50e numéro !

LIREC

Lettre d'information sur les Risques et les Crises

N°50 - MARS 2016

DOSSIER THÉMATIQUE

AIDER LES VICTIMES

ACTUALITÉ NATIONALE

DE L'INTÉRÊT DE LA PLANIFICATION

POINT DE VUE

COMMUNICATION DE CRISE, les maires ont-ils leur mot à dire ?

CONTINUITÉ D'ACTIVITÉ

PLAN DE REPRISE D'ACTIVITÉ PRA

INHESJ

CONTINUITÉ D'ACTIVITÉ

LE PLAN DE REPRISE D'ACTIVITÉ
PRA

Le sujet que nous abordons aujourd'hui traite du Plan de Reprise d'Activité (PRA) (ou de continuité / plan de secours informatique) et fait suite aux précédents articles du feuilleton de la continuité d'activité publié dans les LIREC depuis juin 2015. Ce sujet du PRA est un sous ensemble du Plan de Continuité d'Activité (PCA) pour lequel nous avions présenté les quatre macro-scénarios de risques pouvant impacter une organisation :

- ✓ **Bâtiment impraticable :** *panne totale de l'alimentation électrique, blocage des accès par interdiction administrative suite à fuite de gaz liée à des travaux sur la voie publique, incendie, coupure de la téléphonie suite à des travaux sur la voie publique…*
- ✓ **Perte d'accès aux systèmes d'information :** *coupure du réseau suite à des travaux sur la voie publique, panne matérielle ou logicielle, attaque virale, cyberattaque…*
- ✓ **Indisponibilité durable de personnes (70 % du personnel, toutes compétences confondues) :** *pandémie virale…*
- ✓ **Indisponibilité de fournisseurs essentiels ou de fournisseur de fournisseur :** *indisponibilité de services critiques dispensés par un fournisseur.*

Parfois, les scénarios de risque peuvent se combiner pour générer un risque encore plus important, par exemple pour la crue de la Seine.

Nous traitons ici spécifiquement de la riposte prévue pour pallier le scénario d'indisponibilité du système d'information, quelle qu'en soit la cause, pour lequel le PRA constitue une solution de réponse indispensable.

Il faut noter dès maintenant que les incidents de production informatique mineurs ou quotidiens ne sont pas traités par le PRA. En effet, ce dernier prend en compte seulement les incidents rares, plus graves pouvant aller jusqu'aux sinistres majeurs qui bloquent partiellement ou totalement l'accès aux systèmes d'information ou leur fonctionnement pour une durée indéterminée. De plus, le déclenchement d'un PRA n'est pas anodin et fait l'objet d'un pilotage par une cellule de crise dédiée.

LA CONTINUITÉ D'ACTIVITÉ ET LE PRA

La démarche générale de « Continuité d'activité » consiste à envisager des interruptions de fonctionnement des activités de l'organisme et à décider de ce que l'on fait en matière de prévention et de réaction. Elle explore deux directions antagonistes qui consistent à :

- mener des actions préventives ou de diminution de risques d'indisponibilité : pour l'informatique en particulier, cela consistera à équilibrer les traitements dans des serveurs mis en grappe, capables de se relayer l'un l'autre afin que l'utilisateur ne voit rien si l'un d'eux tombe,
- préparer des plans de reprise : lorsque le sinistre est là, que la prévention n'a pas suffi, il faut savoir réagir et pour cela, il faut avoir envisagé préalablement les moyens de secours.

Ainsi, comme on peut le constater précédemment, la prévention ne peut pas tout éviter. Concernant le système d'information, même si le service informatique a bien réparti des serveurs dans deux salles sur un même site, celui-ci peut être contraint en même temps à l'arrêt forcé par un incendie ou un arrêt électrique imposé par les pompiers suite à une fuite de gaz, par exemple.

On voit alors qu'il faut aussi prévoir une possibilité de reconstruire ou récupérer des moyens en-dehors de la zone sinistrée, par exemple d'autres serveurs chez un hébergeur ou d'autres bureaux chez un site partenaire. La planification de tout cela, associée à celle des ressources techniques et humaines constitue le PRA ou « Plan de Reprise d'Activité ».

