Septembre 2021 • Vol. 8 n° 8

PASSION AFFAIRES *et technologies*

ARSolutions affaires et technologies

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

« Avec ARS, nous pouvons nous concentrer sur la gestion et la croissance de notre entreprise...

Avec les différentes mesures mises en place par ARS en matière de sécurité, nous savons que notre entreprise est bien supportée dans la protection contre les cyberattaques.

ARS nous a guidés dans l'apprentissage des cybermenaces, comment les prévenir et les identifier, ce qui nous permet de focaliser l'esprit tranquille sur la gestion et la croissance de notre entreprise. »

ORTHOFAB

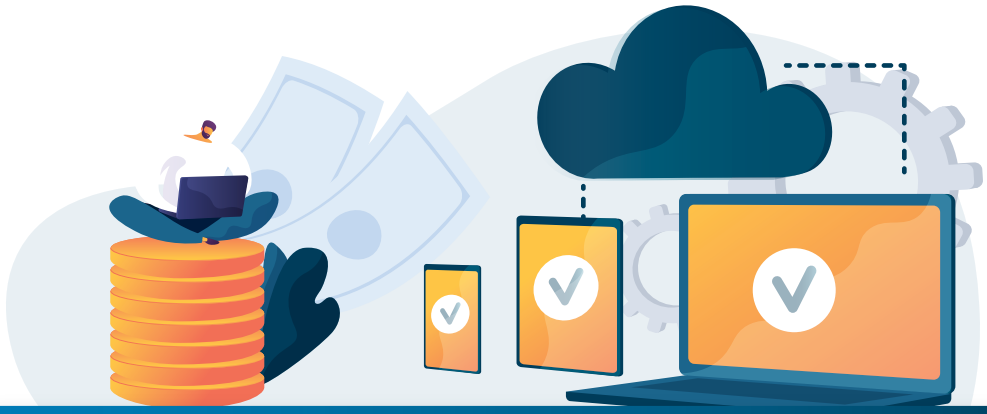
Marie-Andrée Lapierre
Vice-présidente/directrice de l'exploitation
Orthofab

Suivez-nous

Affaires-TI

Les coûts du cloud suscitent un nouveau débat

TEMPS DE LECTURE 2:30



En 2011, Marc Andreessen a déclaré que le cloud allait envahir le monde. Le mois dernier, deux membres de sa société d'investissement Andreessen Horowitz ont fait valoir que le cloud a monopolisé l'argent des entreprises.

En 2018, nous avions rédigé un article sur les coûts imprévisibles et difficiles à contrôler du cloud dans lequel on faisait mention que **37 % des organisations considéraient déjà que les coûts imprévisibles représentaient un problème majeur,** selon le sondage SoftwareONE.

Dans un article intitulé "The Cost of Cloud, a Trillion Dollar Paradox" (Le coût du cloud, un paradoxe de plusieurs milliards de dollars), **Martin Casado et Sarah Wang, investisseurs associés d'Andreesen Horowitz, ont procédé à une analyse des coûts du cloud en se basant sur une cinquantaine de sociétés de logiciels publiques. Leur conclusion était qu'en opérant à grande échelle, le coût du cloud pouvait doubler la facture d'infrastructure d'une entreprise.**

Ils estiment la valeur du marché à 100 milliards de dollars, en raison de l'impact des coûts du cloud sur les marges. Une entreprise citée dans l'article a constaté que les prix du cloud public étaient **10 à 12 fois supérieurs au coût d'exploitation de son propre centre de données.**

« Le problème avec l'article d'Andreessen, c'est qu'il ne voit pas ce qui concerne le coût lui-même », a déclaré M. Rich Hoyer, directeur des clients FinOps chez SADA Inc., dans une interview accordée à SiliconANGLE.

SUITE À LA PAGE 2 ▼

« La façon dont une entreprise devrait envisager la question est de faire une analyse du retour sur investissement de ses coûts de cloud. Ne prenez pas la décision en vous basant sur le fait qu'elle est moins chère. Demandez-vous comment les charges de travail vont améliorer les opérations de l'entreprise pour créer de nouvelles opportunités ».

L'exemple de Dropbox

L'analyse d'Andreessen s'est attirée des critiques en citant Dropbox Inc. comme un exemple frappant. Il y a environ 8 ans, **Dropbox a pris la décision de migrer les milliards de fichiers de 500 millions d'utilisateurs d'Amazon Web Services inc. (AWS) vers une infrastructure personnalisée dans des centres de colocation.** Cette décision a permis d'économiser près de 75 millions de dollars sur une période de 2 ans avant son introduction en bourse en 2018, selon les chercheurs.

