Sécurité cloud : 5 éléments à retenir du rapport Netwrix

De nombreuses entreprises manquent encore de visibilité sur leurs données stockées dans le cloud. Un choix risqué. C'est l'un des enseignements d'un rapport* international sur la cybersécurité publié par Netwrix.

Des directeurs des systèmes d'information (DSI), des administrateurs systèmes, des consultants et des responsables de la sécurité IT de PME et de grandes entreprises ont été interrogés. Toutes ces organisations utilisent le cloud (public 39%, hybride 35%, privé 26%).

Voici 5 des éléments majeurs à retenir de ce rapport :

1. **IPI** > Une minorité stocke des données financières (26%) et des actifs de propriété intellectuelle (16%) dans le cloud. En revanche, 50% des répondants (60% en France) ont déclaré que leur entreprise stocke dans le cloud des données contenant des informations personnelles identifiables (IPI) de clients et d'employés.

Elles le font d'abord pour réduire leurs coûts (cité par 31% des répondants) et pour rendre accessibles ces informations à leurs travailleurs à distance (25%).

2. **Classification** > 75% des organisations (50% en France) qui stockent des IPI dans le cloud, mais qui n'ont pas identifié et classifié toutes ces informations avant de les migrer, ont subi au moins un incident de sécurité ces douze derniers mois.

« Un taux 3,5 fois plus élevé que celui atteint par les organisations qui ont fait le choix de la classification des données », a indiqué l'éditeur spécialisé de logiciels dans son rapport.

3. **Initiés ou tiers** > 36% des répondants (60% en France) ont reconnu ne pas avoir été en mesure de déterminer quels étaient les acteurs (initiés, partenaires, consultants externes…) à la source de ces incidents de sécurité cyber.

4. « **Cloud first** » > Il n'empêche, 21% des organisations ont adopté une stratégie tournée vers le « cloud d'abord ». 28% ont même l'intention de se tourner vers le « 100% cloud » dans les 5 ans à venir, voire 35% pour les entreprises de plus petite taille.

5. **Ou sortie ?** > D'autres déchantent. Aussi, 48% des organisations qui stockent toutes leurs données sensibles dans le cloud prévoient ou pourraient envisager de rapatrier des données sur site (on-premise). En cause : des problématiques de sécurité et de conformité (RGPD, NIS…) (24%) et des coûts jugés trop élevés (22%).

Budgets serrés

Les principales mesures que les répondants prennent ou envisagent de prendre pour renforcer la sécurité des données dans le nuage sont :

Le chiffrement de données (59%) et la surveillance de l'activité utilisateur autour de ces données (52%). Le renforcement des règles de sécurité (51%) et la formation des employés (43%) suivent.

Mais les ressources allouées ne sont pas toujours à la hauteur. Or, pour 55% du panel, les budgets consacrés à la sécurité cloud n'évoluent pas à la hausse en 2019.

(crédit photo © shutterstock)

* *Pour le « Netwrix Cloud Data Security Report 2019 » 749 managers IT et consultants en Amérique, en Europe, en Asie et en Australie ont été interrogés sur les données stockées dans le cloud public, hybride ou privé par leur organisation.*