** Le monde semble avoir évolué assez rapidement ces derniers temps avec la pandémie qui a poussé des millions de travailleurs à se tourner vers Microsoft Teams. La société a fait grandement jaser avec **sa fonction *365 Productivity Score***, qui semblait évaluer individuellement la productivité des employés.

SUITE À LA PAGE 2 ▼

SUITE DE LA PAGE 1 ▲

VOYONS VOIR COMMENT TEAMS PEUT CONTRIBUER À L'AMÉLIORATION DU RENDEMENT DE VOS EMPLOYÉS :

1. FAIRE ÉQUIPE AVEC L'INFORMATION. Dès le mois de juin, **Microsoft a expliqué qu'elle enregistrait les activités des équipes au profit des employeurs et que c'était à eux de décider ce qu'ils en faisaient** : « Nos clients sont les responsables du traitement des données fournies à Microsoft, tel qu'indiqué dans les conditions des services en ligne et ils déterminent les bases juridiques du traitement ». Les équipes passent l'aspirateur sur tous vos chats, messages vocaux, réunions partagées, fichiers, transcriptions, les détails de votre profil, y compris votre adresse électronique et votre numéro de téléphone.

En septembre, Microsoft a offert un peu plus d'informations sur le rapport d'activités des équipes : « Le tableau vous donne les détails d'utilisation par usager ». **Tout est enregistré, du nombre de réunions organisées par l'utilisateur au nombre de messages urgents qu'il a envoyés.** Même le temps de partage d'écran des individus est indiqué. C'est remarquablement détaillé. Un mois plus tard, la société a proposé « une nouvelle expérience d'analyse et de rapports pour Microsoft Teams » : mesure des paramètres de confidentialité, des types d'appareils, d'horodatage, des raisons pour lesquelles une personne a pu être bloquée et du nombre de messages qu'un utilisateur a envoyés dans un chat privé.

VOICI QUELQUES EXEMPLES DE DONNÉES RÉCOLTÉES PAR USAGER :

Le nom d'utilisateur est le nom d'affichage de l'utilisateur. Vous pouvez cliquer sur le nom d'affichage pour accéder à la page de configuration de l'utilisateur dans le centre d'administration de Microsoft Teams.
Les messages du canal sont le nombre de messages uniques que l'utilisateur a postés dans un chat d'équipe pendant la période spécifiée.
Les messages de réponse sont le nombre de messages de réponse uniques que l'utilisateur a postés dans un canal d'équipe pendant la période spécifiée.
Le nombre de messages postés est le nombre de messages postés uniques par l'utilisateur dans un canal d'équipe pendant la période spécifiée.
Les messages de chat sont le nombre de messages uniques que l'utilisateur a postés dans un chat privé pendant la période spécifiée.
Les messages urgents sont le nombre de messages urgents que l'utilisateur a postés dans un chat pendant la période spécifiée.

2. DES RAISONS DE S'INQUIÉTER? Certains employés s'inquiètent toutefois de l'ampleur du travail de surveillance potentiel des équipes. Par exemple, Teams enregistre-t-elle vraiment les messages réels qu'un utilisateur envoie dans un chat de Teams? Est-ce qu'un employé peut faire quelque chose pour améliorer la confidentialité? Voici la réponse d'un porte-parole de l'entreprise : « Chez Microsoft, nous pensons que les données sont essentielles pour permettre aux employés et aux organisations d'en faire plus ». « Nous pensons également que le respect de la vie privée est un droit de l'homme et nous sommes profondément engagés envers la vie privée de chaque personne qui utilise nos produits. Seul l'administrateur global a des droits sur l'expérience d'analyse et de rapport, qui permet de comprendre la manière dont l'organisation utilise Microsoft Teams et non de s'attarder au contenu du message en soi ».

3. UNE BONNE GESTION D'ÉQUIPE? Du point de vue de Microsoft, vous pourriez voir le dilemme (commercial). Vous voulez impressionner vos clients et obtenir leur engagement total, mais vous savez que la protection de la vie privée est un sujet important. Vous essayez donc d'offrir le plus possible, en demeurant le plus près possible de la ligne de conduite en matière de respect de la vie privée et au-delà du score de productivité.

Bien qu'il ne faut pas oublier ce que les employés font réellement par opposition à ce que les données pourraient « dire » qu'ils font, **les données demeurent tout de même un soutien légal par la traçabilité des informations et la transmission de preuves.** L'important est d'être transparent avec vos employés en les informant des données auxquelles vous avez accès et par l'établissement d'une politique de confidentialité.

