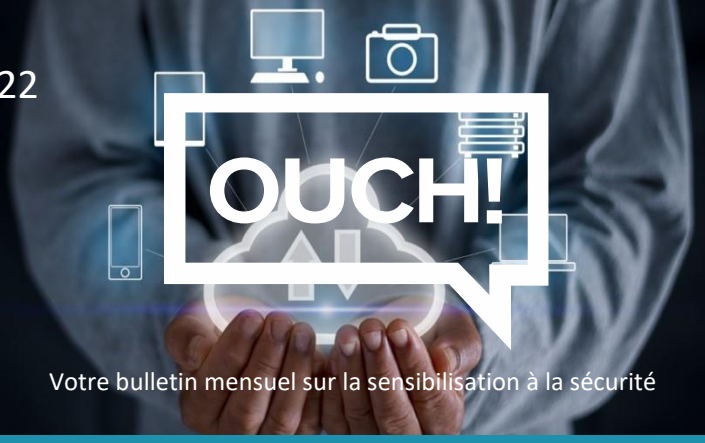
OUCH! Septembre 2022



Votre bulletin mensuel sur la sensibilisation à la sécurité

Faites-vous des sauvegardes ?

Aperçu

Si vous utilisez un ordinateur ou un appareil mobile assez longtemps, tôt ou tard finira par mal tourner. Vous pouvez supprimer accidentellement les mauvais fichiers, avoir une panne matérielle ou perdre un appareil. Ou même pire, un virus peut infecter votre appareil et effacer ou crypter vos fichiers. Dans ces moments-là, les sauvegardes sont souvent le seul moyen de reconstruire votre vie numérique.

Les sauvegardes sont des copies de vos informations stockées ailleurs que sur votre ordinateur ou votre appareil mobile. Lorsque vous perdez ou ne pouvez pas accéder à des données importantes sur votre appareil, vous pouvez les récupérer à partir de sauvegardes. Bon nombre des fichiers que nous créons aujourd'hui sont déjà automatiquement stockés et sauvegardés dans le nuage, comme les documents Microsoft Word stockés dans Microsoft OneDrive, Dropbox ou Google Drive, ou les photos personnelles stockées dans Apple iCloud. Mais il se peut que certains fichiers que vous créez ne soient pas automatiquement stockés dans le nuage ; ou peut-être souhaitez-vous des sauvegardes supplémentaires à des fins personnelles.

Quoi, quand et comment

La première étape est de décider ce que vous voulez sauvegarder : (1) des données spécifiques qui sont importantes pour vous ; ou (2) tout, y compris peut-être tout votre système d'exploitation. De nombreuses solutions de sauvegarde sont configurées par défaut pour utiliser la première approche et ne sauvegarder que les dossiers les plus utilisés. Si vous n'êtes pas sûr de ce que vous devez sauvegarder ou si vous voulez être très prudent, pensez à tout sauvegarder.

Deuxièmement, décidez de la fréquence de sauvegarde des données. Les programmes de sauvegarde intégrés, tels que Time Machine d'Apple ou Sauvegarde et restauration de Windows, vous permettent de créer un programme automatique "définissez-le et oubliez-le". Les options de programmation les plus courantes sont l'horaire, la journée et la semaine. D'autres solutions peuvent offrir une "protection continue" dans laquelle les fichiers sont immédiatement sauvegardés lorsqu'ils sont modifiés ou enregistrés. Au minimum, nous recommandons des sauvegardes quotidiennes automatisées des fichiers critiques.
Enfin, décidez comment vous allez sauvegarder. Il y a deux façons de procéder : la sauvegarde locale ou la sauvegarde dans le nuage. Les sauvegardes locales reposent sur des dispositifs que vous contrôlez physiquement, tels que des lecteurs USB externes ou des dispositifs accessibles par le réseau. L'avantage des sauvegardes locales est qu'elles vous permettent de sauvegarder et de récupérer rapidement de grandes quantités de données. L'inconvénient est que si vous êtes infecté par un logiciel malveillant, il est possible que l'infection se propage à vos sauvegardes. De plus, en cas de catastrophe, comme un incendie ou un vol, vous pourriez perdre vos sauvegardes ainsi que votre ordinateur.

Si vous utilisez des dispositifs externes pour les sauvegardes, stockez une copie hors site dans un endroit sûr et assurez-vous que vos sauvegardes sont correctement étiquetées. Pour plus de sécurité, pensez à crypter vos sauvegardes.

Les solutions basées sur le cloud sont des services en ligne qui sauvegardent et stockent vos fichiers sur internet. En général, vous installez une application sur votre ordinateur. L'application sauvegarde ensuite automatiquement vos fichiers, soit selon un calendrier défini, soit lorsque vous les modifiez ou les enregistrez. Parmi les avantages des solutions en nuage, citons leur simplicité, l'automatisation des sauvegardes et l'accès aux fichiers depuis presque n'importe où. De plus, comme vos données résident dans le nuage, les catastrophes domestiques telles qu'un incendie ou un vol n'affecteront pas votre sauvegarde. Le principal inconvénient est la bande passante qu'il consomme. Votre capacité de sauvegarde et de restauration dépend de la quantité de données que vous sauvegardez et de la vitesse de votre réseau. Vous ne savez pas si vous voulez utiliser des sauvegardes locales ou dans le nuage ? Soyez très prudent et utilisez les deux.

Avec les appareils mobiles, la plupart de vos données, comme les e-mails, les SMS ou les photos que vous prenez, sont automatiquement stockées dans le nuage. Toutefois, les configurations de votre application mobile, les préférences du système et d'autres fichiers peuvent ne pas être stockés dans le nuage. En sauvegardant automatiquement votre appareil mobile, non seulement vous préservez ces informations, mais il est plus facile de transférer vos données lorsque vous passez à un nouvel appareil.

Points clés supplémentaires

- Testez régulièrement le fonctionnement de vos sauvegardes en récupérant et en ouvrant un fichier.
- Si vous reconstruisez un système à partir d'une sauvegarde, y compris le système d'exploitation, veillez à appliquer de nouveau les derniers correctifs de sécurité et les dernières mises à jour avant de l'utiliser à nouveau.
- Si vous utilisez une solution en nuage, choisissez-en une qui soit facile à utiliser et étudiez les options de sécurité. Par exemple, votre fournisseur de sauvegarde en nuage prend-il en charge la vérification en deux étapes pour sécuriser votre compte en ligne ?

Les sauvegardes sont un moyen simple et peu coûteux de protéger votre vie numérique.

Rédacteur Invité

Greg Scheidel est le responsable de la cybersécurité chez Iron Vine Security, avec plus de 30 ans d'expérience en informatique et en sécurité informatique. Il est également instructeur chez SANS, où il enseigne l'architecture de sécurité, l'ingénierie et la confiance zéro dans le cours SEC530. Vous pouvez le contacter sur Twitter @greg_scheidel.

Ressources

Authentification multifactorielle : https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Utiliser le cloud en toute sécurité : https://www.sans.org/newsletters/ouch/securely-using-the-cloud/
Gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/password-managers/
Héritage numérique : https://www.sans.org/security-awareness-training/resources/digital-inheritance

Traduit pour la communauté par : Juliette Busson