PROTECTION
DU
SYSTEME D'INFORMATION

SOMMAIRE

1. INTRODUCTION

La personne, qui a en charge un site informatique, se doit de définir la qualité de service qu'elle s'engage à fournir à l'ensemble de ses clients-utilisateurs.

La qualité de cette prestation doit être négociée avec les représentants des clients-utilisateurs, afin de trouver un compromis entre la teneur de la prestation et le coût de celle-ci. Cela pourra donner lieu, même en interne, à la signature d'un contrat de service.

Ce contrat de service s'orientera autour de 4 axes principaux :

- La confidentialité et la sécurité d'accès aux ressources
- La sécurité des données et la politique de sauvegarde
- La disponibilité de l'« énergie informatique »
- L'aptitude à faire face à un sinistre informatique

Le contrat de service permettra de fixer les règles de la relation client-fournisseur entre les utilisateurs et le site informatique.

Il favorisera la mise en place d'une répartition analytique des dépenses informatiques vers les clients-utilisateurs, par la création d'unités d'œuvre.

En contrepartie, les moyens financiers (investissements et fonctionnement) et humains à mettre en place devront être négociés, soit globalement, soit avec chaque entité « budgétaire » selon l'organisation de l'entreprise.

2. LA CONFIDENTIALITE ET LA SECURITE D'ACCES AUX RESSOURCES

Toutes les enquêtes l'affirment, la principale source de perte d'intégrité du système d'information provient d'actes de malveillance ou d'erreurs humaines du propre personnel de l'entreprise (beaucoup plus que de l'intrusion par des hackers par exemple). Pour pallier ce risque, la meilleure protection consiste à limiter l'accès, pour un utilisateur, aux seules ressources dont il est amené à avoir l'usage professionnellement.

2.1. Préalable

Avant de définir une stratégie sur la confidentialité et la sécurité d'accès aux ressources, il convient de répondre à la question clé :

A-t-on besoin de prendre de telles mesures dans mon entreprise ?

Ce n'est qu'après avoir répondu par l'affirmative à cette question, que l'on adoptera la démarche suivante :

- évaluer, pour l'entreprise, les risques liés au non-respect de la confidentialité des données (techniquement, commercialement, légalement, etc.)
- établir la liste des ressources (matérielles, applicatives, données, etc.) susceptibles de nécessiter la mise en place de mesures de contrôle d'accès
- Déterminer les personnes pouvant définir le niveau de sécurisation d'accès à ces ressources
- Affecter à chacune de ces ressources le niveau de contrôle d'accès requis
- Appréhender les conséquences d'une sécurisation maximum

2.2. La gestion des utilisateurs

Si l'on veut être à même d'assurer un bon niveau de confidentialité et d'administrer précisément l'accès aux ressources, il est essentiel de donner un identifiant individuel à chaque utilisateur (PUID : Personal User IDentifier ou User ID). A ce nom d'utilisateur sera associé un mot de passe obligatoire ou optionnel, selon le niveau de protection souhaité.

Il convient également de déterminer le nombre d'accès concurrents pour un même utilisateur, c'est-à-dire le nombre de connexions simultanées avec un même identifiant.
Pendant longtemps la connexion unique a été la règle, mais pour des raisons liées à la sécurité des personnes, ceci est en train d'évoluer (cas de Windows NT Server par exemple) sans pour autant que ce soit toujours paramétrable.

La possibilité de déconnexion automatique d'un utilisateur sans activité depuis un temps donné sur les ressources est souvent préconisée, car cela signifie généralement que la personne n'est plus présente devant son poste de travail et qu'elle a omis de se déconnecter, ce qui enfreint les règles élémentaires de confidentialité.

La définition des horaires de connexion pour chaque utilisateur est également recommandée.

Un soin particulier devra être apporté à toutes les connexions provenant de l'extérieur de l'établissement : employés " nomades " (commerciaux, techniciens de maintenance, etc.) ou travail à domicile (cadres, exploitants, etc.).
La majorité des risques d'intrusion dans le système d'information provient, en effet, de ce type de connexions, car elles s'effectuent hors du système de protection de l'entreprise et souvent dans des plages horaires, où le contrôle " humain " des accès est des plus réduit.
C'est par la mise en œuvre d'un système lourd et automatisé d'authentification (appels réentrants, cartes à puce, etc.), que l'on peut réellement parvenir à sécuriser ce type d'accès. Si une telle dépense n'est pas envisageable, il conviendra de ne proposer que des accès réduits pour ces connexions, ce qui revient souvent à créer deux identifiants pour un même utilisateur (l'un pour ses connexions dans le cadre de l'entreprise, l'autre pour ses connexions à distance).

