Fiche Pratique

CRiP Club des Responsables d'Infrastructures et de Production

En association avec le CCA

PRA - PCA

PRA et sinistre régional

De l'opportunité de posséder un troisième site informatique ou site de secours ultime

Synthèse

Un sinistre d'ampleur régionale impacte par définition une zone géographique étendue qui peut s'étendre sur des centaines de kilomètres carrés. Le sinistre régional, du fait de son ampleur, peut arrêter le fonctionnement d'un site de type Dual Site ou d'un site de production et de son site de secours si ce dernier ne se situe pas à une distance suffisante. De plus, ce type de sinistre s'accompagne souvent de conséquences catastrophiques, à même de paralyser une région entière : il se produirait vraisemblablement des pertes humaines, les moyens de communications se trouveraient largement endommagés, toutes les entreprises du secteur seraient alors impactées.

Pour pallier ce type de sinistre, il est nécessaire d'anticiper un événement d'ampleur régionale en mettant en place un troisième site distant de plusieurs centaines de kilomètres du ou des sites primaires. Ce site a pour finalité première d'assurer un secours ultime, de protéger le capital informationnel le plus critique de l'entreprise. Il faut donc y prévoir une solution de survie a minima, avec accès au réseau d'entreprise et stockage de données. Les autres équipements y seraient mis en place après le sinistre seulement, et financés par les assurances. Il permettrait la survie de l'informatique de l'entreprise.

Actuellement, il n'existe pas d'obligation réglementaire imposant de posséder un tel site.

En 2012, une infime quantité de sociétés disposent d'un tel site assurant une reprise d'activité, même a minima, suite à un sinistre régional ; les coûts étant jugés trop importants au regard de la faiblesse du risque. Les SAIV – Secteur d'Activité d'Importance Vitale – ont l'obligation de répartir leurs systèmes d'information sur plusieurs sites. Seules quelques filiales françaises de sociétés américaines ont mis en place un troisième site de secours. Les SAIV – Secteur d'Activité d'Importance Vitale – doivent répartir leurs systèmes d'information sur plusieurs sites.

Néanmoins, le dérèglement climatique s'accentuant, le risque de sinistre régional devrait progresser.

Mai 2012

Contexte

Suite, par exemple, à une tempête, à une inondation, à un blocage généralisé de l'économie (type événements de Mai 1968), à un tremblement de terre, à une catastrophe nucléaire, à un sinistre type SEVESO, à un acte terroriste, etc., une surface de plusieurs dizaines ou centaines de km² peut se trouver sinistrée. On parle alors de sinistre régional. L'impact atteint une ampleur catastrophique.

En France, nous pouvons citer dans cette catégorie la crue centennale de la Seine (1910), les tempêtes Lothar et Martin (décembre 1999) et Xynthia (2010), les pluies torrentielles dans le Gard. A l'automne 2011, la première tempête tropicale constatée en Europe a eu lieu dans le département du Var.
En Italie, le tremblement de terre dans les Abruzzes a malheureusement causé la mort de plusieurs dizaines de personnes et impacté gravement plusieurs entreprises. Nous avons connaissance de deux de ces entreprises qui ont réussi à reprendre leur activité, l'une par une solution prévue de contournement et l'autre par une solution opportuniste :

- Une usine pharmaceutique, entièrement détruite, a assuré sa continuité d'activité grâce à la mise en place prévisionnelle de stocks tampons à plusieurs centaines de kilomètres, un an avant le sinistre. L'usine n'a pas été reconstruite.

- L'un des centres informatiques d'une entreprise d'électronique, entièrement détruit, a été replié sur un autre centre informatique de la région de Rome. Le matériel a été récupéré avant l'interdiction d'accès sur la zone. La reprise d'activité informatique a eu lieu en quelques jours.

Problématique

Deux sites informatiques distants de quelques dizaines de kilomètres peuvent être rendus impraticables pendant plusieurs semaines par un sinistre régional. D'autant plus que ce type de sinistre implique des désorganisations de fond allant bien au-delà du seul choc initial : pertes humaines et perturbations considérables dans les communications, les déplacements et le fonctionnement économique de la zone touchée.

