OUCH! | Septembre 2014

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

OUCH!

Dans ce numéro...

Utilisation du Cloud en toute sécurité

Vue d'ensemble

"Le Cloud" est une technologie puissante que les personnes et les organisations adoptent toutes rapidement. "Cloud" peut signifier différentes choses pour différentes personnes, mais signifie généralement l'utilisation d'un fournisseur de services sur Internet pour stocker et gérer vos données en ligne. L'un des avantages du Cloud n'est pas seulement de pouvoir accéder facilement et de synchroniser vos données depuis vos appareils partout dans le monde, mais également de pouvoir partager vos informations avec qui vous voulez. La raison pour laquelle nous appelons ces services "Le Cloud" est que vous ne savez pas toujours où vos données sont stockées physiquement. Le Cloud computing comprend par exemple la création de documents sur Google Docs, le partage de fichiers via Dropbox, la mise en place de votre propre serveur sur Amazon Cloud, ou encore le stockage de votre musique ou des photos sur iCloud d'Apple. Ces services en ligne peuvent vous rendre potentiellement beaucoup plus productif, mais ils comprennent aussi des risques particuliers. Dans ce numéro, nous couvrirons la façon dont vous pouvez profiter du Cloud en toute sécurité.

Editeur invité

James et Kelli Tarala (**@isaudit** / **@kellitarala**) sont les principaux consultants de Enclave Security et ont rédigé de nombreux cours de formation au SANS, y compris le SANS Audit 566: exécution et audition des vingt contrôles critiques de sécurité et MGT 415: Introduction pratique aux évaluations des risques.

Sélection d'un fournisseur de Cloud

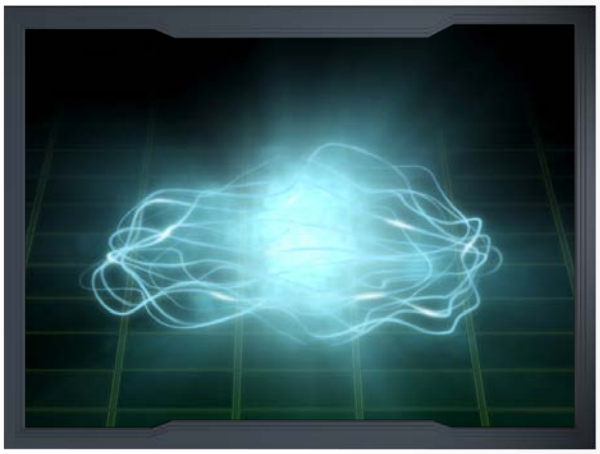
Le Cloud n'est ni bon ni mauvais, c'est un outil conçu pour faire avancer les choses, à la fois au travail et à la maison. Toutefois, lorsque vous utilisez ces services, vous confiez vos données privées à des étrangers et vous vous attendez à ce que ces derniers les gardent à la fois sécurisées et disponibles. En tant que tel, vous voulez être sûr de choisir un service le plus judicieusement possible. En ce qui concerne les ordinateurs au bureau ou les informations ayant trait à votre activité professionnelle, vous devez consulter votre responsable pour savoir si vous pouvez utiliser des services dans le Cloud. Si vous êtes autorisé à utiliser le Cloud, s'il vous plaît, n'oubliez pas de demander quels services Cloud vous êtes autorisé à utiliser et comment vous pouvez vous en servir. Si vous envisagez un service Cloud pour votre usage personnel, il est important de tenir compte des points suivants.

1. **Support**: Est-il facile d'obtenir facilement de l'aide ou une réponse à une question que vous vous posez ? Y'a-t-il un numéro de téléphone auquel vous pouvez appeler ou une adresse e-mail à laquelle vous pouvez écrire? Y a-t-il d'autres possibilités de support, tels que des forums publics ou Foires aux questions sur le site web du fournisseur de service?
2. **Simplicité**: Le service est-il facile à utiliser? Plus le service est complexe, plus il devient facile de commettre des erreurs

Utilisation du Cloud en toute sécurité

ou de perdre des données. Utilisez un fournisseur de Cloud que vous trouvez facile à comprendre, à configurer et à utiliser.