Si l'on veut éviter que les utilisateurs notent leurs différents identifiants (post-it sur l'écran ou dans le tiroir à stylos du bureau), il est souvent nécessaire de mettre en œuvre des outils puissants. Ceux-ci permettent de se connecter avec un seul identifiant sur l'ensemble des ressources (serveurs, SGBDR, applications, progiciels, etc.). Ces outils ne sont, pour l'instant, disponibles que sur les gros systèmes propriétaires (exemple : RACF d'IBM), en raison de l'absence de normes ou de standards.

2.3. Les mots de passe

S'il est nécessaire de maintenir un niveau de confidentialité acceptable, le mot de passe devra rester secret (y compris pour l'administrateur de la sécurité) et, pour ce faire, on respectera les règles minimales suivantes :

- Durée de vie maximale du mot de passe d'un mois
- Un même mot de passe ne pourra pas être réutilisé pendant une durée donnée
- Le mot de passe aura une longueur minimale de 4 caractères

La plupart des systèmes de sécurité proposent en standard des outils permettant de mettre en œuvre ces règles. Il est possible d'aller beaucoup plus loin et des organisations imposent d'utiliser des mots de passe non significatifs (la même séquence de caractères n'existe pas dans un dictionnaire et / ou il comprend systématiquement des chiffres et des lettres).

2.4. Les profils

Dans la plupart des cas, de nombreux utilisateurs possèdent les mêmes droits d'accès sur une ressource. Afin de faciliter l'attribution de ceux-ci, il est utile de créer des " profils de connexion " qui permettent d'associer un utilisateur au type d'accès auquel il a droit sur la ressource.

Il s'agit donc en fait de regroupement d'utilisateurs dans des entités plus larges. L'allocation des droits se fera très finement sur cette entité et chaque utilisateur sera affecté à l'une des entités créées.

Dans ce domaine, le vocabulaire est très dépendant du système de sécurité, on parlera de :

- Groupes globaux et groupes locaux sur Windows NT Server
- Scripts de connexion (ou login script) sur Novell Netware
- Groupes d'utilisateurs sur AS/400

Il en résulte que l'ensemble des droits d'un utilisateur sera la somme des droits des différents profils auxquels il appartient.

2.5. Le contingentement

La limitation du nombre d'accès à une ressource (par exemple pour des problèmes de licence) ou de la consommation (impressions en couleur, modem, etc.) ne sera pas abordée ici.

3. LA POLITIQUE DE SAUVEGARDE

3.1. Préalable

Avant toute chose, il faut distinguer les domaines de décision des utilisateurs et des exploitants.

Les utilisateurs doivent essentiellement se prononcer sur la partie " données ".
Ils doivent définir :

- Les données à sauvegarder
- La périodicité de ces sauvegardes
- La durée de conservation des supports
- Le délai souhaité de remise à disposition des données en cas de restauration

La personne, à même de prendre cette décision, est ce que l'on appelle le propriétaire d'application.

Les informaticiens ont la responsabilité de l'environnement des données et doivent prévoir les sauvegardes :

- Du système d'exploitation
- Des outils système
- Des logiciels (applications, progiciels, langages, etc.) et des programmes
- De l'ensemble des paramétrages
- Des structures des bases de données et du dictionnaire

3.2. L'archivage et la sauvegarde

Il est essentiel de différencier les sauvegardes des archives.

Par exemple le fichier d'impression d'un bulletin de paie est une archive, alors que l'on peut sauvegarder les éléments ayant permis d'établir ce bulletin.
Dans un cas, on veut uniquement stocker un ensemble d'informations que l'on ne modifiera jamais.
Dans l'autre cas, on souhaite mémoriser les informations dans l'optique de pouvoir les retraiter (nouveau calcul) ou de les modifier.

