Sécurité Cloud : quand les DSI peinent à suivre le rythme

La confiance des équipes IT dans le cloud public augmente. Toutefois, des erreurs de configuration et la confusion autour de la responsabilité partagée dans le cloud pèsent sur la sécurité des déploiements, selon le « Cloud Threat Report 2020 » d'Oracle et de KPMG.

75% des 750 professionnels IT interrogés* considèrent que le cloud public d'infrastructure est plus sécurisé que leurs propres datacenters. En revanche, 92% jugent que leur organisation n'est pas bien préparée pour sécuriser les services utilisés (SaaS, PaaS, IaaS).

Les erreurs de configuration les plus courantes concernent :

– des comptes à privilèges trop étendus (mentionnés par 37% des répondants)
– des ports ouverts de serveurs web (35%)
– un déficit d'authentification multifacteur pour accéder à des services clés (34%)
– une incohérence autour des listes de contrôle d'accès au stockage objet (33%)

À quel prix ? Les organisations qui ont découvert des services cloud mal configurés disent avoir subi au moins 10 incidents associés à une perte de données l'an dernier.

Responsabilité partagée dans le cloud

Amazon Web Services (AWS), Microsoft Azure (partenaire stratégique d'Oracle) et bien d'autres s'appuient sur une approche partagée de la responsabilité dans le cloud.

Selon les auteurs du rapport, ce modèle de responsabilité partagée entre le fournisseur de services cloud et son client n'est pas toujours bien compris.

En outre, 8% seulement des responsables de la sécurité informatique déclarent comprendre parfaitement ce modèle censé permettre de distinguer les tâches de sécurité qui dépendent du fournisseur cloud de celles dont la responsabilité incombe au client.

Globalement, 70% des professionnels IT pensent que trop d'outils spécialisés sont nécessaires pour sécuriser leur empreinte dans le cloud public.

Pour mieux faire, près 9 répondants sur 10 (87%) considèrent l'intégration de capacités d'intelligence artificielle et d'apprentissage machine comme une urgence.

**Le rapport agrège les résultats d'une enquête menée en ligne par Enterprise Strategy Group (ESG) pour Oracle et KPMG. 750 professionnels de la cybersécurité et de l'IT d'entreprises de taille intermédiaire et de grands groupes privés et publics ont été interrogés. France, Royaume-Uni, États-Unis, Canada, Japon, Singapour et Australie sont couverts.*

(crédit photo via pexels)