Source : Chris Matyszczyk pour Technically Incorrect

RANSOMWARE

Même si vous payez la rançon, vos données ne seront toujours pas effacées…

3:45 TEMPS DE LECTURE

De plus en plus de cybercriminels conservent les données volées après une attaque, même si la victime a payé une rançon pour leur suppression (d'après un rapport récemment publié par Coveware, basé sur les chercheurs en sécurité de ZDNet).

Vol de données et publication en ligne

La situation dont on parle ici vise certains types d'attaques par ransomwares où les attaquants ciblent des entreprises et organisations gouvernementales ne pouvant se permettre de longues périodes d'arrêt. L'idée dans ce cas-ci est de menacer les victimes de publier des informations sensibles en ligne, afin qu'elles paient la rançon plutôt que de restaurer leur réseau à partir de sauvegardes.

Certains groupes ont même créé des portails spécialisés (appelés *leak sites*) où ils publient les données des entreprises qui refusent de payer la rançon demandée. Si elles acceptent de payer la clé de déchiffrement, les cyberattaquants promettent de supprimer les données volées.

Il faut toutefois savoir que les fraudeurs respectent rarement leurs promesses et que vous ne pourrez jamais avoir la certitude que vos données ne sont plus en circulation sur le Net. Certains fournissent des preuves de suppression falsifiées et reviennent à la charge avec d'autres demandes de paiement une semaine après le versement de la rançon par les victimes (double extorsion).

La meilleure stratégie à adopter

Ne pas payer la rançon! La clé, c'est l'anticipation. En mettant en place **un programme global de cybersécurité**, vous serez en mesure de faire face aux cyberattaques et de détecter les tentatives d'exfiltration. Ce programme doit comprendre à la fois une stratégie de sauvegardes adaptée, une cybersurveillance ainsi que la sensibilisation de vos employés face aux tentatives d'hameçonnage.

Il ne faut pas oublier qu'on met en moyenne **160 jours avant de détecter une brèche** si on n'a pas les outils en place. Ce qui veut dire que les cyberattaquants ont amplement le temps d'exfiltrer des données sensibles. Trop d'entreprises se retrouvent encore au pied du mur et se sentent dans l'obligation de payer la rançon. Pourtant, il existe des outils qui leur sont accessibles.

Le FBI et la majorité des experts en cyberattaques s'entendent sur le fait de ne pas payer les cybercriminels puisque vos chances de récupérer vos données sont minces et que ceci encourage la cybercriminalité.

Derrière les coulisses du *Ransomware as a Service*

Ce sont les groupes comme Maze et ses filiales qui offrent aux cybercriminels un **accès à leur plateforme de *leak site* comme un *Ransomware as a Service (RaaS)***. Les fraudeurs paient un abonnement annuel et peuvent ainsi publier les données volées aux entreprises. Maze et ses filiales auraient publié accidentellement des données sur leur plateforme avant même d'avoir avisé les victimes du vol de leurs fichiers. Il y a également eu des cas de publication même après le paiement d'une rançon. Ces incidents ont aussi eu lieu avec d'autres groupes. Les données ont finalement été retirées, mais ont été lues et téléchargées par des centaines, voire des milliers de personnes. Si vous mettez en place les outils nécessaires, ces groupes devront alors se contenter du peu de données qu'ils auront réussi à voler avant que le chiffrement ne soit détecté et bloqué.

Connaître les menaces, les anticiper, se préparer à une crise causée par une cyberattaque et agir adéquatement sont les éléments clés que les entreprises doivent maîtriser dès maintenant pour limiter ou annuler l'impact sur leurs activités. **La meilleure stratégie est de vous préparer.**

Source : ZDNet.com

Rançongiciels

Votre entreprise est-elle prête à faire face aux dernières versions d'attaques par rançongiciel?

Inscrivez-vous avant le 28 février 2021 pour une évaluation SANS FRAIS de votre stratégie de sauvegardes!