Si un salarié souhaite, que son entreprise lui fournisse une copie d'un bulletin de salaire datant de plusieurs mois, il est impossible de le faire en relançant le traitement sur des informations sauvegardées. En effet, les règles de la paie auront probablement évolué dans l'intervalle et les résultats diffèreront donc de ceux que comportait l'original.

En général, lorsque l'on archive, on manipule des " images " (photographies, documents, éditions, etc.) sous forme numérique ou que l'on a numérisé pour en faciliter la réutilisation et la conservation. L'usage habituel d'une archive est sa réédition.

3.3. Les supports de sauvegarde

Il existe deux principales technologies pour les supports de sauvegarde : le magnétique (bandes, cartouches, cassettes, disquettes, disques) et l'optique (CD-ROM, etc.).
On utilise habituellement des supports magnétiques, car ils sont de nombreuses fois réinscriptibles, mais les supports optiques ont de meilleures caractéristiques techniques. Ils sont plus couramment utilisés pour faire de l'archivage.

Les principales caractéristiques techniques d'un support de sauvegarde sont :

- Le taux de transfert
- Le temps d'accès

Les supports de type ruban sont très fortement pénalisés, de par leur structure, sur le temps d'accès. Ceci n'est pas préjudiciable lors de la sauvegarde, mais allonge énormément la durée des restaurations partielles.

Les autres caractéristiques à surveiller concernent la fiabilité :

- Durée de vie du support
- Nombre de réécritures garanties

C'est à partir de ces caractéristiques que l'on définira les règles d'utilisation des supports de sauvegarde. Il faudra, ainsi, noter la date de mise en service d'une bande, le nombre de réécritures qu'elle a subi et la remplacer lorsqu'un des deux paramètres aura atteint sa valeur maximale (on ne va pas faire des économies de bout de chandelle, alors qu'il s'agit de sécuriser un système d'information).

3.4. Les différents types de sauvegarde

La **sauvegarde totale** (ou complète) permet de « copier » l'ensemble des informations du répertoire choisi.

La **sauvegarde incrémentielle** (ou incrémentale ou partielle) permet de « copier » toutes les informations ayant changé depuis la dernière sauvegarde incrémentielle ou totale.
Une sauvegarde incrémentielle s'inscrit dans un cycle ayant obligatoirement commencé par une sauvegarde totale.

Lors de la sauvegarde totale, effectuée par exemple dans la nuit du samedi au dimanche, tous les fichiers seront « copiés » et marqués par le logiciel de sauvegarde (changement de la valeur du bit d'archive). Le lundi soir, ne seront « copiés » par une sauvegarde incrémentielle, que les fichiers non marqués (création ou déplacement) et les fichiers modifiés dans la journée (depuis la dernière sauvegarde). Le mardi soir, les fichiers « copiés » seront ceux qui rempliront les mêmes conditions que précédemment : création, déplacement ou modification dans la journée.
Si dans la journée du mercredi, il y a une panne de la machine et que l'on souhaite restaurer les données sur une autre machine, il faudra en premier lieu restaurer la sauvegarde totale, puis successivement les sauvegardes incrémentielles du lundi et du mardi.

La **sauvegarde différentielle** permet la « copie » des informations modifiées depuis la dernière sauvegarde totale, mais sans marquage (pas de changement de la valeur du bit d'archive). Comme pour la sauvegarde incrémentielle, une

sauvegarde différentielle s'inscrit dans un cycle ayant obligatoirement commencé par une sauvegarde totale.

Lors de la sauvegarde totale, tous les fichiers seront « copiés » et marqués par le logiciel de sauvegarde. Le lundi soir, ne seront « copiés » que les fichiers non marqués (création ou déplacement) et les fichiers modifiés dans la journée (depuis la dernière sauvegarde). Le mardi soir, les fichiers « copiés » seront ceux qui auront été créés, déplacés ou modifiés le lundi ou le mardi (depuis la dernière sauvegarde totale).
Si dans la journée du mercredi, il y a une panne de la machine et que l'on souhaite restaurer les données sur une autre machine, il faudra en premier lieu restaurer la sauvegarde totale, puis uniquement la sauvegarde différentielle du mardi.

3.5. La journalisation

Les sauvegardes incrémentielles et différentielles sont surtout adaptées à la copie de fichiers. Lorsqu'il s'agit de sauvegarder des données, on s'appuie, en plus de la sauvegarde totale, sur la journalisation. Celle-ci est activée, soit par le Système de Gestion de Base de Données (SGBD), soit, sur gros système, par celui du moniteur transactionnel (CICS d'IBM par exemple).

