



Faut-il réviser le plan de reprise d'activité après sinistre ?¹

Certains problèmes restent d'actualité dans les entreprises. Les deux activités de *sauvegarde/restauration* et de *reprise d'activité après sinistre*, bien que traitées dans les entreprises depuis longtemps, sont encore deux sujets de préoccupation. Pourquoi ces deux domaines continuent-ils d'intéresser les directions des systèmes d'information (DSI) ? Parce que leur situation dans les entreprises n'est pas aussi bonne qu'elle devrait l'être : les pratiques utilisées – quand elles le sont – ne répondent pas souvent aux véritables besoins.

Or, quand on dialogue avec les DSI sur leur protection de données, on s'aperçoit que beaucoup de sauvegardes/restaurations présentent des *faiblesses* et que les plans de reprise d'activité (PRA) ou de continuité d'activité (PCA) sont soit *ignorés* soit encore *en cours de définition*. Heureusement, nous rencontrons des situations où ces deux activités sont exécutées avec succès.

Nous avons réalisé, chez une grande société de service informatique indépendante (fonction personnel), une étude visant à faire évoluer leur système de continuité de service après sinistre. Qu'elle était la situation existante ? Un plan de reprise d'activité très bien conçu et régulièrement testé.

Il comportait, parmi ses principaux composants :

- un système de sauvegarde/restauration bien adapté à leur environnement informatique ;
- une *organisation de continuité d'activité après sinistre* comprenant une personne dont une partie de son temps est dédiée à cette activité, un plan de reprise dynamique et évolutif, une analyse des risques, des tests réels et réguliers (deux fois par an), un site externe de reprise ;
- un comité de direction parrainant toutes les actions nécessaires pour obtenir un plan de reprise efficace et à coût acceptable.

Il faut noter que les périodes de tests sont concrètes car elles impliquent en direct tous leurs clients (plusieurs milliers). Tous les systèmes de production sont arrêtés, ainsi que les réseaux de connexion avec les clients. Seuls les systèmes et réseaux d'un site de reprise, et les personnes dédiées à ce nouveau rôle, sont actifs afin de servir pendant une journée, dans un nouveau contexte légèrement affaibli, leurs clients.

Quant à la demande d'évolution de leur système de continuité d'activité après sinistre, elle consistait à remplacer leur site de reprise, trop proche (une dizaine de kilomètres) du site d'exploitation, par un nouveau site beaucoup plus éloigné (un millier de kilomètres) et pouvant rendre des services supplémentaires au réseau européen de l'entreprise.

Cet exemple simplifié montre toute la largeur de la palette des plans de protection des systèmes d'information des entreprises : allant de l'insuffisant (voire inexistant) au plus évolué.

Rappelons que le risque, danger éventuel plus ou moins prévisible, met clairement l'accent sur l'incertitude de sa survenue et la possibilité d'anticiper le péril. C'est pourquoi *l'atténuation des risques* prend une grande importance. Aussi, la plupart des entreprises doivent prendre la mesure des risques qu'elles encourent dans certains domaines critiques, en disposant, par exemple, d'un plan de reprise après sinistre *adapté à leur métier*.

StorageAcademy est à votre disposition pour vous aider à bâtir ou améliorer votre PRA/PCA.

¹ Provient de l'éditorial de JC Maury rédigé pour la revue Perspectives n° 38 de Gartner France