5 conférences à suivre au Cloud Computing World Expo

Quelque 5 000 visiteurs sont attendus les 1er et 2 avril prochains au CNIT Paris La Défense pour une nouvelle édition du Cloud Computing World Expo.

Cette année et pour la première fois, on trouvera un espace dédié à la sécurité pour favoriser les rencontres et les échanges.

Parmi le vaste programme de conférences proposées, nous vous recommandons tout particulièrement les 5 sessions suivantes :

- **« Shadow IT » : la détecter, l'évaluer, la surveiller, l'éradiquer (…ou pas !)**
- **Que garantissent vraiment les Clouds souverains à leurs clients (confidentialité, sécurité, sûreté, indépendance technologique, performances) ?**
- **Labels « Secure Cloud », Cloud Confidence, référentiel Anssi… : que sont ces initiatives françaises et quels objectifs poursuivent-elles réellement ?**
- **Zoom sur la réversibilité : engagement du prestataire, faisabilité, maintenabilité, tests, réalisation, vérifications…**
- **Juridique : Les 5 articles-clés à exiger (et à négocier) sur le contrat vous liant au prestataire Cloud**

Autres ressources :

- Le site du Cloud Computing World Expo

Nos empreintes digitales dans iCloud ?

Si l'on en croit Rob Price, journaliste à Business Insider, Apple envisagerait de stocker les empreintes digitales de ses clients dans le Cloud afin de pouvoir les synchroniser sur d'autres dispositifs.
L'objectif décrit dans le brevet déposé par Apple étant de faciliter les transactions financières avec les équipements Apple. Ce brevet est extrêmement surprenant car on se souvient que lors de la sortie de l'iPhone 5S (1er modèle avec

le lecteur d'empreinte Touch ID), de nombreux utilisateurs et journalistes s'étaient inquiétés de la sécurité des données biométriques.

Apple avait tout de suite réagit en déclarant que toutes les précautions avaient été prises pour sécuriser les données biométriques du Touch ID. Ainsi, selon Apple, ces données sont chiffrées puis stockées dans un container sécurisé au cœur de la puce A7. D'autre part, Apple avait affirmé qu'elles n'étaient jamais stockées sur les serveurs Apple ni même sauvegardées dans iCloud. Le brevet déposé par Apple à l'OMPI va donc à l'encontre de ces déclarations. Apple doit certainement penser qu'une fois le Touch ID adopté, les utilisateurs ne pourront plus vraiment faire marche arrière même si l'usage des données biométriques n'est plus celui initialement annoncé. Et quand on connait les nombreuses vulnérabilités du système iOS (en particulier toutes celles concernant le chiffrement et le container Keychain) et les pratiques de la NSA (que nul ne peut désormais contester depuis les révélations de Snowden), on est en en droit d'avoir les plus grandes inquiétudes pour la sécurité de nos données biométriques.

Alors après nos numéros de cartes bancaires, nos mots de passe, voici donc prochainement nos empreintes digitales dans le Cloud d'Apple. Il serait intéressant que la CNIL et l'Europe se prononcent rapidement sur ce projet afin d'éviter que la plus grosse capitalisation boursière du monde ne nous l'impose très rapidement.

Autre ressource :

- Apple Is Considering Storing Your Fingerprints In iCloud

L’App Outook interdite au Parlement Européen

Quelques jours seulement après le lancement par Microsoft de la nouvelle App Outlook pour iOS et Android, la DG ITEC (DSI du Parlement européen) vient d’en interdire l’usage à tous les membres du Parlement européen. Motif invoqué : L’application pose d’importants problèmes de sécurité. Ainsi, la DG ITEC a adressé en interne à l’ensemble des utilisateurs le message suivant : « *Vous êtes priés de ne pas installer ces applications, et au cas où vous les auriez déjà installée pour accéder à votre messagerie professionnelle, nous vous demandons de es désinstaller immédiatement et de changer votre mot de passe […] les applications envoient sans permission des informations de mot de passe à Microsoft et stockent les courriels dans un service cloud de tierce partie sur lequel le Parlement n’a aucun contrôle.*» Microsoft a officiellement réagit ce matin (15 février) en annonçant travailler avec les administrateurs du Parlement européen afin de fournir la documentation nécessaire pour éviter les comportements dangereux de l’application. Microsoft a également reconnu travailler sur l’amélioration de la sécurité de l’application et s’est engagé à une mise à jour dans les prochains mois.
On ne peut que se réjouir de la vigilance de la DSI du Parlement Européen sur cette affaire mais s’interroger quand même sur la réactivité de nos institutions sur d’autres incidents de sécurité. Puisque nous parlons d’Outlook sous iOS, pourquoi par exemple une vulnérabilité critique découverte dans iOS le 8 janvier 2014 et corrigée par Apple le 21 février 2014 n’a-t-elle fait l’objet d’aucun message d’alerte de la part de l’ENISA ou de l’ANSSI ? Certes le bulletin Bulletin d’actualité (CERTFR-2014-ACT-009) de l’ANSSI l’indique effectivement le 28 février 2014 mais le risque réel se situait entre le 8 janvier (première exploitation effective de la faille) et le 21 février (disponibilité du correctif fourni Apple). Et dans cet exemple, ce n’est pas uniquement les mots de passe de messagerie qui pouvaient être compromis par une attaque MITM totalement transparente mais l’ensemble des flux chiffrés entre le terminal (iPhone ou iPad) et le Cloud (mots de passe de toutes les applications, numéros de cartes bancaires, etc…).

