Panoptinet

Gardez un oeil sur votre réseau

Dropbox : vos documents ne sont pas confidentiels

admin · Thursday, June 23rd, 2011

Les utilisateurs du service Dropbox pensaient que les documents qu'ils sauvegardaient en ligne étaient parfaitement sécurisés, grâce à un cryptage AES 256 bits. En théorie seulement, car dans les faits, l'entreprise garde une copie de la clé de chiffrement, et l'utilise ! Pourquoi une telle pratique ? Et comment utiliser des services de stockage en ligne en toute sécurité ?

Cette révélation concerne Dropbox, mais s'applique probablement à tous les services en ligne similaires : stockage (sauvegarde), partage maitrisé et synchronisation de documents numériques.

Officiellement, tout document envoyé sur son compte Dropbox est **crypté en AES 256 bits**. Il s'agit d'un chiffrement assez résistant, et réellement appliqué sur Dropbox. Mais un cryptage n'est efficace que si on est le seul à posséder la clé (mot de passe) ! Or les employés de la société Dropbox, Inc. ont accès à une **copie de la clé**, pour une simple et raison : pour éviter tout encombrement inutile des serveurs, l'entreprise vérifie que tout nouveau document n'est **pas déjà hébergé** par un autre utilisateur. Auquel cas une seule copie du document est réellement stockée (au lieu de 2), et des raccourcis sont créés pour que chaque titulaire du document y ait accès. Ce type d'opération serait impossible sans une copie de la clé de chiffrement.

Depuis cette révélation, le site annonce plus clairement que **les employés peuvent accéder aux données**, mais de manière régulée : accès restreints aux seules métadonnées (informations sur le document et non le document lui-même), consultables par une "petite" équipe seulement, et de manière exceptionnelle.

Le problème tient surtout dans le fait qu'il existe une copie de chaque clé de cryptage, et que les utilisateurs n'ont pas la main sur cette seconde clé. Imaginons un instant qu'un **piratage** (très à la mode ces temps-ci), qu'un **bug** ou qu'un **salarié mal intentionné** affecte une ou plusieurs copies de ces clés !
C'est justement ce qu'il s'est passé dernièrement : un bug est survenu lors d'une mise à jour du service, il était alors **possible de se connecter avec n'importe quel mot de passe** (à condition de connaître l'adresse mail d'un compte Dropbox). Pendant 4h, il était théoriquement possible de se connecter à **25 000 000 de comptes** ! Et par

conséquent à de très nombreux **documents personnels ou confidentiels**...

Le bug a été résolu 5 minutes après sa découverte, et l'entreprise a de suite communiqué sur son blog par souci de transparence. Si Dropbox, Inc. continue d'enquêter sur d'**éventuelles connexions frauduleuses**, il semblerait que moins de 1% d'utilisateurs se soit connecté lorsque le bug était actif, avant que toutes les sessions en cours ne soient volontairement interrompues.

Le stockage en ligne est pourtant une solution intéressante pour sauvegarder ses documents importants : les serveurs qui hébergent les données sont souvent bien **sécurisés**, et les données envoyées dessus sont enregistrées sur de serveurs "**miroirs**" pour pallier à tout éventuel dysfonctionnement. Cela en fait une solution beaucoup plus sûre que nos traditionnels disques durs (qui peuvent lâcher à tout moment) ou CD/DVD inscriptibles (qui s'usent en quelques années). Mais les services comparables à Dropbox connaissent aussi leurs points faibles. Voici ce qu'il est possible de faire pour les contourner :

- Soit mettre en place soit même un serveur de sauvegarde local ou distant, mais cela suppose des compétences techniques particulières. Et les risques (intrusion, incendie, etc.) demeurent.
- Soit utiliser un service comme Dropbox, mais en prenant le soin de **crypter tout document avant envoi** (avec un logiciel spécialisé ou directement avec le système d'exploitation s'il propose cette fonctionnalité). Cela peut être problématique si la synchronisation automatique est activée.

Nous utilisons aujourd'hui beaucoup de services en ligne, à qui nous donnons volontiers de **nombreuses informations personnelles**, en toute confiance, et sans se poser trop de questions. Mais bien identifier quelles informations sont transmises à quelle entité permet souvent de **limiter le partage de données**, et de prendre conscience des **risques** possibles.

Source : MacBidouille