Cloud : les entreprises perdent-elles le contrôle des données ?

La publication étendue de données, des terminaux au cloud, offre des opportunités de croissance aux entreprises, mais elle n'est sans risque, rapporte McAfee, sondage à l'appui.

79% des 1000 professionnels et décideurs informatiques interrogés* dans 11 pays déclarent que leur entreprise stocke des données dans le cloud public. Selon le rapport, 26% des fichiers stockés dans le nuage contiennent des données sensibles. Or, dans 91% des cas, les données dormantes ne sont pas chiffrées par les fournisseurs de services cloud.

Par ailleurs, 41 services cloud par entreprise en moyenne sont « approuvés », comme Microsoft Office 365, par exemple, mais bien d'autres sont utilisés hors du contrôle de l'IT. « Il y a des milliers d'autres services cloud utilisés ponctuellement, certains pour une seule tâche et d'autres plus régulièrement, mais sous le radar et en attente d'être la prochaine application approuvée », ont souligné les auteurs du rapport publié par l'éditeur de logiciels de sécurité.

Ils ont aussi relevé que près de 8 organisations sur 10 autorisent l'accès aux services cloud approuvés (SaaS, PaaS, IaaS) depuis des terminaux personnels. Aussi, dans 1 cas sur 4, des données sensibles sont téléchargées du cloud vers un appareil non géré par l'entreprise. Celle-ci risque alors d'en perdre la trace… Or, 52% des organisations utilisent des services cloud qui ont déjà subi des exfiltrations de données. De surcroît, une entreprise sur cinq déclare manquer de visibilité sur les données qui se trouvent dans ses applications cloud.

Sécurité centrée sur la data

Autre enseignement du rapport : 49% des fichiers chargés sur un service cloud sont partagés au sein d'un même programme ou entre les services de différents fournisseurs. Or, 1 fichier sur 10 contenant des données sensibles partagées dans le cloud est en accès public.

Certes, 93% des RSSI jugent qu'il est de leur responsabilité de sécuriser les données dans le cloud. Mais 30% des organisations disent manquer de personnel qualifié pour protéger leurs applications accessibles en tant que service (SaaS).

Une minorité (41% tout de même) dit pouvoir contrôler les tentatives d'accès depuis des terminaux personnels aux données de l'entreprise dans le cloud. Ils sont moins nombreux (34%) à contrôler les paramètres de collaboration pour leurs services cloud.

Aussi, 37% des organisations utilisent une solution de prévention de pertes de données (DLP) pour protéger et superviser leurs applications dans le cloud. En moyenne, se sont 45 737 incidents qui sont identifiés chaque mois par ce biais.

Pour McAfee, la protection orientée réseau ne suffit donc plus pour sécuriser les usages cloud. Les entreprises auraient intérêt à intégrer un modèle de sécurité « data-centric » pour adapter leur niveau de protection à la dispersion des données dans le cloud.

*****_Les résultats ont été comparés aux données agrégées et anonymisées d'utilisation du cloud par 30 millions d'individus. Tous couverts par McAfee MVISION Cloud, la solution de courtage en sécurité d'accès cloud (CASB – Cloud Access Security Broker) du fournisseur américain. (source : « Enterprise Supernova: the data dispersion cloud adoption and risk report » McAfee – janvier 2020)._

(crédit photo © shutterstock)