OUCH! | Août 2015

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Sauvegarde & Récupération

Vue d'ensemble

Tôt ou tard, vous serez confronté à un problème qui vous fera perdre vos données personnelles, vos documents ou vos photos. Cela peut aller de la suppression par erreur du mauvais fichier, à la défaillance matérielle, à la perte de votre laptop ou encore à l'infection de votre ordinateur. Dans ces moments-là, les sauvegardes sont souvent les seules solutions pour restaurer votre vie numérique. Dans cette newsletter, nous expliquons ce que sont les sauvegardes, comment sauvegarder vos données et comment développer une stratégie qui vous convienne.

Editeur invité

Heather Mahalik est une experte criminalistique reconnue dans le monde de l'industrie, spécialisée dans l'analyse des smartphones. Elle est co-auteur de Practical Mobile Forensics, rédactrice technique de Learning Android Forensics et elle a co-écrit le FOR585 Advanced Smartphone Forensics et FOR518 Macintosh Forensics pour l'institut SANS. Vous pouvez suivre Heather sur **Smarterforensics.com** et sur Twitter : **@heathermahalik**.

Que sauvegarder et quand ?

Les sauvegardes sont des copies de vos informations qui sont stockées ailleurs. Lorsque vous perdez des données importantes, vous pouvez restaurer ces données grâce à vos sauvegardes. Le problème, c'est que la plupart des gens ne font pas de sauvegardes, ce qui est dommage puisqu'elles sont simples et peu coûteuses. Il y a deux approches quant à savoir quoi sauvegarder : (1) des données spécifiques qui sont importantes pour vous, ou (2) tout, y compris l'intégralité de votre système d'exploitation. La première approche rationalise vos sauvegardes et optimise l'espace sur votre disque dur, cependant la seconde approche est plus simple et plus complète. Si vous ne savez pas quoi sauvegarder, nous vous recommandons de tout sauvegarder.

La décision suivante consiste à savoir à quelle fréquence vous devez effectuer la sauvegarde de vos données. Les options communes proposent des sauvegardes horaires, quotidiennes ou hebdomadaires, etc. Pour les usages domestiques, les programmes de sauvegarde d'Apple Time Machine ou Windows Backup and Restore pour Microsoft vous permettent de créer une sauvegarde automatique récurrente « set it and forget it » (« programmez-la puis n'y pensez plus »). Ces solutions sauvegardent automatiquement toutes vos données pendant la journée pendant même que vous travaillez sur votre ordinateur. D'autres solutions proposent la « protection en continue » grâce à laquelle tout nouveau document ou document modifié sera immédiatement sauvegardé dès qu'il sera refermé. Nous recommandons une sauvegarde quotidienne au minimum. Finalement la question que vous devez vous poser est la suivante: « Quelle quantité d'information pourrais-je me permettre de perdre si je devais restaurer mon ordinateur depuis ma sauvegarde? »

Comment sauvegarder

Il existe deux façons de sauvegarder vos données: le support physique ou le stockage sur le Cloud. Le support physique

Sauvegarde & Récupération

signifie tout type de matériel, tels que les DVD, clés USB ou disques durs externes. Quel que soit le support que vous choisissez, ne sauvegardez jamais vos fichiers sur le même appareil qui contient vos fichiers originaux. Le problème que vous pouvez rencontrer avec les supports physiques est que si il se produit une catastrophe à votre emplacement (comme un incendie ou de vol), alors non seulement vous pouvez perdre votre ordinateur, mais les sauvegardes avec. En tant que tel, vous devriez avoir un plan pour stocker des copies de votre sauvegarde hors site dans un endroit sûr. Si vous les stockez hors site, assurez-vous de les étiqueter avec ce qui a été sauvegardé et quand. Pour une sécurité optimale, cryptez vos sauvegardes.

Les sauvegardes fiables automatisées sont souvent votre dernière ligne de défense pour la protection de vos données.

