OUCH! | Novembre 2016

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

OUCH!

Dans ce numéro...

- Aperçu
- Choisir un fournisseur
- Protéger vos données

Sécurisez votre utilisation du Cloud

Aperçu

“Le Cloud” est vu de plusieurs manières différentes en fonction des personnes, souvent il est perçu comme un outil sur internet permettant de sauvegarder et manager des systèmes d’information à votre place. Un des avantages du cloud, c’est qu’il est facilement accessible depuis plusieurs types de « device » partout dans le monde et chacun de ces « device » peuvent être synchronisés. Vous pouvez également partager des informations avec qui vous voulez très simplement. On appelle ces services du « Cloud » car vous ne savez pas où sont stockées physiquement les données. Voici quelques exemples de services cloud : la création de documents sur google docs, le partage de fichiers via dropbox, la création de votre serveur sur AWS (Cloud amazon), sauvegarder des données clients sur Salesforce ou encore archiver vos musiques sur l’iCloud d’Apple. Tous ces services en ligne vous font gagner du temps et améliorent votre productivité, néanmoins ils ne sont pas sans risques. Dans cette newsletter nous allons voir comment optimiser la sécurité de tous ces services Cloud.

Editeur invité

Dave Shackleford (**@daveshackleford**) est un consultant possédant la société Voodoo Security, il est l’auteur de plusieurs cours SANS. Il a entre autre rédigé les cours suivants : Virtualization and Private Cloud Security and Security 524: Cloud Security Fundamentals.

Choisir un fournisseur

Le Cloud n’est pas bon ou mauvais, c’est un outil pour travailler et optimiser les taches, que ce soit au bureau où à la maison. Lorsque vous utilisez ces services, vous confiez des informations privées et confidentielles à un tiers, vous êtes en droit d’attendre qu’elles soient toujours sécurisées et disponibles. C’est pourquoi vous devez choisir votre fournisseur avec précaution. Pour le domaine professionnel votre première vérification doit être de valider que l’utilisation du Cloud est autorisée par votre politique de sécurité intérieur. Si vous êtes autorisés à utiliser le cloud vous devez vérifier le périmètre sur lequel vous pouvez l’utiliser ainsi que les règles d’utilisations associées. Si vous envisagez le cloud pour votre usage personnel, prenez en compte les considérations suivantes :

1. **Support** : Est-ce facile de joindre le support et d’avoir votre réponse ? Y-a-t-il une adresse email à laquelle vous pouvez écrire, des forums de discussions pour poser vos questions, ou encore des FAQ complètes sur leur site ?

Sécurisez votre utilisation du Cloud

2. **Simplicité** : Leur service est-il simple d'utilisation ? Plus le service est compliqué, plus vous pourrez facilement faire une erreur qui pourrait exposer ou effacer accidentellement vos données. Choisissez un fournisseur que vous trouvez facile d'utilisation et que vous comprenez facilement.
3. **Sécurité** : Vos données personnelles sont-elles collectées ? Et si oui lesquelles ? Comment allez-vous télécharger vos données depuis le cloud, comment sont-elles stockées ? Les données sont-elles chiffrées et si elles le sont qui peut les déchiffrer ?
4. **Les conditions d'utilisations** : Prenez un moment pour revoir les conditions d'utilisations (vous serez surpris, elles sont souvent simples à lire). Prenez conscience de vos droits et de qui peut lire vos données. Vous devez également contrôler les responsabilités de chacun en cas d'incident de sécurité.

Le cloud rend vos données plus accessible et vous aide à améliorer votre productivité. Mais il faut faire attention à la manière dont vous accéder aux informations et comment vous les partager.

Protéger vos données

Une fois que vous avez choisi votre fournisseur l'étape suivante est de garantir que votre utilisation du cloud est correcte. La façon dont vous allez accéder à vos données aura souvent un impact fort sur la sécurité de vos fichiers. Voici quelques éléments clés que vous pouvez prendre en compte :

1. **L'authentification** : Utilisez un mot de passe ou une passphrase forte pour vous connecter à votre compte. Si votre fournisseur permet l'utilisation de la double authentification, nous recommandons fortement que vous l'utilisiez. C'est le point le plus important pour protéger vos données.
2. **Le partage de fichier/dossiers** : Le Cloud facilite grandement le partage… Parfois même un peu trop… Dans les cas les plus critiques vous pouvez rendre public tous vos documents sur internet alors que vous pensiez ne les partager qu'avec une personne bien précise. La meilleure façon de s'en prémunir est de ne jamais partager vos fichiers de façon systématique avec une personne. Vous devez partager les fichiers de façon pertinente et temporaire uniquement avec les personnes autorisées. Si une personne n'a plus besoin d'accéder à certaines informations, il faut supprimer les autorisations. Votre fournisseur doit vous donner un moyen facile de contrôler les droits d'accès.
3. **Le partage via des liens** : L'une des particularités communes à tous les fournisseurs est le partage de fichiers ou dossiers via des liens internet. Vous pouvez partager ce que vous voulez en ne fournissant qu'un lien aux personnes

Sécurisez votre utilisation du Cloud

avec qui vous souhaitez partager un dossier ou fichier. Il faut cependant être prudent car ce système est, de base, peu sécurisé. Toute personne connaissant le lien peut accéder aux données concernées. Quand bien même vous ne partagez le lien qu'avec une personne, celle-ci peut ensuite le diffuser à ses contacts ou alors le lien peut apparaitre dans les moteurs de recherche. Vous perdez alors rapidement le contrôle de votre donnée. Lorsque vous utilisez ce type de lien, assurez-vous de définir un mot de passe pour protéger l'accès et définissez une durée de vie du lien.

4. **Configuration** : Vous devez comprendre les options de sécurité proposées par votre fournisseur. Par exemple si vous partagez un dossier avec une personne, cette personne peut-elle le partager à son tour sans que vous en ayez conscience ? Vous devez également vérifier que vous pouvez voir qui a accédé à votre fichier partagé. Lors d'un partage vous devez également pouvoir choisir si les destinataires ont les droits de lecture uniquement ou alors de lecture/écriture ? Ce qui signifierait que les fichiers peuvent être modifiés par une autre personne que vous.
5. **Antivirus** : Assurez-vous que votre antivirus est activé et à jour sur les différents ordinateurs que vous utilisez pour partager vos données. En effet si un fichier que vous partagez est corrompu, tous les ordinateurs accédant à ce fichier peuvent être par la suite corrompus également.

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

Phishing :	https://securingthehuman.sans.org/ouch/2015#december2015
Gestionnaire de mots de passe :	https://securingthehuman.sans.org/ouch/2015#october2015
La double authentification :	https://securingthehuman.sans.org/ouch/2015#september2015
Phrases de passe :	https://securingthehuman.sans.org/ouch/2015#april2015
Les sauvegardes :	https://securingthehuman.sans.org/ouch/2015#august2015

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduit par : Marilyn Combet