La continuité d'activité ne peut se passer de PRA correctement dimensionnés. Ce point est d'ailleurs très important car il convient, en cas de sinistre, de pouvoir mettre à disposition dans des délais acceptables et convenus des moyens adéquats hors zone sinistrée. Dans un contexte de PRA, il ne s'agit pas de doubler tous les moyens pour le lendemain matin car un organisme doit être conscient des coûts générés par cette solution de PRA pour couvrir des risques peu fréquents et des priorités financières à gérer au quotidien.

LES SCÉNARIOS DE RISQUES

Quels sont les scénarios de risque envisagés dans un PRA ?

Tout d'abord, il faut considérer que les menaces sont multiples, mais elles sont catégorisables selon l'origine de leur nature : soit environnementale, soit accidentelle, soit délibérée. Vous trouverez dans le tableau suivant un extrait de la norme ISO27005 donnant plusieurs exemples.

Ces menaces, quand elles se concrétisent par des événements réels, deviennent des scénarios de risques qui se traduisent eux-mêmes par une indisponibilité du système d'information. Dès que l'on sait ou estime que les besoins de continuité

SUITE P.46 …

Tableau 1 - Extrait de la norme ISO 27005

Type de menaces	Menaces
Dommage physique	Incendie, dégât des eaux, destruction de matériel ou de support ...
Catastrophes naturelles	Phénomène climatiques, phénomène sismique, inondation ...
Perte de services techniques essentiels	Panne du système de climatisation ou d'alimentation en eau, perte de la source d'alimentation en électricité, panne du matériel de télécommunications ...
Compromissions d'informations	Cyber attaque, dénis de service informatique, virus, ...
Défaillances techniques des composants du système d'information	Panne de matériel, dysfonctionnement, blocage, saturation, ...
Actions non autorisées	Destruction ou altération des données

des métiers (Délai d'Indisponibilité Maximum Admissible (DMIA) – niveau de Perte de Données Maximum Admissible (PDMA) vont être dépassés ou le sont déjà, la mise en œuvre du PRA devient nécessaire.

De plus, les sinistres peuvent aussi combiner des scénarios indirects, voire cumulatifs [l'effet papillon] directs et indirects. Exemples : (1) une fuite de gaz dans le voisinage d'un centre informatique, les pompiers exigeant la coupure de l'électricité complète ! vous ne pouvez pas démarrer votre générateur : donc arrêt absolu minimum de 4 h garanti. (2) accident de camion transportant des matières toxiques, les matières se répandant et contaminant toute votre climatisation, les autorités déclassent vos locaux (inaptes au séjour de personnel). Il faut nettoyer tous les conduits et filtres de tous les organismes du voisinage. Bilan un mois d'arrêt forcé !

Il est impossible de vouloir modéliser tous les scénarios de risques, même s'il convient de détecter les plus vraisemblables. Comme pour le PCA, l'approche par l'analyse des impacts sur le système d'information reste la plus efficace pour identifier les solutions potentielles de PRA.

LES SOLUTIONS DE SECOURS (OU DE PRA) ET LES TYPES D'ARCHITECTURE DE REPRISE D'ACTIVITÉ

Reprendre l'activité, c'est aussi basculer les infrastructures techniques vers un site de secours. Aujourd'hui, nombreuses sont les solutions techniques existantes, pour répondre pratiquement à toutes les exigences... Toutefois, elles correspondent globalement à trois concepts de base :

- le secours dit « à froid » (cf. Figure 1) : c'est certainement la plus ancienne technique, datant de l'époque où la technologie ne permettait pas de faire beaucoup mieux... Pour autant, il est encore beaucoup utilisé. Le principe est le suivant : le site de secours n'est pas directement utilisable au quotidien, en cas d'activation du PRA, les moyens techniques du site de secours doivent être mis en œuvre, les serveurs remontés (et mis à jour) et les données restaurées à partir des sauvegardes.

- le secours dit « actif-passif » (cf. Figure 2) : dans ce cas, le site de secours est opérationnel au quotidien, tenu à jour en permanence, les données sont répliquées (en temps réel ou pas). En cas d'activation du PRA, la bascule technique peut être rapide car les moyens de PRA sont « en veille » et activables en « production principale » moyennant des actions de démarrage et de réajustement de réseau.

