OUCH! | Août 2017

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

OUCH!

Dans ce numéro...

Sauvegarde & Récupération

Vue d'ensemble

Si vous utilisez un ordinateur ou un appareil mobile depuis assez longtemps, tôt ou tard vous serez confronté à un problème qui pourrait vous faire 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

Keith Palmgren est un professionnel de la cybersécurité avec plus de 30 ans d'expériences dans le domaine de la sécurité informatique. Il est également instructeur senior à l'institut SANS et auteur du cours SANS SEC301 ; « Introduction à la sécurité de l'information ». Keith gère la pratique de ses conseils en sécurité avec succès. Il est présent sur Twitter : **@kpalmgren**.

Sauvegardes : Quoi, quand et comment ?

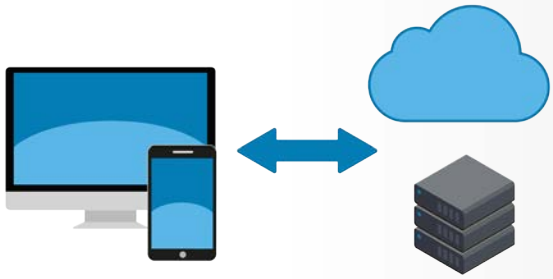
Les sauvegardes sont des copies de vos informations qui sont stockées ailleurs. Lorsque vous perdez des données importantes, vous pouvez restaurer ces données grâce à vos sauvegardes. Le problème, c'est que la plupart des gens ne font pas de sauvegardes, ce qui est dommage puisqu'elles sont simples et 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.

Dans un second temps, vous devez décider à quelle fréquence vous devez effectuer la sauvegarde de vos données. Les programmes de sauvegarde intégrés tels que « Time Machine » d'Apple ou la sauvegarde et la restauration de Microsoft Windows vous permettent de créer une sauvegarde automatique récurrente « set it and forget it » (« programmez-la puis n'y pensez plus »). Les options communes incluent chaque heure, chaque jour, chaque semaine, etc. D'autres solutions offrent une « protection continue » dans laquelle les fichiers nouveaux ou modifiés sont sauvegardés immédiatement chaque fois que vous enregistrez un document. Nous recommandons au minimum des sauvegardes quotidiennes automatisées.

Enfin, vous devez décider de la façon dont vous allez sauvegarder. Il existe deux façons de sauvegarder vos données : les médias physiques ou le stockage basé sur le Cloud. Chaque approche présente des avantages et des inconvénients. Si vous n'êtes pas sûr de l'approche à adopter, vous pouvez utiliser les deux en même temps. Les supports physiques sont des appareils que vous contrôlez tels que les disques USB externes ou les périphériques réseau Wi-Fi accessibles. L'avantage

Sauvegarde & Récupération

d'utiliser vos propres médias physiques est qu'ils vous permettent de sauvegarder et de récupérer de nombreuses quantités de données très rapidement. L'inconvénient d'une telle approche est que si vous êtes infecté par des logiciels malveillants, tels qu'un Ransomware, il est possible que l'infection se propage dans vos sauvegardes. De plus, si vous êtes victime d'une catastrophe, comme le feu ou le vol, cela peut entraîner la perte non seulement de votre ordinateur, mais aussi de vos sauvegardes. En tant que tel, si vous utilisez des périphériques externes pour les sauvegardes, vous devez stocker une copie de votre sauvegarde hors site dans un emplacement sécurisé. Assurez-vous que les sauvegardes que vous stockez hors site soient correctement étiquetées.



Les sauvegardes fiables et automatisées sont bien souvent votre dernière ligne de défense pour protéger vos données.

Les solutions basées sur le Cloud sont des services en ligne qui stockent vos fichiers sur Internet. En règle générale, vous installez une application sur votre ordinateur. L'application sauvegarde automatiquement vos fichiers sur un calendrier ou lorsque vous les modifiez. L'avantage des solutions basées sur le Cloud est leur simplicité, les sauvegardes sont souvent automatiques et vous pouvez généralement accéder à vos fichiers depuis n'importe où. En outre, comme vos données résident sur le Cloud, les catastrophes domestiques telles que le feu ou le vol n'auront pas d'incidence sur votre sauvegarde. Enfin, les sauvegardes sur le Cloud peuvent vous aider à vous prémunir des infections malveillantes telles que les Ransomware, car de nombreuses solutions Cloud vous permettent de récupérer des versions pré-infectées. L'inconvénient majeur est que les sauvegardes sur le Cloud peuvent être plus lentes, surtout si vous avez une grande quantité de données. En outre, la confidentialité et la sécurité sont importantes. Par conséquent, posez-vous la question suivante : le service de sauvegarde fournit-il de solides contrôles de sécurité tels que le cryptage de vos données et la vérification en deux étapes ?

Enfin, n'oubliez pas vos appareils mobiles. L'avantage avec les appareils mobiles est que la plupart de vos données sont déjà stockées sur 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 sur le Cloud, telles que vos configurations d'applications mobiles, vos photos récentes et vos préférences systèmes. 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 de pouvoir les récupérer.

Sauvegarde & Récupération

Vérifiez périodiquement que vos sauvegardes fonctionnent en récupérant un fichier et en vous assurant qu'il soit identique à l'original. Assurez-vous également d'effectuer 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.

Points clés

Quelle que soit la solution utilisée pour sauvegarder vos données, assurez-vous d'automatiser vos sauvegardes et de les vérifier périodiquement.

- Lors de la reconstruction d'un système à partir d'une sauvegarde, assurez-vous de réappliquer les dernières mises à jour et mises à jour de sécurité avant de l'utiliser à nouveau.
- Les sauvegardes périmées ou obsolètes peuvent devenir un handicap, détruisez-les pour empêcher l'accès à des personnes non autorisées.
- Si vous utilisez une solution sur le Cloud, recherchez les politiques et la réputation du fournisseur et assurez-vous qu'elle réponde à vos besoins. Posez-vous les questions suivantes : chiffre-elle vos données ? Est-ce qu'elle supporte une authentification forte comme la vérification en deux étapes ?

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.answer.ch et http://answersecurity.com/

Sources

Phrases de passe :	https://securingthehuman.sans.org/ouch/2017#april2017
La vérification en deux étapes :	https://securingthehuman.sans.org/ouch/2015#september2015
La sécurité sur le Cloud :	https://securingthehuman.sans.org/ouch/2016#november2016
Chiffrement :	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware :	https://securingthehuman.sans.org/ouch/2016#august2016

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduit par : Marilyn Combet