Autres ressources :

- Le Parlement européen bannit les apps Outlook pour iOS et Android
- La nouvelle application Outlook interdite au Parlement européen
- Microsoft Working with European Parliament to Unban Outlook Android/iOS App

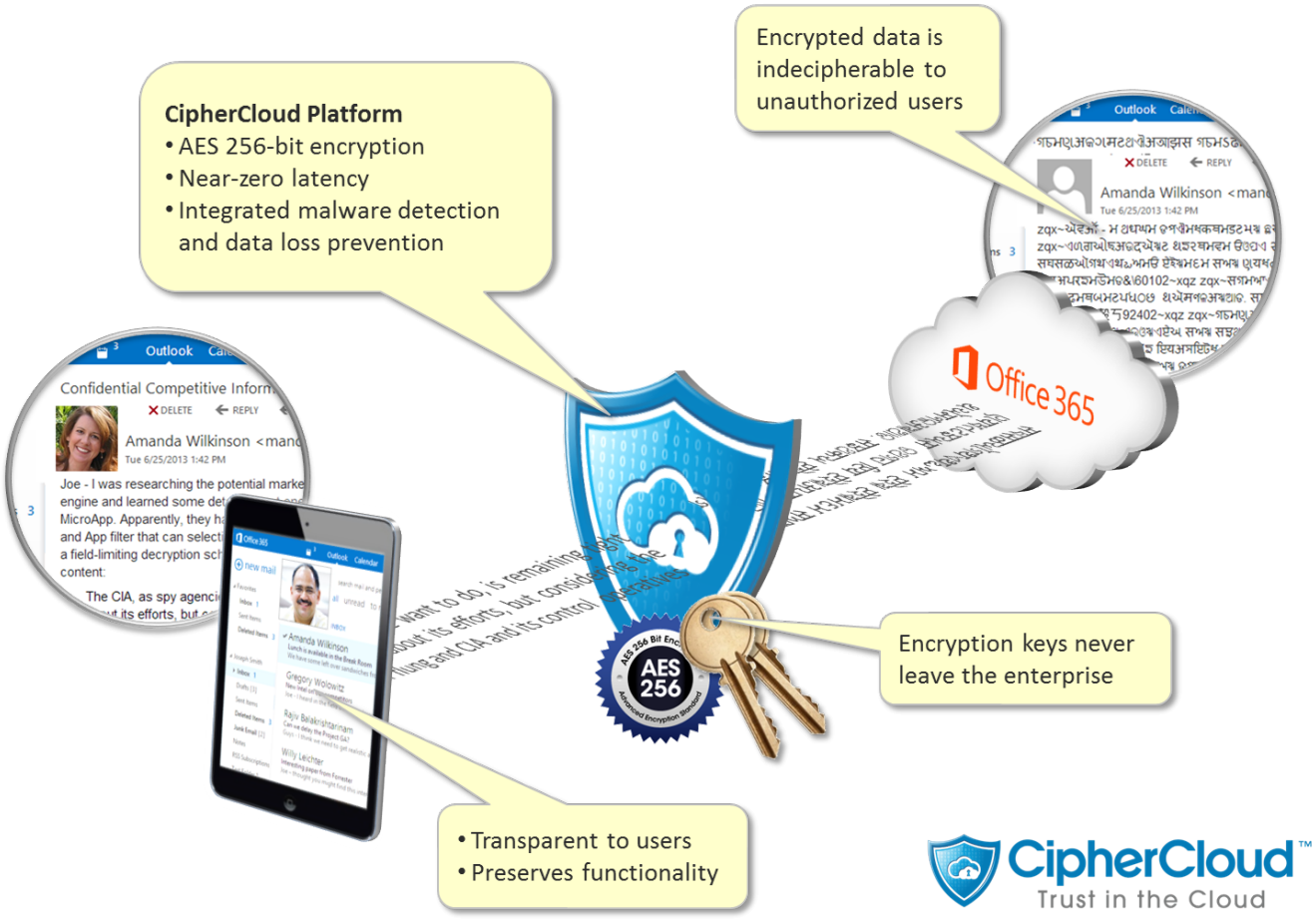
---

Ciphercloud s’installe en France

Par communiqué de presse en date du 5 février 2015, Ciphercloud annonce l’ouverture de ses bureaux parisiens dans le cadre d’une expansion rapide sur le marché français. Ces nouveaux bureaux couvriront les ventes, les services et l’assistance clientèle.

Mais connaissez-vous Ciphercloud ?
Ciphercloud est une société américaine qui propose d’assurer la sécurité des données dans un cloud public en toute indépendance du fournisseur. Le principe repose un proxy de chiffrement qui sécurise les données sur les flux vers le cloud. Les clés de chiffrement utilisées ne sont jamais accessibles par le fournisseur du service. Les solutions de Ciphercloud permettent par exemple de sécuriser une base de données dans AWS, des emails dans Office365 ou dans Gmail, des données clients chez Saleforce ou bien encore des fichiers dans Box.

Schéma de principe avec Office 365 :



Nous publierons prochainement sur SecuriteCloud.com une présentation détaillée des solutions de Ciphercloud avec les avantages bien sûr mais aussi les limites de ce type de solution. Dans le cadre de ce dossier, nous sommes à la recherche de retours clients. Si vous avez mis en œuvre (ou simplement testé) Ciphercloud dans votre entreprise et si vous souhaitez nous faire part de votre expérience, merci de nous contacter.

Autres ressources :

- CipherCloud étend son activité à la France