- le secours dit « actif- actif » (cf. Figure 3) : les technologies (relativement...) récentes permettent d'avoir ce type de site de secours. Ici, les deux sites sont en production (en répartition de charge) et sont le secours l'un de l'autre. Le fait d'être en production implique qu'ils sont tenus à jour en permanence, que les données sont répliquées en temps réel. En cas d'activation du PRA, la bascule technique peut être très rapide.

Attention : la réplication synchrone entre les deux sites n'est possible techniquement qu'à faible distance (environ 30km) et peut être onéreuse. Cette solution ne répond pas au sinistre de zone qui rendrait indisponible en même temps ces deux sites proches. Il faut noter que plusieurs organismes s'affranchissent de ce sinistre régional par la mise en œuvre d'une solution à distance (par exemple > 250 kms) « à froid » ou « actif – passif » décrites précédemment.

Dans les schémas ci-dessous, le chiffre en vert correspond à la charge maximale théorique du site en mode nominal, le chiffre en rouge à la charge maximale théorique du site en mode secours.

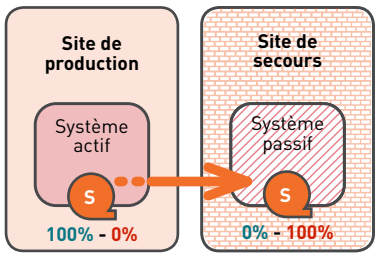

Figure 1 - Secours « à froid »

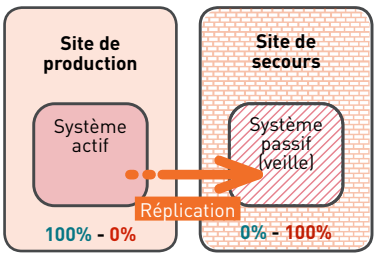

Figure 2 - Secours « actif-passif »

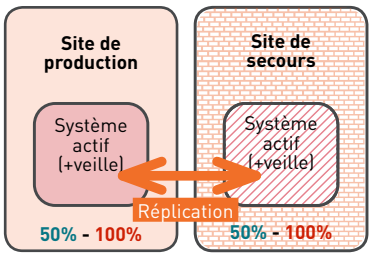

Figure 3 - Secours « actif-actif »

Tableau 2 – Avantages et inconvénients en fonction des types de solution de secours

Type de secours	Mise en œuvre	Perte de donnée à la reprise d'activité	Délai total de reprise des applications	Coûts	Distance entre les sites
Secours « à froid »	☺	☹	☹ > 48 h	☺	☺
Secours « actif-passif »	😐	😐	😐 < 24 h	😐	☺
Secours « actif-actif »	☹	☺	☺ < 4h	☹	😐

Le tableau ci-dessus présente de son côté les principaux avantages et inconvénients en fonction des types de solution de secours identifiés précédemment.

Bien entendu, ces différentes solutions peuvent également être mixées, pour répondre aux différents enjeux et aux exigences de continuité d'activité déterminées par les Métiers et aux moyens disponibles (humains et financiers).

Attention : en cas de corruption de données sur le site de production initial, la réplication sur le site de secours peut produire une corruption de données sur ce site de secours lui-même dont les données ne sont alors pas réutilisables. Un retour arrière à une situation non corrompue est forcément nécessaire à partir d'un niveau de sauvegardes adéquat.

LES SAUVEGARDES DE RECOURS

L'élaboration d'une stratégie de PRA ne saurait être complète sans la prise en compte au préalable d'une vraie stratégie de sauvegarde et de restauration garantissant en toute circonstance le redémarrage de l'activité.

Une question revient de plus en plus souvent : « Pourquoi continuer à avoir une politique de sauvegarde drastique alors qu'il existe de multiples solutions de réplications de données en temps réel, d'images système, RAID5, ...? ».

Pour rappel, les sauvegardes permettent de revenir en arrière face à une corruption de données (virus, vers, ...) ou à une suppression involontaire ou malveillante d'informations ou encore à une mise à jour défaillante, ... Elles permettent également de reconstruire un système complet et de faire face à une erreur humaine (erreur de sens de réplication, effacement, mise en production d'une version bugée...).

Cette stratégie de sauvegarde doit prendre en compte la notion de PDMA (Perte de Données Maximale Admissible) demandée par les Métiers et acceptée par la Direction Générale.