Les solutions de Cloud computing sont différentes, ces dernières ont en effet un service où vos fichiers sont stockés quelque part sur Internet. Selon la quantité de données que vous souhaitez sauvegarder, cela peut être un service payant. Il fonctionne en installant un programme sur votre ordinateur qui sauvegarde automatiquement vos fichiers à votre place. L'avantage de cette solution c'est que dans la mesure où vos sauvegardes sont sur le Cloud, si une catastrophe se produit chez vous, vos sauvegardes seront toujours en sécurité. En outre, vous pouvez accéder à vos sauvegardes, ou même souvent seulement à des fichiers individuels, à partir de presque n'importe où, même lorsque vous voyagez. L'inconvénient est que les sauvegardes sur le Cloud (et la récupération) peuvent être plus lentes, surtout si vous avez une grande quantité de données. Si vous n'êtes pas sûr que l'option de sauvegarde soit le meilleur choix pour vous (les médias physiques ou sur le Cloud), gardez à l'esprit que vous pouvez toujours faire les deux.

Enfin, n'oubliez pas vos appareils mobiles. L'avantage avec les appareils mobiles est que la plupart de vos données sont déjà stockées dans le Cloud, telles que vos e-mails, vos événements de calendrier ou vos contacts. Cependant, vous pouvez avoir des renseignements qui ne sont pas stockés dans le Cloud, telles que vos configurations d'applications mobiles, vos photos récentes et vos préférences système. En sauvegardant votre appareil mobile, non seulement vous conservez ces informations, mais il est plus facile de reconstruire un dispositif, comme lorsque vous en installez un nouveau. Un iPhone / iPad peut sauvegarder automatiquement vers le iCloud d'Apple. Les appareils mobiles Android ou d'autres dépendent du fabricant ou du fournisseur de service. Dans certains cas, vous pourriez avoir à acheter des applications mobiles conçues spécifiquement pour les sauvegardes.

Récupération

La sauvegarde de vos données constitue seulement la moitié de la bataille; vous devez être certain que vous pouvez les récupérer. Vérifiez tous les mois que vos sauvegardes fonctionnent en récupérant un fichier et en validant le contenu. En outre, soyez certains de faire une sauvegarde complète du système avant une mise à jour majeure (comme le déplacement vers un nouvel ordinateur ou appareil mobile) ou une réparation majeure (comme le remplacement d'un disque dur) et vérifiez bien qu'il est restituable.

Sauvegarde & Récupération

Points clés

- Automatisez vos sauvegardes autant que possible et vérifiez-les régulièrement.
- Lors de la reconstruction d'un système complet de sauvegarde, assurez-vous de réappliquer les derniers correctifs et mises à jour de sécurité avant de l'utiliser à nouveau.
- Les sauvegardes périmées ou obsolètes peuvent devenir un handicap, et doivent être détruites pour empêcher l'accès à des utilisateurs non autorisés.
- Si vous utilisez une solution Cloud, faites des recherches sur les politiques et la réputation du fournisseur et assurez-vous qu'il répond à vos exigences. Par exemple, a-t-il crypté vos données quand elles sont stockées? Qui a accès à vos sauvegardes? Soutient-il l'authentification forte telle que la vérification en deux étapes?

Ressources publiques

N'utilisez jamais les ordinateurs publics, tels que ceux que l'on trouve dans les halls d'hôtels, les librairies ou les cybers cafés. Vous n'avez aucune idée de qui a pu utiliser cet ordinateur avant vous, il se peut que cette personne ait, volontairement ou involontairement, infecté cet ordinateur. Lorsque cela est possible, n'utilisez que des appareils que vous contrôlez et auxquels vous faîtes confiance pour vos activités en ligne. Si vous n'avez d'autre choix que d'utiliser un ordinateur public, n'utilisez aucun service qui vous demande de vous identifier ou d'entrer un mot de passe.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.
Pour en savoir plus, veuillez vous référer aux liens suivants :
http://www.answersolutions.ch et http://answersecurity.com/

Sources

Phrases de passe :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_fr.pdf
Vérification en deux étapes :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_fr.pdf
Utilisation du Cloud en toute sécurité :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_fr.pdf
Chiffrement :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_fr.pdf
Conseil du jour :	http://www.sans.org/tip_of_the_day.php

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet