demeure une solution bon marché, simple et assez efficace, qui a tout du moins le mérite d'exister.

- Quand toutes les autres solutions ont échoué, recourir au stockage de bandes à l'abri des désastres reste la solution ultime.
- La réglementation l'exige dans un certain nombre de cas.
- La proximité technologique avec l'archivage (qui n'est pas une sauvegarde) fait que certains utilisateurs conservent des archives à partir des sauvegardes sur bandes.

Dans la réalité, on constate que la sauvegarde sur bande combinée aux autres techniques mentionnées précédemment permet d'arriver à des solutions de compromis d'efficacité et de coût intéressantes.

La problématique spécifique de la sauvegarde des données sur PC, en particulier sur les ordinateurs portables, sera vue dans le chapitre 9.

Objectif : restaurer les données

Il ne faut surtout pas perdre de vue l'objectif auquel tous ces moyens techniques doivent parvenir : restaurer les données qui ont été perdues. La sauvegarde n'a en effet aucun intérêt si les données ne peuvent être restaurées ou si la restauration ne fournit pas de données correctes.

Les grandes entreprises ne possèdent généralement pas un seul système de sauvegarde et restauration, mais plusieurs. On distingue trois catégories de sauvegardes, souvent dictées par les outils eux-mêmes.

- **Les sauvegardes complètes** : tout est sauvegardé en totalité. La restauration est ainsi aisée, car il n'y a aucune question à se poser. En revanche, la sauvegarde est longue et si les données ont peu évolué, la quantité de cassettes ou autre média s'accroît inutilement, car contenant de nombreuses données identiques d'une fois sur l'autre.
- **Les sauvegardes incrémentielles** : ne sont sauvegardées que les données qui ont changé par rapport à la sauvegarde précédente, la première sauvegarde étant complète. Cette méthode est rapide et peu consommatrice d'espace sur les bandes. Cependant, lors de la restauration des données, elle implique souvent de rechercher toute une série de bandes de sauvegardes diverses. À l'inverse de la précédente, cette méthode est donc efficace en sauvegarde mais difficile en restauration.
- **Les sauvegardes différentielles** : après une première sauvegarde complète, cette méthode ne sauvegarde que les données ayant été modifiées depuis la dernière sauvegarde complète. La restauration nécessite alors d'avoir seulement la dernière sauvegarde complète et la dernière sauvegarde différentielle. Envisagée en général fichier par fichier, cette méthode est un bon compromis : plus longue en sauvegarde que la sauvegarde incrémentielle, mais plus rapide en restauration.

Gérer les cassettes et autres supports

Les cassettes de sauvegarde ou autre média (disques optiques, DVD, etc.) nécessitent une gestion particulièrement soigneuse dans le cadre du plan de continuité. Les aspects suivants doivent être absolument pris en compte :

- Les cassettes doivent être entreposées dans un lieu sûr, à l'abri des risques qui pèsent sur les systèmes dont elles sont les sauvegardes.
- Les employés qui viendront récupérer les cassettes en cas de sinistre doivent pouvoir les trouver et les identifier facilement.
- Si certaines cassettes sont constituées en lots à manipuler ensemble, ceux-ci doivent être évidents (regroupés dans une mallette, par exemple).
- À l'inverse, il peut arriver que certaines cassettes ne doivent pas se trouver ensemble (sauvegardes de clients différents, par exemple, qui ne doivent absolument pas être mélangées) : cela doit être clairement identifiable.
- Dans les cas où des contraintes s'appliquent sur les lots de cassettes (confidentialité, urgence, destination particulière, etc.), celles-ci doivent être indiquées et faciles à comprendre par les personnes chargées de les récupérer.
- Il peut être intéressant d'indiquer une priorité de traitement ou de prise en compte, lorsque les lots de cassettes ne peuvent être déménagés en une seule fois. Celle-ci est basée alors sur les délais de restauration (par exemple : immédiat, moins de 4 heures, même jour, moins de 24 heures, de 24 à 72 heures, plus de 72 heures).
- Le moyen de transport peut être éventuellement indiqué sur les lots.
- Il est indispensable de tester régulièrement la lisibilité des cassettes et de copier à neuf celles qui vieillissent mal, avant qu'elles ne deviennent illisibles.
- Les cassettes devenues inutiles doivent être éliminées (ou recyclées).
- Les consignes des fabricants pour le stockage doivent être respectées absolument.

Un système de gestion informatique des sauvegardes peut être utile pour administrer tout cela.