La journalisation consiste non pas à stocker des données, mais à enregistrer les transactions ou requêtes ayant mis à jour ces données. C'est ce journal qui doit être sauvegardé.

Pour récupérer les données, on restaurera tout d'abord le contenu de la dernière sauvegarde totale, puis on réappliquera le journal, ce qui consistera à « réexécuter » les transactions et les requêtes enregistrées depuis la dernière sauvegarde.

3.6. Le plan de sauvegarde

En dehors des sauvegardes liées à l'environnement informatique, il faudra établir un plan de sauvegarde en fonction des informations données par les responsables d'application ou les utilisateurs.

Sur ce plan, on détermine :

- Les données à sauvegarder
- La périodicité
- Le type de sauvegarde
- Le support retenu
- La durée de conservation des supports

Grâce à ce plan, on déterminera la « rotation des supports ».

Par exemple, si l'on fait une sauvegarde totale tous les samedis soirs, une sauvegarde différentielle tous les jours et que l'on décide de conserver une sauvegarde mensuelle, on définira une rotation ressemblant à la suivante :

- Un support pour chaque jour de la semaine
- Ce support sera réutilisé dès la semaine ou la quinzaine suivante selon la précision de restauration attendue
- Un support pour chaque sauvegarde totale
- Ce support sera réutilisé la semaine, la quinzaine ou plutôt le mois suivant pour plus de sécurité
- La dernière sauvegarde du mois sera conservée

Il faudra donc pour une année, si l'on conserve la protection maximale proposée :

- 12 supports pour les sauvegardes mensuelles
- 4 supports pour les sauvegardes hebdomadaires (cas des mois de 5 semaines compris)
- 10 supports pour les sauvegardes journalières

Sur le cahier d'exploitation, on fera apparaître :

- L'ordre des sauvegardes
- La procédure de sauvegarde, si nécessaire
- La procédure de restauration

Il existe, en général, un cahier pour suivre les supports (utilisation, informations contenues, lieu de stockage, etc.).
Il convient également de joindre au support, un document rappelant ce qu'il contient et le rang du support s'il a été nécessaire d'en utiliser plusieurs pour faire intégralement la sauvegarde (par exemple : bande 4 sur 8).

3.7. Le stockage des supports

En aucun cas il ne faut conserver les supports dans le même local que le serveur.
Il vaudrait mieux les stocker dans un endroit sûr, si possible dans un bâtiment différent.
On peut également acquérir une armoire ignifugée, mais le coût en est souvent rédhibitoire pour les petites organisations.
Certaines archives sont parfois confiées aux banques pour un stockage dans un coffre, mais il est difficile de mettre en place un tel système pour les sauvegardes.
Une solution utilisée par beaucoup de PME/PMI est de stocker les supports dans le coffre de l'entreprise ou alors de les confier au dirigeant qui les conservera à son domicile.

4. GESTION DE LA DISPONIBILITE

Pendant longtemps, et plus particulièrement sur les grosses architectures propriétaires, le seul indicateur de performance de la production informatique était le temps de réponse. Autant l'intérêt de cette mesure était évident à une époque où l'informatique était essentiellement transactionnelle, autant l'absence de contrôle sur le respect des délais de livraison des traitements et des états pouvait surprendre quand on connaît également l'importance des « batchs » à cette époque.

Aujourd'hui, on doit plutôt trouver des indicateurs permettant de calibrer la qualité du service apporté aux utilisateurs.

Dans les pays anglo-saxons, on parle par exemple souvent de la mise à disposition de l'« énergie informatique », au même titre que l'électricité ou le téléphone. Cet indicateur est très bien adapté à la mesure de la performance du réseau.

