Safe Harbor & Privacy Shield : Comment l’entreprise peut avoir le contrôle complet de son propre cloud ?

	Safe Harbor & Privacy Shield : Comment l’entreprise peut avoir le contrôle complet de son propre cloud ?

L'invalidation de l'accord Safe Harbor a provoqué une certaine incertitude chez de nombreuses entreprises qui ne savent plus comment sauvegarder leurs données en toute sécurité et légalité – tout en les mettant à la disposition de leurs collaborateurs.

Début février, l'accord Safe Harbor 2.0 – surnommé Privacy Shield – a vu le jour, mais de nombreux doutes sur sa légitimité subsistent.
Dans ce contexte, l'incertitude demeure au sein des entreprises qui se posent de nombreuses questions autour de la conformité et ne savent pas si le Privacy Shield sera une solution sur le long terme. Il est toutefois possible de contourner les problématiques liées à l'instabilité de telles réglementations en trouvant la bonne solution – ainsi qu'un fournisseur de services adapté.

Il existe deux alternatives pour sauvegarder et utiliser ses données en toute sécurité dans le cloud sans se soucier de problématiques de conformité.
D'une part, l'entreprise peut rechercher un fournisseur de cloud computing exploitant ses Data Centers dans un pays européen. D'autre part, les entreprises sont tout à fait capables de constituer leur propre cloud et d'y mettre leurs données, ressources informatiques et applications à la disposition de leurs collaborateurs. Le marché du stockage externe offre de nombreuses solutions pour ces deux approches. Le rôle, pour tous les grands acteurs sur le marché, étant d'offrir aux clients une sauvegarde et un partage parfaitement sûrs de leurs données dans le cloud.

Les utilisateurs du cloud doivent pouvoir faire entièrement confiance à leur fournisseur de services
Dès qu'une entreprise prend la décision d'utiliser une architecture cloud public pour stocker une partie de ses informations, elle doit trouver un fournisseur adapté à ses exigences mais également irréprochable en termes de fiabilité.
La priorité dans cette démarche, lorsque l'on souhaite éviter des soucis de conformité, est de s'assurer que le fournisseur mette à disposition ses centres de données en Europe. En outre, l'entreprise est parfaitement en droit de demander si la sauvegarde de données de son fournisseur est effectuée exclusivement dans ses propres centres de données ou s'il en fournit une copie à d'autres centres de données d'un pays tiers. L'évaluation des accords de niveau de service (SLA), de la méthode et de la chronologie de sauvegarde appliquée pour telles ou telles données mais aussi des conditions de leur récupération sont des points à examiner lors du choix du fournisseur.
Cela permet d'établir une solution de confiance entre l'utilisateur et son service cloud. C'est sur la base de cette confiance et de la garantie que leurs données ne quittent pas l'Europe que les utilisateurs peuvent opter pour différents services de cloud.
D'autre part, l'utilisateur doit impérativement veiller à ce que le fournisseur utilise un encodage afin d'écarter tout risque d'utilisation abusive (intentionnelle ou aléatoire) de ses données.

L'entreprise peut avoir le contrôle complet de son propre cloud
La deuxième option garantie une sauvegarde et un partage des données parfaitement sûrs dans une architecture cloud, et confère donc à l'entreprise le plein contrôle sur ses informations et services numériques. Légèrement plus complexe, cette option consiste à créer sa propre architecture cloud privée.
L'entreprise devra certes gérer davantage de ressources, mais elle pourra puiser pleinement dans les services mis à disposition, les droits d'accès, la sélection des applications et l'assistance technique. Ces avantages garantiront une meilleure flexibilité aux collaborateurs de l'entreprise, ainsi que des outils nécessaires pertinents pour faciliter leurs tâches et les mêmes droits d'utilisation que s'ils travaillaient dans un cloud public. La sécurité des données et des appareils sera également garantie conformément aux mesures internes prises par l'entreprise.
Un cloud privé n'est pas concerné par les effets de Privacy Shield et permet d'utiliser différents services basés sur le cloud computing. En effet, les applications telles que « Box » ou « Dropbox » ne devraient plus être utilisées dans un environnement influé par de telles réglementations.

La pratique BYOD est une tendance très actuelle dans le monde de l'entreprise, mais elle complique l'intégration des terminaux dans les procédures de sauvegarde et rend difficile un contrôle complet sur toutes les informations de l'entreprise. L'utilisation combinée d'un cloud privé et de solutions d'accès, de synchronisation et de partage des fichiers est susceptible de remédier à cela. Les collaborateurs pourront ainsi accéder en toute sécurité aux données depuis n'importe quel terminal, les synchroniser et les partager avec leurs collègues, clients, partenaires et fournisseurs.
Un tel logiciel peut remplacer le serveur FTP et permet, par exemple, le libre-service en créant différents comptes utilisateurs tout en déchargeant les tâches de l'administrateur. L'intégration de solutions MDM facilite la gestion des appareils portables et assure un contrôle souple des données et des comptes.
Via l'utilisation d'une bonne solution d'accès, de synchronisation et de partage, le responsable informatique peut mettre en place une meilleure gouvernance des données en établissant des droits d'accès mais peut aussi retracer le transfert ou le partage éventuels des données concernées.
Les entreprises désireuses d'utiliser un cloud parfaitement sûr et de conserver le plein contrôle de leurs ressources et données opteront donc pour un cloud privé et des applications adaptées aux besoins de leurs collaborateurs et personnel informatique.

La sécurité doit être la priorité absolue
La débâcle provoquée par l'invalidation du Safe Harbor a permis de tirer une leçon très importante. La sécurité et la confidentialité des données doivent être des priorités absolues, quelle que soit la solution choisie par une entreprise, qu'il s'agisse d'un cloud privé ou public. Les informations numériques doivent donc impérativement être encodées avant de quitter l'entreprise ou – mieux – le réseau protégé. Une procédure de sauvegarde, par exemple, offre déjà une certaine protection, mais pour toutes les entreprises désireuses d'empêcher définitivement tout accès illicite à leurs données personnelles ou d'entreprise, l'encodage est une priorité absolue. Seul un encodage efficace est apte à garantir la protection et la sécurité des données … [Lire la suite]

Réagissez à cet article

Source : *Safe Harbor & Privacy Shield : comment assurer la conformité ? – JDN*