> **Exemple : un oubli fâcheux**
>
> La société de service informatique SLBanque gère l'informatique de la Banque du Musée, en banlieue parisienne. Les systèmes de production (ordinateurs, stockage) sont situés dans un centre informatique proche du périphérique. Des sauvegardes sont effectuées régulièrement et, tous les lundis, des convoyeurs viennent prendre livraison de mallettes de cartouches à destination d'un centre d'entreposage en province proche.
>
> Un lundi, des travaux importants ont lieu au centre, nécessitant de désactiver en partie l'ouverture automatique des portes. Les convoyeurs effectuent malgré tout leur transfert habituel, et une fois partis, des livreurs arrivent avec du matériel d'un tout autre ordre. Après 45 minutes, la livraison est finie et l'on ferme enfin les portes à la main. C'est là qu'on aperçoit une mallette de cassettes oubliée, restée là pour caler une porte !

> Il n'a pas été possible de retrouver ou d'appeler les convoyeurs. Fort heureusement, le nom du client était indiqué sur la mallette et celui-ci, une fois averti, a prévenu qui de droit.
>
> **Et pourtant...** le client aurait-il constaté seul qu'il lui manquait une mallette ? Cette mésaventure a conduit par la suite la société SLBanque et ses clients à revoir leurs procédures de sortie des cassettes de sauvegarde.

Robots de sauvegarde

Les robots de sauvegarde sont des matériels périphériques qui servent à sauvegarder et restaurer les données sur un support en général amovible (cassette, cartouche…). Ils sont la plupart du temps partagés par différents environnements techniques et utilisés par de nombreux serveurs ou NAS. Leur constitution mécanique, comportant un grand nombre de pièces en mouvement, les rend fragiles et leur fiabilité dépend avant tout d'une bonne maintenance.

Le matériel avec lequel la sauvegarde est effectuée peut être différent de celui avec lequel la restauration sera réalisée : il suffit de ne pas se trouver sur le même site. Des précautions de compatibilité sont nécessaires, sous peine de ne pouvoir restaurer correctement.

Il existe des systèmes qui virtualisent les bandes et les dérouleurs de bandes : les VTS (*virtual tape servers* ou serveurs à bande virtuelle). Nombre d'opérations d'écriture et de lecture se font alors sur disques au lieu de se faire sur du matériel réel à bande. Toutefois, la sécurité des opérations de sauvegarde est garantie par la réalisation finale de cassettes de sauvegarde appropriées. Ces systèmes permettent ainsi d'éviter les créations inutiles de cassettes.

Tous ces systèmes proposent souvent d'autres fonctions en option, dont il faut tenir compte dans le cadre d'un plan de continuité. En effet, il faut être sûr de pouvoir restaurer :

- la compression des données – il faut pouvoir décompresser lors de la restauration ;
- le chiffrement – de la même manière, il faut pouvoir déchiffrer et avoir les droits techniques et administratifs pour le faire ;
- la déduplication (élimination de doublons pour gagner de l'espace), qui pose le même type de contraintes.

La capacité à effectuer une restauration correcte sur un système potentiellement différent du système de sauvegarde est fondamentale. Sans cela, en effet, toute sauvegarde est inutile. Parmi les points à considérer, on compte :

- la compatibilité des formats en tous genres (cassette, dérouleur, chargeur, codage, etc.) ;
- la compatibilité des logiciels, qui est une exigence très forte – dans presque tous les cas, on aura besoin pour la restauration du même logiciel que celui qui a servi pour la sauvegarde ;

- une bonne gestion des droits associés – l'administrateur qui charge une sauvegarde doit disposer des droits nécessaires, l'outil doit l'autoriser à opérer ;
- les performances – la restauration ne devant pas durer dix heures si l'on dispose d'un temps limité à quatre heures, les débits doivent être calculés correctement ;
- l'état des matériels de restauration, qui doit être vérifié et testé, avec des contrats de maintenance convenables ;
- l'existence et l'actualité des licences d'utilisation.

Tous ces aspects sont importants, surtout dans les cas où le logiciel et les moyens de restauration utilisés sur un site de secours ne sont pas ceux que ce site emploie pour son usage propre.

Les antivirus et anti-intrusion

La protection contre les virus informatiques et les intrusions malveillantes concerne le domaine de la sécurité. Toutefois, les divers systèmes qui permettent cette protection font partie des éléments critiques ou à considérer comme tels dans une approche de continuité. La protection étant à base d'éléments actifs (c'est-à-dire qui doivent fonctionner pour être efficaces), la perte de ces éléments expose la société à un risque et ne peut être admise longtemps.