Il faudrait donc pour y faire face disposer d'un site supplémentaire situé à une distance suffisamment importante pour limiter les risques de voir à la fois les sites principaux et ce site de secours ultime impactés simultanément. Pour ce faire, il faut prendre en compte l'éloignement, mais aussi des facteurs supplémentaires et vérifier que le site supplémentaire ne se trouve pas soumis aux mêmes risques que les sites principaux : éviter la localisation sur une même plaque sismique ou sur le même bassin fluvial par exemple, sur le chemin des mêmes tempêtes. Il faut aussi se soucier de l'indépendance des réseaux de fourniture d'électricité et de connexion au réseau de télécommunications. Enfin, il faut vérifier que les différents sites ne risquent pas de se trouver affectés par les mêmes perturbations des réseaux de transports.

> *Rappelons que la distance entre deux sites informatiques n'est actuellement pas réglementée en France. Certaines sociétés américaines imposent à leurs filiales françaises de posséder un site de secours distant d'environ 500 kilomètres de leur(s) site(s) principal(aux).*

Rappelons aussi que la réplication synchrone inter-sites est limitée par la distance. L'éloignement admissible varie en fonction du profil des applications et des systèmes mis en œuvre. Des distances de 40 à 100 km ont été constatées. Mais les lois physiques fondamentales limitant la vitesse de propagation de la lumière dans une fibre optique font que la latence engendrée lors de réplications sur des distances plus importantes provoquerait des ralentissements problématiques en particulier dans les traitements batch.

Enfin, l'exploitation d'un site éloigné peut poser des problèmes d'intervention. Une grosse partie des opérations sont certes réalisables par télé-exploitation. Cependant certaines opérations physiques de maintien en condition opérationnelle exigent une présence physique sur site. Il faut donc posséder soit des équipes locales, soit un contrat de sous-traitance avec une entreprise capable d'intervenir sur place.

Analyse

Le rôle du troisième site n'est pas d'assurer le redémarrage de l'ensemble des traitements informatiques de l'entreprise, mais de permettre au moins le redémarrage des éléments qui autorisent une poursuite de l'activité même sur un mode dégradé. De plus, dans ce cas de reprise ultime, on peut accepter un délai de reprise et des pertes de données raisonnables. Les niveaux de pertes acceptables et les délais de reprise doivent être précisés dans l'étude préliminaire en fonction des moyens de secours envisagés. Ils doivent être validés par la Direction Générale.

Il existe des stratégies très différentes concernant ce site de recours ultime, stratégies déterminées en particulier par les possibilités physiques des entreprises. Les entreprises possédant déjà au moins deux datacenters dans des régions éloignées non soumises aux mêmes risques (par exemple un maillage de sites multi-nationaux) peuvent en fait se dispenser de posséder ce troisième site, ou en réduire fortement le besoin. Il faudra cependant, et ce dans toutes ces situations, mettre en place les procédures et les exercices nécessaires pour se préparer à réagir à un sinistre de type régional.

La possession d'un troisième site apporte par ailleurs quelques avantages :

- Un principe général de maîtrise du risque pour les sites informatiques consiste à éviter d'attirer sur eux l'attention de personnes mal intentionnées, en veillant à leur discrétion. La localisation du troisième site de secours doit être tenue secrète, ou du moins rester confidentielle. Il est conseillé de lui donner un nom mnémonique et en règle générale de donner le moins de publicité possible à ce site en limitant l'affichage d'informations trop visibles.
- Un troisième site secours s'avérera potentiellement utile dans un changement de stratégie de sauvegarde. Par exemple en abandonnant l'externalisation des cassettes au profit d'une externalisation sur un troisième site, dans le cadre d'un projet VTL.
- Le troisième site de secours peut être utilisé pour héberger la pré-production. Il faut s'organiser pour gérer la charge du réseau, en cas de fonctionnement réel sur ce site.
- Certaines entreprises ont trois sites. Pour des raisons variées (acquisition d'une autre société, mise en place d'un dual site avec deux sites rapprochés, appartenance à un groupe international), l'un des sites devient alors naturellement le site de secours ultime pour pallier des sinistres régionaux.

