RSSI : 3 points à retenir sur les risques liés aux tiers

Malgré la hausse du nombre de services IT externalisés et de données partagées, les entreprises manquent de visibilité sur leur exposition aux risques liés aux tiers.

C'est l'un des enseignements d'un rapport anglophone commandé par Opus, éditeur de solutions de conformité, gestion du risque et connaissance client, au Ponemon Institute.

1000 responsables de la sécurité des systèmes d'information (RSSI) et gestionnaires du risque ont été interrogés. (source : *2018 Data Risk in the Third-Party Ecosystem*).

1. Big data, gros risques

59% des répondants ont déclaré que leur organisation a été victime d'une violation de données provoquée par un fournisseur ou une tierce partie l'an dernier.

Un taux en hausse de 3 points par rapport à la précédente édition du rapport.

Malgré tout, les entreprises continuent de partager des informations sensibles avec des tiers dont elles connaissent peu les pratiques data.

2. Faire l'inventaire

Chaque organisation partage des informations avec plusieurs centaines de tiers (plus de 500 en moyenne par entité). Or, 34% des répondants seulement disposent d'un inventaire « complet » des tiers avec lesquels des informations sensibles sont partagées.

Le manque de contrôle centralisé, le déficit de ressources et la complexité des relations fournisseurs sont les principaux freins cités par les RSSI.

Dans ce contexte, moins d'un département de sécurité IT sur deux considère efficace la gestion du risque lié aux tierces parties pratiquée dans l'entreprise.

3. Coopérer

Malgré la pression réglementaire (RGPD…), une courte majorité déclare manquer de visibilité sur les pratiques de fournisseurs en matière de protection des données.

Pour Opus, qui lui-même compte AWS et Rackspace parmi ses partenaires technologiques, les RSSI et les gestionnaires du risque ont tout intérêt à coopérer.

Et à mettre en oeuvre un plan de détection et d'atténuation des risques. L'ensemble nécessite, selon l'éditeur, une « gouvernance stricte » et des technologies d'automatisation.

(crédit photo © GlebStock – Shutterstock)