3. **Sécurité**: Comment obtenir vos données à partir de votre ordinateur vers le Cloud, la connexion est-elle chiffrée? Comment vos données sont-elles stockées dans le Cloud, sont-elles chiffrées et si oui, qui peut les déchiffrer?
4. **Conditions d'utilisation**: Prenez un moment pour revoir les Conditions de Service (elles sont souvent étonnamment faciles à lire). Confirmez qui peut accéder à vos données et quels sont vos droits légaux.



Le Cloud peut rendre vos informations plus accessibles et aider à vous rendre plus productif, mais faites attention à la manière dont vous stockez et partagez vos informations.

Sécurisation de vos données

Une fois que vous avez sélectionné un service Cloud, la prochaine étape est de vous assurer que vous utilisez vos services Cloud correctement. La façon dont vous accédez et partagez vos données peut souvent avoir un impact beaucoup plus important sur la sécurité de vos fichiers que vous ne l'imaginez. Ci-dessous, certaines étapes clés que vous devriez prendre en considération :

1. **Authentification**: Utilisez un mot de passe fort et unique pour vous authentifier sur votre compte Cloud. Si votre fournisseur de Cloud offre la double authentification, nous vous recommandons fortement de l'activer.
2. **Partage de fichiers / dossiers**: Le Cloud permet de partager vos fichiers et dossiers très simplement, parfois même trop. Dans le pire des cas, vous pouvez rendre accidentellement public vos fichiers ou même des dossiers entiers à l'ensemble du monde. La meilleure façon de vous protéger est par défaut de ne pas partager un de vos fichiers avec n'importe qui. Ainsi, ne donnez l'accès à des fichiers ou des dossiers spécifiques qu'à des personnes en particulier (ou groupes de personnes) et au cas par cas. Quand quelqu'un n'a plus besoin d'accéder à vos fichiers, supprimez ses autorisations. Votre fournisseur de Cloud doit vous fournir un moyen facile de savoir qui a accès à vos fichiers et dossiers.
3. **Partage de fichiers / dossiers à l'aide de liens**: Un trait commun de certains services de Cloud est la capacité de créer un lien Web qui pointe vers vos fichiers ou dossiers. Cette fonction vous permet de partager des fichiers avec qui vous voulez en fournissant simplement un lien Web. Toutefois, cette approche est très peu sécuritaire, toute personne qui connaît ce lien peut avoir accès à vos fichiers ou dossiers personnels. Si vous envoyez le lien à une seule personne, cette personne pourrait partager ce lien avec d'autres ou il pourrait apparaître sur les moteurs de recherche. Si vous partagez des données en utilisant un lien, assurez-vous de désactiver le lien une fois qu'il n'est plus nécessaire ou, si possible, protégez-le avec un mot de passe.

Utilisation du Cloud en toute sécurité

4. **Réglages**: Il est important de comprendre les paramètres de sécurité offerts par votre fournisseur de Cloud. Par exemple, si vous partagez un dossier avec d'autres personnes, peuvent-elles à leur tour partager vos données avec d'autres à votre insu?
5. **Antivirus**: Assurez-vous que le logiciel antivirus est bien à jour sur l'ensemble des machines utilisées pour accéder à vos fichiers. Si un fichier que vous partagez est infecté, les autres ordinateurs accédant à ce même fichier peuvent l'être aussi.
6. **Sauvegarde**: Même si votre fournisseur de Cloud est sensé sauvegarder vos données, pensez à faire vos propres sauvegardes régulièrement. Non seulement cela permet de protéger vos données si jamais votre fournisseur de Cloud venait à fermer, ou s'il devenait inaccessible pour quelque raison que ce soit. Il peut être beaucoup plus facile de récupérer de grandes quantités de données à partir de votre sauvegarde locale plutôt que de devoir tout télécharger depuis le Cloud. Vérifiez également à quelle fréquence votre fournisseur Cloud sauvegarde vos fichiers, s'il vous permet d'en récupérer des versions antérieures, et combien de temps il laissera vos sauvegardes disponibles.

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/

Ressources

Mots de passe forts:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_fr.pdf
Gestionnaires de mots de passe:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_fr.pdf
Sauvegardes:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_fr.pdf
Termes de sécurité:	http://www.securingthehuman.org/resources/security-terms

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