Certaines applications se montrent incompatibles avec un hébergement sur le site de secours ultime, et la direction générale de l'entreprise doit en être informée. Nous citerons en particulier les applications de type temps réel, ou celles devant rester très proches des automatismes industriels et qui ne supportent donc pour des raisons techniques aucun éloignement.

En cas d'indisponibilité simultanée des deux sites principaux, le recours au troisième site pourrait s'avérer inutile si le délai de remise à niveau d'un des deux sites est acceptable par la Direction de l'entreprise.

L'expérience montre qu'en cas de sinistre régional, les fournisseurs se mobilisent pour mettre à disposition des moyens de remplacement. Mais cela reste aléatoire. Et compte tenu de la demande simultanée de plusieurs entreprises, des priorités seront appliquées, voire des réquisitions seront lancées.

> *Notons enfin que la mise en place de procédures de réplication asynchrone sur les baies du troisième site ne supprime pas le risque de corruption de données.*

Un principe général de maîtrise du risque pour les sites informatiques consiste à éviter d'attirer sur eux l'attention de personnes mal intentionnées, en veillant à leur discrétion. La localisation du troisième site de secours doit être tenue secrète, ou du moins rester confidentielle. Il est conseillé de lui donner un nom mnémonique et en règle générale de donner le moins de publicité possible à ce site en limitant l'affichage d'informations trop visibles.

Conclusion

Les avantages de la mise en place d'un troisième site sont :

- L'augmentation de la robustesse de l'entreprise en cas de survenue d'un sinistre régional. Les risques climatiques augmentent depuis plusieurs années en fréquence et en intensité.

- Les sauvegardes de recours sont mieux protégées.

Par contre les inconvénients suivants s'opposent à la mise en place de ce troisième site :

- Essentiellement un coût trop important par rapport à la probabilité d'occurrence des risques couverts.

- L'absence de réglementation sur la distance inter-sites.

- La non-conformité du RTO et RPO sur un troisième site avec les besoins de continuité de certaines applications.

- Le cas des entreprises manipulant des données sensibles, ce qui pose problème en cas de transfert de ces données sur des sites distants et peut s'opposer à la mise en place d'un troisième site.

Notons aussi que dans un sinistre d'une telle ampleur les conséquences humaines risquent de s'avérer si difficiles à gérer que la possession d'un site de recours ultime ne constituerait d'une partie mineure de l'organisation à mettre en place.

En ce qui concerne l'absence de réglementation inter-sites, la perception des risques diffère cependant de façon considérable en Europe et aux États-Unis. Ces derniers ont développé une plus grande sensibilité aux sinistres naturels, effectivement plus fréquents sur leur continent, ce qui les incite à une meilleure prise en compte des problèmes de sinistres régionaux.

> *Pour rappel, l'existence d'un troisième site nécessite la mise en œuvre d'exercices annuels faute de quoi il ne sert à rien …*

Conclusion

L'adoption d'un troisième site est fortement liée à la couverture du risque que souhaite atteindre l'entreprise (et bien entendu à l'estimation du rapport cout/prime). La résilience ne tient parfois qu'à peu de choses.

Les approches de virtualisation lancées depuis plusieurs années et l'émergence des offres Cloud devraient à terme offrir des solutions alternatives moins onéreuses et plus agiles pour aider les entreprises à répondre à la nécessité de reprise d'activité ultime après sinistre.

Rédaction : Groupe de Travail PRA-PCA - Assistance Editoriale : Renaud Bonnet, CRiP - Création Fred.lameche - www.anousdejouer.fr

CRiP

Club des Responsables d'Infrastructures et de Production
15 rue vignon 75008 PARIS - contact@crip-asso.fr www.crip-asso.fr

Club de la Continuité d'Activité
73 rue Anatole France 92300 LEVALLOIS PERRET - contact@clubpca.eu www.clubpca.eu