Lorsque l'on parle de qualité du service rendu aux utilisateurs de l'informatique, toutes les composantes (ou le maximum d'entre elles) doivent être prises en compte :

- Accès au réseau
- Disponibilité des applications
- Intégrité des données
- Fonctionnement du poste de travail

Il convient donc de mettre en place un (ou plusieurs) indicateur permettant de rendre compte de tous ces éléments. La mesure communément utilisée est le **taux de disponibilité** (ou taux de service) de l'ensemble de ces ressources.
Selon l'étendue de la plage horaire sur laquelle on estime cette mesure valide, on cherchera à atteindre des taux pouvant aller jusqu'à 99 %.
Ceci signifie que si l'on estime que les services doivent être disponibles de 8 h à 20 h et 5 jours par semaine, la somme des durées d'indisponibilité de l'ensemble des ressources devra être inférieure à 36 minutes par semaine pour tenir un objectif de 99 %…

Pour parvenir à atteindre des objectifs aussi ambitieux, tous les dysfonctionnements potentiels devront être analysés et corrigés. On pourra alors être amené à utiliser les méthodes issues de la production des biens : analyse de risque, diagramme d'Ichikawa, cercles de progrès, etc.

On essayera ainsi de :

- Rechercher les différents événements pouvant conduire à une interruption totale ou partielle de l'exploitation du site informatique (analyse des risques)
- Connaître les moyens permettant de faire face à ces interruptions
- Déterminer les personnes susceptibles de déceler un éventuel dysfonctionnement afin d'en être au plus vite tenu informé
- Évaluer les contraintes qu'impose un fonctionnement 24 heures sur 24 et 7 jours sur 7 de l'exploitation informatique
- Évaluer les durées « prévisibles » des interruptions en fonction des moyens mis en œuvre et les coûts respectifs de ces moyens

C'est à partir de la plage d'ouverture et du taux de disponibilité souhaités par les clients, ainsi que de la complexité de l'environnement informatique, que l'on tentera de

déterminer les moyens matériels et humains à mettre en œuvre pour tenir les objectifs fixés.

Si, par exemple, la plage d'ouverture est très large, il est souhaitable que la présence d'informaticiens soit la plus continue possible. Sur un site industriel fonctionnant 24 heures sur 24, 7 jours sur 7 et pour lequel le fonctionnement informatique doit être permanent, il conviendra de maintenir des informaticiens en poste dans les mêmes conditions ou de mettre en place un système d'astreinte et d'exploitation à distance. La production informatique sera en outre complexifiée par l'impossibilité de faire l'exploitation « à froid ». Une grande partie des ressources sera continuellement en fonctionnement, ce qui ne facilite pas les sauvegardes, les mises à jour matérielles et logicielles, etc.
Dans un tel établissement, les moyens à mettre en œuvre pour assurer un taux de disponibilité proche de 100 % seront considérables : automates d'exploitation, espace disque redondant, machines de réserve (spare), personnel, etc.

5. GESTION DE LA CONTINUITE

Les équipements informatiques sont susceptibles de subir des dégradations dues soit à des phénomènes extérieurs, soit à leur propre dysfonctionnement : incendies, dégâts des eaux, surtensions, court-circuits, crashs de disques, etc.

Bien qu'il soit impératif de passer des contrats de maintenance sur les équipements, ceux-ci ne sont que d'une très faible utilité en cas de sinistre et ne peuvent être une garantie suffisante en ce qui concerne la continuité de service.

Il en résulte qu'il faut être à même, en cas de dégradation majeure du système informatique, de proposer une solution de repli permettant le maintien en fonctionnement de tout ou partie des services offerts par l'informatique, avec ou sans interruption de service.
L'ensemble des procédures permettant le redémarrage au plus vite des services offerts suite à un sinistre constitue le **plan de reprise d'activité** ou **PRA** (Disaster Recovery Plan en anglais).
Il peut également exister un **plan de continuité d'activité** (ou **PCA**) qui s'intègre en général dans une procédure globale impliquant l'ensemble de l'entreprise. Celui-ci vise à poursuivre l'activité sans interruption du service.

En aucun cas, le PRA ne peut se substituer aux mesures conservatoires de rigueur ci-après.

5.1. La sécurisation du système informatique

Les mesures habituelles de protection du système informatique sont les suivantes :

- Contrat de maintenance sur les équipements sensibles
- Mise en place de ressources supplétives (matériel de rechange)
- Contrôle d'accès physique aux appareils sensibles (y compris les équipements réseau)
- Protection électrique des machines
- Protection thermique des équipements
- Protection incendie adaptée pour les salles des machines

Pour l'ensemble de ces mesures, il faut vérifier que le coût de la protection est « raisonnable » en regard du risque à pallier.