- Évaluation de votre mode de fonctionnement actuel en cas de rançongiciels
- Analyse de votre processus de sauvegardes en place
- Rapport d'observations et de recommandations
- En toute confidentialité avec la signature d'une entente

Contactez-nous au : info@ars-solutions.ca • 418 872-4744 #233

L'importance d'avoir une politique de télétravail en période de pandémie

3:45 TEMPS DE LECTURE

La proportion des télétravailleurs québécois est passée de 10 % à 57 % en raison de la pandémie. Puisque la transition n'était pas prévue et qu'elle s'est faite très rapidement, **aucune loi spécifique n'a encore été établie concernant le télétravail.** Afin d'éviter les différends entre les employeurs et les télétravailleurs, l'idéal serait **d'établir une politique ou une entente sur le télétravail** qui toucherait, entre autres, des points comme les suivants : obligations employeur/employé, équipement et matériel fourni, horaire et déplacements exigés, modes de communication, procédures, clause de renonciation à la protection au droit à la vie privée (par employé), etc. Cette solution vous évitera les complications des enjeux légaux engendrés par l'obligation de travailler de la maison.

Les chartes et le droit à la vie privée

Certains employeurs vont parfois exiger à leurs employés d'activer leur caméra lors d'une vidéoconférence, que ce soit pour dynamiser la réunion, vérifier qu'ils sont bien à leur domicile ou s'assurer que leur lieu de travail est sécuritaire. Cependant, cette obligation contrevient à certains points de la Charte des droits et libertés de la personne (RLRQ, c. C-12) : « **5. Toute personne a droit au respect de sa vie privée.** 6. Toute personne a droit à la jouissance paisible et à **la libre disposition de ses biens**, sauf dans la mesure prévue par la loi. »

Il y aurait toutefois 2 façons de contourner cette atteinte aux droits fondamentaux, notamment par l'acceptation de l'employé face aux conditions de travail associées à l'exercice de sa prestation de travail en télétravail et par la démonstration de l'employeur que l'atteinte est justifiée, par exemple lorsque le gouvernement annonce un confinement obligeant la fermeture des bureaux.

Loi sur les normes du travail

L'employeur fournit habituellement les outils et l'équipement nécessaires à l'exécution des tâches de l'employé. Mais jusqu'où l'employeur doit-il aller en contexte de télétravail? Si la climatisation est fournie au bureau, doit-elle l'être également au domicile de l'employé? D'où l'importance de rédiger un contrat de travail qui précise ce genre d'engagements reliés au milieu de travail. Si l'employé accepte le télétravail, vous pourriez d'ailleurs lui faire renoncer à la clause sur l'obligation de lui fournir le même environnement qu'au bureau.

La santé et la sécurité au travail

L'employeur a plusieurs obligations en ce qui concerne la santé et la sécurité au travail. Par exemple, il doit **« s'assurer que l'organisation du travail et les méthodes et techniques utilisées pour l'accomplir sont sécuritaires et ne portent pas atteinte à la santé du travailleur »** (art.51 par. 3). Comment concilier les obligations de l'employeur et le respect au droit à la vie privée de l'employé? Pour assurer l'ergonomie de l'espace de travail, il est possible d'exiger la visite d'un ergonome au domicile de vos employés et pour la santé ainsi que la sécurité de ceux-ci, il est préférable d'effectuer un rappel des principes et de la politique.

La confidentialité

L'exportation des données de l'entreprise au domicile de l'employé devient un enjeu de sécurité pour plusieurs employeurs, car ils ont peu de contrôle sur l'environnement de travail et les personnes ayant accès au matériel. **Cela augmente le risque de fuite de données et met à risque votre entreprise.** Sachez toutefois que vos employés ont une obligation à respecter à ce sujet : art. 2088 du Code civil du Québec : « 2088. Le salarié, outre qu'il est tenu d'exécuter son travail avec prudence et diligence, doit agir avec loyauté et honnêteté et **ne pas faire usage de l'information à caractère confidentiel** qu'il obtient dans l'exécution ou à l'occasion de son travail. »

Sur les employeurs sondés aux fins d'un sondage mené par Léger pour le compte de la Chambre de commerce et d'industrie de Québec, **10 % des employeurs croient que les employés sont plus productifs en télétravail**, 62 % n'y voient pas de différence et 24 % sont persuadés que les employés sont plus efficaces au bureau. **93 % des employeurs ont pris ou prendront les mesures pour faire revenir les employés au bureau.** S'agit-il ici d'un problème de gestion, de législation, d'adaptation ou de confiance? Chose certaine, il faudra apprendre à vivre avec cette nouvelle réalité, car l'obligation de travailler à distance ne semble pas prête d'être levée...

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