Le rapatriement réexaminé

Une enquête menée en novembre dernier par Arlington Research auprès de 350 décideurs en matière de TI a révélé que **72 % des personnes interrogées avaient déplacé une ou plusieurs applications d'un cloud public vers une infrastructure sur site.** Les données les plus récentes d'Enterprise Technology Research ont montré que **55 % des entreprises interrogées prévoyaient augmenter leurs dépenses avec AWS en 2021.**

Des coûts plus élevés pour le cloud

Bien qu'il n'y ait pas encore de mouvement massif des charges de travail de la part du nuage public, le coût d'admission mérite tout de même d'être examiné. Les commentaires de Casado sur son fil Twitter ont noté que l'analyse comparative menée par sa recherche avec Wang a révélé que **les dépenses de cloud représentaient environ 50 % du coût des marchandises, et ont même atteint 80 % dans le cas d'une grande entreprise.**

Le coût contre la charge de travail

Les principaux fournisseurs de cloud auront une décision critique à prendre. Vont-ils réduire leurs prix et sacrifier leurs marges bénéficiaires ou rester fermes et accepter la perte de charges de travail au profit de l'infrastructure sur site? Cette décision représente une somme d'argent considérable. Gartner, une entreprise américaine de conseil et de recherche dans le domaine des techniques avancées, prévoit que **les dépenses liées au cloud public atteindront 304 milliards de dollars rien qu'en 2021, contre 257 milliards l'année précédente.**

Ce qui est peut-être plus significatif du point de vue de l'entreprise, c'est que les deux plus grands fournisseurs de cloud public - AWS et Microsoft Corp - sont les deuxième et quatrième plus grandes entreprises du monde en termes de capitalisation boursière suivies par Google LLC.

Aucun des dirigeants consultés pour cet article n'était prêt à accepter que l'un des principaux fournisseurs de services en cloud atteigne cette augmentation très bientôt. Ces sociétés sont trop bien capitalisées et le niveau d'innovation serait difficile à égaler. « Tant que ces fournisseurs de cloud public continueront à fournir de nouveaux services innovants, je pense qu'ils pourront continuer à imposer des coûts plus élevés », a déclaré M. Travis Rehl, vice-président du produit chez CloudCheckr.

Source : Mark Albertson

Les utilisateurs d'Office 365

visés par une nouvelle attaque d'hameçonnage

TEMPS DE LECTURE 1:50

Les utilisateurs d'Office 365 sont désormais dans le collimateur des cybercriminels dans le cadre d'une nouvelle campagne d'hameçonnage, selon un avertissement que l'équipe de Microsoft Security Intelligence (MSI) a publié sur Twitter.

Les malfaiteurs utilisent des **adresses électroniques qui semblent légitimes avec des noms d'expéditeur qui imitent des services de bonne foi pour esquiver les filtres de messagerie.** Microsoft avertit que les cybercriminels se surpassent pour utiliser des techniques d'évasion de détection qui ont une apparence authentique et convaincante. Microsoft met donc en garde les utilisateurs d'Office 365 contre cette nouvelle campagne d'hameçonnage astucieuse et inquiétante.

« Une campagne d'hameçonnage active utilise des adresses courriel usurpées d'expéditeurs d'apparence légitime et leurs messages contiennent les noms d'utilisateurs et les domaines cibles **pour essayer de passer à travers les filtres de messagerie »**, a expliqué MSI sur Twitter.

La campagne d'hameçonnage cible les organisations utilisant Office 365 et dont les employés envoient souvent des pièces jointes à leurs collègues. MSI a trouvé des courriels d'hameçonnage qui semblaient être envoyés par une source fiable. Plusieurs de ces courriels contenaient de fausses pièces jointes Microsoft SharePoint portant des étiquettes telles que "Livres de prix", "Primes" et "Rapports du personnel".

Les cybercriminels utilisent une tactique appelée "typosquatting" qui consiste à enregistrer des domaines mal orthographiés qui, à première vue, semblent proches d'une marque connue. La plupart des lecteurs rapides négligeraient la subtile faute de frappe.

Si les utilisateurs mordent à l'hameçon et cliquent sur le lien "Ouvrir", ils sont dirigés vers une **page qui les incite à saisir leurs informations d'identification Microsoft ou Google.** Selon MSI, ces pages d'ouverture de session sont très convaincantes et font croire aux utilisateurs qu'ils sont sur un site Web légitime.

MSI n'a cessé de souligner l'apparence authentique de ces courriels d'hameçonnage. **Les employeurs ne peuvent donc pas toujours compter sur le bon jugement de leurs employés** pour identifier les courriels suspects. C'est pourquoi MSI a lancé son programme Microsoft Defender pour Office 365 comme solution, ajoutant que ce logiciel "détecte et bloque" ces courriels.