En ce qui concerne les **contrats de maintenance**, il faut veiller à la présence d'une clause garantissant le délai de remise à disposition. Le délai d'intervention en tant que tel n'apporte rien…

Pour la quantité de **matériel de rechange** (spare) à prévoir, tout dépend du coût, de l'obsolescence et de l'importance de l'équipement. Il est envisageable d'avoir des switchs d'avance, mais c'est plus difficile pour des routeurs ou des répéteurs optiques par exemple.

Il est important de veiller à ce que les équipements ne puissent pas être détériorés ou voir leur fonctionnement interrompu. Le mieux est de prévoir, autant que possible, des lieux réservés (salle des machines) ou des armoires fermées à clé (baie de brassage et autres équipements réseau). Ces derniers sont souvent les

plus difficiles à protéger, alors que leur influence sur la qualité du service offert est primordiale.
Il existe de nombreux systèmes de **contrôle d'accès** aux appareils sensibles. Cela va du plus simple (la salle ou l'armoire fermée à clé) au plus complexe (l'empreinte rétinienne), en passant par les digicodes, cartes à puce et consorts. Il convient cependant d'adapter le coût du système mis en œuvre avec le niveau de sécurité souhaité (nous ne sommes ni dans un James Bond, ni dans Ocean's eleven).

Tous les équipements ne peuvent recevoir une **protection électrique**, il faut cependant prévoir des Alimentations Sans Interruption (ASI ou UPC en anglais), couramment appelées onduleurs, pour sécuriser les serveurs et les têtes de réseau. Ceci permet de se prémunir contre les surtensions et autres incidents liés à une qualité du courant, mais surtout donne le temps d'éteindre « proprement » (à froid) les équipements.
Les onduleurs protègent efficacement des risques électriques dus à la foudre, lorsque la surtension est transmise par le secteur. Pour sécuriser totalement une installation contre ce risque, les mesures à prendre sont d'une telle ampleur, qu'elles doivent être intégrées dès la construction des bâtiments (plan de masse, mise à la terre, etc.) et ne sont en général mises en œuvre que dans des cas très spécifiques.

La mise en place d'une **climatisation** est de moins en moins obligatoire, en effet la plage de température de fonctionnement des équipements informatiques est de plus en plus étendue. Cependant il convient de se méfier des élévations de température lorsque les matériels fonctionnent dans des lieux clos.

La **protection incendie** résulte d'une double problématique : il faut stopper le feu sans que le remède soit pire que le mal. Les systèmes habituels à base de projection d'eau (sprinklers) permettent la protection des personnes, mais conduisent à la destruction des équipements.
Il est possible de mettre en place des systèmes d'extinction à base de gaz rares, la mise en place de ceux-ci est une affaire de spécialistes et la réglementation liée à leur usage très rigoureuse.

5.2. Le plan de reprise d'activité

Afin de pouvoir redémarrer au plus vite le site informatique en cas de sinistre, il convient de :

- Connaître les différents risques de sinistre informatique auquel est exposé le site (incendie, dégâts des eaux, sabotage, etc.) : audit des vulnérabilités ;
- Évaluer les pertes d'exploitation (arrêt de la production, des livraisons, des prises de commandes, etc.) consécutives à une interruption de service : analyse des risques ;
- Évaluer le temps de redémarrage du site informatique en cas de sinistre ;
- Définir les différents moyens permettant de réduire la durée d'interruption et évaluer leurs coûts respectifs.

Ces points peuvent être déterminés en s'appuyant sur la méthode MEHARI (MEthode Harmonisée d'Analyse des RIsques).

Il faut, bien évidemment, pour favoriser le redémarrage du site que toutes les protections énoncées précédemment soient prises :

- Plan de sauvegarde correct et complet ;
- Qualité du stockage des sauvegardes ;
- Contrôle d'accès aux ressources critiques du site efficace.

On commencera par déterminer l'ordre de reprise des services offerts. Pour ce faire, on réalisera des interviews des représentants des utilisateurs, de leurs hiérarchiques et des responsables d'application, afin d'estimer le degré de criticité de chacun des services offerts et prévoir :

- Le planning de redémarrage des applications ;
- L'échéancier de remise à disposition qualitatif et quantitatif des ressources.

Une fois ces éléments spécifiés, il sera possible de déterminer les moyens à mettre en place suite à un sinistre et cela dans le respect d'un échéancier préalablement établi.