Globalement, il existe trois types de sauvegardes répondant à trois besoins différents.

1- Les sauvegardes courantes de « Production » : elles ont pour vocation de répondre de façon rapide et efficace à un incident courant d'exploitation (ex : effacement d'un fichier, ...). Elles doivent être accessibles immédiatement afin de résoudre le problème au plus vite. Un stockage physique des supports de sauvegarde sur place peut s'envisager, idem si la solution de sauvegarde est sur disque.

2- Les sauvegardes de « Recours » : elles ont pour objectif de faire face à un sinistre majeur (cas du PRA). Elles doivent contenir des images complètes et fiables du système d'informations en vue de pouvoir le reconstruire en partant de zéro : données, applications, fichiers de configurations, procédures techniques, carnet d'exploitation...

Quelques points d'attention : de telles sauvegardes doivent être pensées en amont de la mise en production d'une nouvelle application ou de toute autre solution impactant le Système d'Information. Elles devront être réalisées sur des périodes prédéfinies et régulières même si la prise de sauvegarde peut se révéler délicate à mettre en œuvre (à quel moment sauvegarder, combien de temps peut durer l'opération compte tenu de l'importance des volumes à sauvegarder ?). La perte potentielle de données entre deux prises de sauvegardes doit d'autre part être étudiée. Les sauvegardes de recours doivent être impérativement stockées sur un site distant, de préférence hors du périmètre du site principal et accessibles à tous moments (24/24, 7/7). La sécurité de celles-ci doit être optimale, appliquée et contrôlée tant sur les procédures de sauvegardes et restauration que sur la protection des données sauvegardées.

3- Les sauvegardes « d'Archivage » ont pour objet de conserver des données à des moments précis à des fins de preuves. En général, elles ne demandent pas un accès immédiat et ne nécessitent plus d'occuper de la place dans les environnements de Production. Leurs durées de conservation sont variables et dépendent de la législation. Par exemple, les contrôles fiscaux et/ou URSSAF demandent de remonter sur plusieurs années.

Sauvegarder c'est bien, restaurer c'est mieux dit l'adage. Quel que soit le type de sauvegarde, leur fiabilité doit être sans faille et régulièrement éprouvée. Des tests de restauration partiels ou complets doivent être réalisés pour s'assurer de la viabilité des supports, de la bonne restauration des informations sauvegardées et de la cohérence de l'ensemble quant aux besoins exprimés par les Métiers. Ces tests ont aussi pour vocation de préparer les équipes à la restauration et reconstruction d'un ou plusieurs systèmes en phase de stress.

EN SYNTHÈSE

Un PRA dans sa globalité doit être testé et validé régulièrement, sinon, il ne fonctionnera pas en cas de besoin et l'investissement n'aura servi à rien. Des tests techniques et des exercices d'entrainement réguliers probants sont nécessaires. Ce sujet sera développé ultérieurement dans un article consacré à la validation du PCA, incluant le PRA.

D'autre part, il faut bien noter que le site de secours (du PRA) n'est qu'une adaptation du site de production initial. Ainsi, ce site de PRA doit être maintenu en condition opérationnelle en permanence et pour ce faire doit être intégré au processus de gestion des changements informatiques.

De la même façon, le sujet du MCO (Maintien en Condition Opérationnelle) sera développé dans un prochain article.

SUITE P.48 ...

En cas d'indisponibilité du système d'information, qu'elle qu'en soit la cause, pour une durée indéterminée, des milliers de traitements en cours sont arrêtés brutalement, d'autres peuvent éventuellement continuer à fonctionner. Même si le PRA peut s'avérer compliqué à mettre en œuvre et à maintenir car il fait appel à des solutions techniques complexes, même si la reprise d'activité des applications entre elles est compliquée et n'est pas automatisable, néanmoins, le PRA est absolument nécessaire pour éviter à l'organisme de perdre des flux reçus et d'en renvoyer de nouveaux qui engendreraient des doublons (commandes, virements, ordres...), voire un arrêt total de l'organisme.