Donc en cas de doute, ne cliquez sur rien et avisez rapidement votre fournisseur TI pour vérifier la légitimité d'un courriel et éviter sa propagation. N'hésitez pas à nous contacter pour obtenir de l'aide.

Source : Kimberly Gedeon

Vous pouvez empêcher Google de savoir où vous êtes 24/7

3:00 TEMPS DE LECTURE

Si vous utilisez une application Google, l'historique de votre localisation et de vos données peut être stocké. Voici comment désactiver les services de localisation et supprimer l'historique de vos localisations.

Bien que la désactivation de l'historique des localisations semble être une opération suffisante, **certaines applications de Google stockent toujours vos données de localisation,** comme l'a exploré une enquête de 2018 de l'Associated Press. Le simple fait d'ouvrir l'application Google Maps ou d'utiliser Google sur n'importe quelle plateforme pour une recherche enregistre votre emplacement approximatif avec un horodatage. Depuis cette enquête, cependant, Google a facilité le contrôle des données de localisation qui sont enregistrées, et de celles qui sont supprimées, grâce à des fonctionnalités comme "Vos données" dans Maps et Search, qui vous permettent d'accéder rapidement à vos contrôles de localisation.

La désactivation de l'historique des localisations ne supprime que les endroits où vous vous êtes rendu dans la fonctionnalité "Google Maps Timeline", qui enregistre votre position avec certaines données à un moment précis. Sur la page d'assistance de Google consacrée à ce sujet, on peut lire que, même lorsqu'elles sont désactivées, "certaines données de localisation peuvent continuer à être enregistrées dans d'autres paramètres", comme votre activité sur le Web et dans les applications. Google a indiqué qu'il utilisait ces données pour personnaliser davantage les fonctionnalités et les rendre plus utiles, et que ces informations n'étaient jamais communiquées à des tiers ou à des annonceurs. Mais si ça ne vous convient toujours pas, en suivant quelques étapes supplémentaires, **vous pouvez éviter que Google enregistre votre emplacement 24 heures sur 24, 7 jours sur 7.**

Notez simplement que **la désactivation de ce paramètre par défaut présente quelques inconvénients.** Si les paramètres de Google peuvent sembler intrusifs pour certains, ils contribuent également à créer une expérience en ligne ultra-personnalisée, en aidant par exemple les internautes à trouver des commerces à proximité plutôt que dans une autre ville, ou à voir des annonces personnalisées. Selon Google, ces paramètres permettent de fournir aux utilisateurs des informations plus pertinentes que des informations aléatoires.

Notez que pour utiliser efficacement certaines fonctionnalités, comme l'application Maps, Google devra toujours accéder à votre position. Toutefois, en suivant ces 7 étapes, vous évitez que Google ne stocke vos activités futures. Lorsque Google horodate votre activité dans une zone générale, il s'agit d'une zone de plus d'un kilomètre carré comptant généralement plus de 1 000 utilisateurs, afin de protéger la vie privée. La page d'aide de Google à ce sujet indique que cela permet de détecter une activité inhabituelle, telle qu'une connexion depuis une autre ville, tout en préservant la vie privée. Toutefois, **vous pouvez accorder à Google l'autorisation d'utiliser votre localisation précise** - votre emplacement exact, comme une adresse spécifique - pour obtenir les meilleurs résultats de recherches et les plus précis concernant l'endroit où vous vous trouvez.

Vous pouvez donc **préserver votre vie privée et perdre l'expérience personnalisée** de l'Internet, ou **continuer à voir des annonces et des suggestions de recherches pertinentes** au lieu d'informations plus aléatoires et non filtrées.

Source : Kelsey Fogarty

Voici comment désactiver complètement le suivi de localisation de Google :

1. **Ouvrez le site Google.com sur votre ordinateur de bureau ou votre navigateur mobile.**
2. **En haut à droite, connectez-vous à votre compte Google si vous ne l'êtes pas déjà.**
3. **Sélectionnez "Gérer votre compte Google".**
4. **Dans le cadre "Confidentialité et personnalisation", sélectionnez "Gérer vos données et la personnalisation".**
5. **Faites défiler l'écran jusqu'aux "Contrôles d'activité", puis sélectionnez "Gérer vos contrôles d'activité".**
6. **Vous y verrez une case intitulée "Activité Web et applications". À partir de là, vous pouvez faire glisser l'interrupteur à bascule vers la désactivation.**
7. **Avant de sélectionner "Pause", une information vous sera communiquée pour vous permettre de comprendre les effets de la désactivation de ce paramètre.**

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