Par exemple, on pourra dire qu'il faut que 2 jours après le sinistre, 1 poste puisse accéder à la comptabilité, puis 3 au bout d'une semaine, puis l'ensemble après 15 jours.
Et ainsi de suite pour l'ensemble des applications et des ressources.

A partir de ces informations, l'entreprise pourra choisir une solution de secours. Il pourra s'agir soit de :

- Matériels de secours disponibles dans l'entreprise ;
- Équipements disponibles sur le marché achetés très rapidement ;
- Ressources distantes sur un site ami (faisant partie ou non de la même société) ;
- Site de back-up proposé par des sociétés spécialisées dans la mise à disposition de ressources ;
- Matériel mis à disposition en urgence par le constructeur.

Si on choisit l'une des trois dernières solutions, on négociera avec le partenaire de la progressivité de la remise à disposition des ressources. La prestation se situe essentiellement autour de la mise à disposition progressive de ressources CPU, mémoire et disque.
Dans le cas des sites de back-up, il s'agit d'une prestation payante même en dehors des sinistres (comme une assurance), avec une surfacturation à chaque utilisation des ressources au prorata de la consommation. Ces sites proposent annuellement ou bi-annuellement des périodes de test, afin de valider le bon fonctionnement de la solution.

Les procédures de redémarrage impliquent que les 2 sites aient des caractéristiques minimales communes :

- Lecteur des supports de sauvegarde ;
- Système d'exploitation en tenant compte des versions ;
- Système de fichiers et SGBDR.

Afin que le redémarrage de l'activité puisse se faire dans les meilleures conditions sur le site de back-up, on mesure l'importance de la qualité des sauvegardes tant applicatives que celles concernant le paramétrage ou les données.

Il est souvent nécessaire, en plus des fiches de procédures informatiques, de décrire avec une grande précision les méthodes de travail particulières à mettre en œuvre par les utilisateurs lors de chaque étape de la période transitoire. La description de celles-ci n'est bien évidemment pas du ressort du service informatique.

La plus grande difficulté à laquelle il faut faire face est la connexion des postes de l'entreprise avec les moyens du site de secours. En effet, cela implique le bon fonctionnement d'une partie non négligeable des ressources du réseau et des moyens de télécommunication.
Il en découle qu'il s'avère souvent nécessaire de ne pas mettre dans un même lieu la salle d'exploitation (machines, serveurs, disques, etc.) et la tête de réseau (routeurs, backbone, tête de ligne de télécommunication, etc.). Ce qui revient à dire qu'il y a alors 2 lieux à sécuriser et que l'un de ceux-ci ne peut, par essence, être secouru par des ressources distantes.

Comme pour l'ensemble des plans de sécurité informatiques ou non (plan Orsec par exemple), le plus difficile est d'évaluer « à froid » sa qualité et sa pertinence, alors que son coût, lui, apparaît immédiatement.
De ce fait, de nombreux chefs d'entreprise et même certains responsables informatiques n'envisagent pas de mesures supplétives en cas de sinistre informatique. Cette politique de l'autruche semble, comme pour les assurances, plus économique jusqu'au 1er incident grave.
Cependant, il faut admettre qu'un plan mal adapté coûtera cher à l'entreprise, alors que ses résultats seront médiocres en cas de sinistre, particulièrement si les mesures préventives concernant le réseau et les télécommunications ont été négligées.
Le plus important dans la démarche du plan de reprise d'activité est que l'ensemble des « clients » de l'informatique prenne conscience de l'importance de la continuité de service dans ce domaine et des risques qu'ils encourent en cas d'interruption prolongée du service offert. L'incendie de la salle des marchés du Crédit Lyonnais a prouvé qu'il était possible, lorsqu'un plan de secours ambitieux était mis en œuvre, de réduire au plus court l'interruption du service rendu.

5.3. Le plan de continuité d'activité

Comme pour le PRA, l'audit des vulnérabilités et l'analyse des risques devront être menées dans le cadre de la mise en œuvre d'un PCA. Cependant ils aboutiront à la mise en place de solutions correctives : cluster, cloud, SAN, load sharing, load balancing, etc.

Cependant, comme le risque zéro n'existe pas, il convient tout de même de prévoir un PRA.