Depuis plusieurs années, le *World Economic Forum* expose, dans son rapport annuel, la montée en puissance des risques liés à l'indisponibilité du Système d'Information parallèlement à l'augmentation de la cyber menace. Le PRA constitue une réponse à cette préoccupation mais il n'a de sens réel que s'il répond aux attentes et exigences de continuité des métiers, ainsi qu'à l'appétence risque de l'entreprise. Ce PRA du Système d'Information, une fois rodé, constitue ainsi la première étape œuvrant à la continuité globale de l'entreprise en cas de risque majeur ■

LES PROCHAINS ARTICLES DU FEUILLETON « CONTINUITÉ D'ACTIVITÉ » :

✓ la continuité d'activité en lien avec les prestataires externes essentiels

✓ la continuité d'activité et la supply chain (chaîne logistique)

✓ la validation du PCA par des exercices

✓ le maintien en condition opérationnelle des PCA

✓ le système de management de la continuité d'activité et la normalisation

LES CONTRIBUTEURS
(par ordre alphabétique)

Emmanuel BESLUAU

Ingénieur informatique, diplômé de Centrale et de l'Université de Berkeley, Emmanuel BESLUAU a occupé de nombreux postes à responsabilités dans de grands groupes (IBM, Sligos, Centre National Carte Bancaire, Atos-infogérance...). Aujourd'hui, Consultant associé au Duquesne Group, il écrit périodiquement dans la presse informatique et intervient en tant qu'expert reconnu auprès de DSI sur des sujets comme la continuité de service, les architectures techniques des centres informatiques, les bonnes pratiques de production de service (ITIL, sécurité...) Il est administrateur du CCA (Club de la Continuité d'Activité). Il est l'auteur de l'ouvrage « Management de la continuité d'activité» (Eyrolles).

Eric MILTON

Eric MILTON intervient depuis 1996 dans le domaine de la Continuité d'Activité. Faisant le constat que les sujets de la Continuité d'Activité et Gestion de Crise ne sont trop souvent abordés que partiellement, à savoir qu'à travers l'informatique, et peu ou pas sur ce qui fait la richesse des entreprises : les collaborateurs, les métiers, le business, Eric MILTON décide de créer AMAÏS France en 2004. Fort de son expérience acquise auprès de clients de renommée internationale, il a su développer une expertise visant à élaborer des Plans de Continuité d'Activité dans lesquels l'homme a toute sa place pour garantir la pérennité de son entreprise.

François TÊTE

Consultant expert en continuité d'activité et gestion de crise, François TÊTE a commencé sa carrière à la banque WORMS. Suite à un sinistre informatique en 1977, il a acquis une expérience de terrain dans ce domaine. Il s'est ensuite spécialisé dans la continuité d'activité. Il a créé en 1994, le logiciel de gestion de PCA RVR PARAD. Il a été l'un des créateurs en 2007 du Club de la Continuité d'Activité.

Nicolas de THORE

Consultant expert en continuité d'Activité, Nicolas de Thoré a fait sa carrière chez IBM France dans le conseil et la mise en œuvre de solutions et services, dont 15 années en tant qu'expert reconnu en continuité d'activité. A ce jour, Consultant indépendant, il intervient dans la mise sous contrôle du système de management de la continuité, la réalisation de stratégie et plans de continuité aussi bien IT que métier. Il est d'autre part, ancien Vice-Président de la commission PCA (Plan de Continuité d'Activité) à l'AFNOR et actuel Vice-Président du CCA (Club de la Continuité d'Activité). Il est régulièrement sollicité pour intervenir dans des conférences sur le sujet de la continuité.

Lionel MOURER

Lionel MOURER a 27 ans d'expérience professionnelle dans les Systèmes d'Information dont plus de 17 en conseil stratégique et opérationnel en Sécurité du SI et Continuité d'Activité au profit de grands groupes, d'ETI et de nombreuses PME/PMI. Associé-fondateur d'ATEXIO, Lionel intervient sur des missions d'expertise et/ou de conduite de projets complexes, mais aussi en tant que formateur au sein de plusieurs écoles d'ingénieur ainsi que pour des instituts de formation.

Luc VRIGNAUD

Expert en sécurité des systèmes d'informations, en continuité d'activités et gestion de crise; Luc VRIGNAUD a travaillé pour plusieurs acteurs comme Cap Gemini, General Electric... Il est actuellement RSSI et RPCA du Groupe Macif.