OUCH! Août 2021

OUCH!

SANS SECURITY AWARENESS

Votre publication mensuelle de conscientisation à propos de la Sécurité

Utiliser le Cloud en toute sécurité

Aperçu

Vous avez peut-être entendu parler d'un concept appelé « le cloud ». Cela signifie utiliser un fournisseur de services sur Internet pour stocker et gérer vos données. Les exemples incluent la création de documents sur Google Docs, l'accès aux courriels dans Microsoft O365, le partage de fichiers via Dropbox ou le stockage de vos photos sur l'iCloud d'Apple. Alors que vous accédez et synchronisez vos données à partir de plusieurs appareils partout dans le monde et partagez vos informations avec qui vous voulez, vous ne savez souvent pas et ne pouvez pas contrôler où vos données sont physiquement stockées.

Sélection d'un fournisseur Cloud

Les services Cloud ne sont ni bons ni mauvais. Ce sont des outils pour faire avancer les choses. Cependant, lorsque vous utilisez ces services, vous transmettez essentiellement vos données privées à des étrangers, en espérant qu'ils les gardent à la fois sécurisées et disponibles. En tant que tel, vous voulez être sûr de choisir judicieusement votre fournisseur de services. Pour les informations liées au travail, vérifiez auprès de votre superviseur si vous êtes autorisé à utiliser les services Cloud et lesquels sont autorisés. Si vous envisagez d'utiliser les services Cloud à des fins personnelles, tenez compte des éléments suivants:

1. **Confiance:** Pouvez-vous faire confiance au fournisseur de Cloud? Est-ce une entreprise publique bien connue que des millions de personnes utilisent déjà, ou s'agit-il d'une petite entreprise inconnue basée dans un pays dont vous n'avez jamais entendu parler?
2. **Support**: Est-il facile d'obtenir de l'aide ou d'avoir une réponse à une question? Y a-t-il un numéro de téléphone que vous pouvez appeler ou une adresse e-mail que vous pouvez contacter? Existe-t-il d'autres options d'assistance, telles que des forums publics ou une foire aux questions sur leur site Web?
3. **Simplicité**: Est-il facile d'utiliser le service? Plus le service est complexe, plus vous risquez de faire des erreurs et d'exposer ou de perdre accidentellement vos informations. Utilisez un fournisseur Cloud que vous trouvez facile à comprendre, à configurer et à utiliser.
4. **Sécurité**: Comment vos données seront-elles acheminées de votre ordinateur vers le service Cloud? La connexion est-elle sécurisée par cryptage? Comment vos données sont-elles stockées? Est-ce crypté, et si oui, qui peut décrypter vos données? Lorsque vous migrez vos données, n'oubliez pas que la sécurité est une responsabilité partagée entre vous et le fournisseur.

5. **Compatibilité:** Le fournisseur de services prend-il en charge tous les appareils et systèmes d'exploitation que vous utilisez ou prévoyez d'utiliser?
6. **Conditions d'utilisation**: Prenez un moment pour consulter les Conditions d'utilisation (elles sont souvent étonnamment faciles à lire). En vertu des lois de quel pays le fournisseur de services opère-t-il? Portez une attention particulière aux droits que vous cédez à votre prestataire.

Sécurisation de vos données

L'étape suivante consiste à vous assurer que vous utilisez correctement vos services Cloud. La façon dont vous accédez et partagez vos données peut souvent avoir un impact bien plus important sur la sécurité de vos données que toute autre chose. Voici quelques étapes clés que vous pouvez suivre:

1. **Authentification**: Utilisez un mot de passe fort et unique pour protéger votre compte Cloud. Si votre fournisseur Cloud propose une vérification en deux étapes, nous vous recommandons fortement de l'activer.
2. **Partage de fichiers/dossiers**: Les fournisseurs cloud rendent très simple le partage de données - parfois trop simple. Il peut être très facile de partager accidentellement vos informations publiquement. Protégez-vous en n'autorisant que des personnes spécifiques (ou des groupes de personnes) à accéder à des fichiers ou des dossiers spécifiques. Lorsque quelqu'un n'a plus besoin d'y accéder, supprimez-le. Votre fournisseur Cloud devrait fournir un moyen simple de savoir qui a accès à vos fichiers et dossiers.
3. **Paramètres**: Comprenez les paramètres de sécurité proposés par votre fournisseur de Cloud. Par exemple, si vous partagez des images, des fichiers ou un dossier avec quelqu'un d'autre, peut-il partager vos données avec d'autres à votre insu?
4. **Renouveler**: N'oubliez pas de renouveler votre abonnement ou vous pourriez perdre l'accès à vos données.

Rédacteur invité

Tameika Reed (@womeninlinux), fondatrice de Women in Linux. Elle dirige des initiatives axées sur l'exploration de carrières dans les infrastructures, la cybersécurité, les DevSecOps et le leadership. Elle organise une rencontre hebdomadaire sur des sujets allant de l'infrastructure à la blockchain. Elle a parlé à OSCon, LISA, Seagl et HashiConf EU.

Ressources

Attaques d'ingénierie sociale: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Simplifier les mots de passe: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Gestionnaire de mots de passe: https://www.sans.org/newsletters/ouch/password-managers/
La puissance des mises à jour: https://www.sans.org/newsletters/ouch/the-power-of-updating/

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka