

Résilience IT : des entreprises toujours sous pression

La multiplication des cyber attaques et du volume de données échangées met à rude épreuve la résilience informatique des entreprises. C'est ce que révèlent les premiers résultats d'une [enquête*](#) internationale promue par le fournisseur spécialisé Zerto.

91% des décideurs IT interrogés par IDC pour Zerto ont déclaré que leur organisation a connu au moins une interruption d'activité associée aux technologies ces 24 derniers mois.

Par ailleurs, 89% des répondants ont précisé que leur entreprise a été la cible d'une attaque malveillante réussie au cours des 12 derniers mois.

Dans 93% des cas, des données ont été corrompues ou perdues. En outre, 56% ont indiqué que des données ont été jugées irrécupérables à la suite de ces attaques cyber.

53% estiment que leur système de sauvegarde ou de récupération a échoué. 48% pointent une erreur humaine.

Comment mieux gérer le risque ?

Faire converger sauvegarde et protection des données

Pour le cabinet d'études IDC, les entreprises ont tout intérêt à adopter une approche plus intégrée de la sauvegarde, de la récupération après sinistre et de la continuité d'activité.

93% des répondants prévoient d'ailleurs de faire converger leurs outils de sauvegarde et de protection des données dans les 24 mois. Et ce pour éliminer les doublons, sans sacrifier la sécurité.

Or, les tests de résilience IT sont encore trop souvent négligés.

En effet, selon une [autre étude](#) (Ponemon Institute), 77% des organisations n'appliquent pas de manière uniforme dans l'entreprise de plan de réponse aux incidents de sécurité (CSIRP).

De surcroît, parmi les organisations qui gèrent un CSIRP d'envergure, 54% (53% en France) ne réalisent pas de test de résistance régulièrement.

*L'enquête « The State of IT Resilience 2019 » a été menée par IDC auprès de 500 décideurs IT dans le monde. Les premiers résultats ont été dévoilés lors de la conférence ZertoCon 2019.