La DSI : moteur et protecteur des données de l'entreprise

Un rapport récemment publié par l'éditeur de logiciels anti-virus McAfee, met en lumière un chiffre pour le moins inquiétant : les entreprises estiment utiliser environ 30 services cloud, quand elles en exploitent en réalité près de 1 935. Une différence de perception significative qui repose en partie sur des besoin d'agilité accrus et par conséquent de la montée en puissance du shadow IT. Un terme fréquemment utilisé pour désigner des systèmes d'information mis en oeuvre au sein des entreprises sans approbation de la DSI. À l'heure où les services cloud sont plus accessibles que jamais, les différentes divisions des entreprises n'hésitent pas à prendre la mains sur l'IT pour obtenir les ressources dont ils ont besoin, en lieu et place de suivre les procédures d'achat internes établies.

Le shadow IT n'est pas toujours néfaste : il peut parfois permettre à tous les utilisateurs de pouvoir faire preuve d'agilité. Mais sans supervision, il peut vite devenir difficile pour les entreprises de savoir exactement où se trouvent leurs données et leurs applications, sans parler des risques liés à la protection des données sensibles.

L'IaaS mal configuré, un nouveau danger pour les entreprises

Ce même rapport montre également que 21% des fichiers stockés dans le cloud contiennent des données sensibles, soit une augmentation de 17 % au cours des deux dernières années. Il s'agit d'une pratique tout à fait acceptable si les entreprises s'équipent des solutions de stockage et de sécurité adéquates. Malheureusement, les enseignements du rapport révèlent que les entreprises utilisent en moyenne 14 instances IaaS mal configurées qui peuvent compromettre à tout moment la sécurité des données sensibles. Un nombre considérable d'incidents potentiels, eu égard aux 65% d'entreprises dans le monde favorisant l'IaaS. De plus, 5,5% des compartiments AWS S3 actifs ne sont, eux aussi pas configurés correctement : ainsi, toute personne disposant du lien peut accéder aux contenus du compartiment depuis un réseau public. Ce chiffre qui peut sembler bas, mais il montre que près d'un compartiment S3 sur 20 n'est pas sécurisé.

Le cloud public, une menace pour la sécurité ?

Certains détracteurs du cloud annoncent pour bientôt la fin du cloud public, clamant qu'il n'a pas sa place dans le monde de l'entreprise, mais ce n'est pas tout à fait vrai. Tout comme une voiture, ou un couteau japonais, le cloud public peut entraîner des risques s'il est utilisé par des personnes qui ne disposent pas de la protection, de la formation ou de l'expertise nécessaires pour une utilisation optimisée.

Le cloud public a profondément transformé les entreprises, quelle que soit leur taille, en permettant par exemple aux startups de se lancer rapidement sans avoir à investir des sommes colossales dans leur infrastructure matérielle et logicielle. Il a également aidé les services internes des entreprises à réagir rapidement à l'évolution des demandes de leurs clients et du marché. Le cloud public a généré des millions de dollars de chiffre d'affaires pour les entreprises (et les gouvernements) de toutes tailles, partout dans le monde. Mais convient-il à tous les cas d'utilisation ?

Les services IT interne comme fournisseur de services

Dans ce monde en constante transformation, il est plus que jamais vital pour les entreprises de savoir exactement où sont stockées leurs données et comment les protéger afin de faire face aux exigences réglementaires de plus en plus strictes. Si certains collaborateurs ont parfois le sentiment que les services IT, achats et approvisionnement les empêchent de travailler correctement, elles sont pourtant essentielles au fonctionnement des entreprises.

Si la plupart des entreprises croient utiliser une trentaine de services cloud, alors qu'elles en exploitent près de 2000 dans la réalité, en confiant cette responsabilité aux équipes IT internes, les départements métier peuvent se concentrer sur leurs rôles respectifs, au lieu d'assurer eux-mêmes la gestion de leurs services informatiques.

La DSI doit soutenir l'entreprise, en proposant un système de cloud public autorisé, configuré et plus faciles à auditer, tout en déployant des services cloud privés réservés aux données critiques. À l'heure où les entreprises du monde entier découvrent et testent les stacks informatiques bimodales et multimodales, ces solutions multi-cloud peuvent s'imposer comme un choix judicieux. Cependant, elles doivent absolument être gérées de manière centralisée en interne.

En effet, le rôle de l'IT n'est pas de nuire à l'agilité des services métier ou de ralentir le processus d'achats, son objectif est simplement de stocker et protéger correctement les données pour permettre à l'entreprise de se développer en toute sécurité.