Ainsi, les éléments de ces systèmes, tels les équilibreurs de charges, pare-feu, IDS (*Intrusion Detection Systems*) ou scanners divers, doivent être suffisamment pris en compte dans un plan de continuité. On doit porter la même attention aux systèmes de SSO (*Single Sign On*) sans lesquels l'utilisateur ne peut plus se connecter.

En cas de perte de ces systèmes, il doit être possible de reconstituer dans l'urgence des éléments équivalents, de la même manière qu'on le réalise pour des serveurs ou des éléments de stockage.

Ces systèmes résident tantôt dans le réseau, tantôt sur les serveurs et ne doivent pas échapper à la vigilance du RPCA qui devra se rapprocher du RSSI sur tous ces sujets.

Les réseaux du centre informatique

Le centre informatique dispose de plusieurs types de réseaux :

- le réseau assurant la connexion des terminaux et postes de travail aux serveurs ; le protocole IP y est omniprésent ;
- le réseau supportant les échanges des serveurs entre eux, avec plusieurs vitesses et débits possibles : si des protocoles de grappe existent encore, IP à haute vitesse se généralise et on assiste à l'émergence de technologies nouvelles comme Infiniband ;

- le réseau de stockage SAN (*Storage Area Network*), qui connecte le stockage en groupes aux divers serveurs.

Pour optimiser les débits, réduire les risques et isoler les perturbations, ces différents réseaux peuvent être cloisonnés et recourir à des protocoles divers. Ils peuvent aussi, pour des raisons d'efficacité, partager des artères rapides. Les câblages sont de natures différentes, même si la fibre optique se généralise.

En général, on fait encore la distinction entre SAN et réseau traditionnel.

Réseau de stockage SAN

Le SAN (*Storage Area Network*) est un réseau qui assure la connexion entre des contrôleurs de stockage, des unités de disques diverses et des serveurs. On le trouve principalement en salle informatique, dont il ne sort que pour assurer une liaison avec un site secondaire très proche.

La principale technologie réseau du SAN est la technologie d'interconnexion appelée *Fibre Channel* (FC), qui opère principalement – mais pas seulement – sur fibre optique à courtes distances.

La liaison avec le troisième site distant, s'il existe, nécessitera une autre technologie et un couplage avec des routeurs spéciaux.

De nouvelles techniques normalisées apparaissent, tels les protocoles iSCSI (*Internet Small Computer System Interface*), appelé aussi SCSI sur IP, qui consiste à transmettre les commandes et données dans des paquets IP, ou encore FCoE (*Fibre Channel over Ethernet*) qui permet d'utiliser les protocoles de type *Fibre Channel* sur un lien 10 gigabits Ethernet à haute vitesse. Elles rapprochent le SAN des techniques de réseau traditionnel.

Comme tout réseau, le SAN utilise des routeurs et des commutateurs plus ou moins puissants et évolués.

En ce qui concerne le SAN, la fiabilité et la disponibilité méritent la plus grande attention : un SAN en panne, même partiellement, peut paralyser une salle informatique entière, dans le cas où les serveurs principaux ne peuvent plus accéder à leur stockage.

Réseau traditionnel

Concernant le réseau traditionnel, l'analyse et les mesures à prendre ressemblent beaucoup à celles ayant trait aux serveurs. On y retrouve en effet les mêmes orientations et architectures :

- la segmentation ou répartition sur des éléments en grappes de type n+1, avec de petites machines simples dédiées à une tâche particulière (pare-feu, antivirus, détecteurs divers, etc.) ;
- la consolidation (monolithique) sur des équipements très puissants, uniques et donc à tolérance de panne ;
- la virtualisation, qui permet à une même machine d'abriter des fonctions multiples ;

- la redondance qui, associée à une virtualisation simple, permet d'abriter deux machines virtuelles dans une même machine physique et d'en arrêter une sans interrompre l'autre.

Les évolutions du réseau sont par ailleurs dictées par les évolutions des serveurs : si l'on consolide dix serveurs pour n'en faire qu'un seul, le réseau qui les reliait change de nature de même que sa vulnérabilité aux pannes. Les deux approches doivent être associées pour obtenir une configuration à haute disponibilité.

Performance et fiabilité des réseaux

Quel que soit le type de réseau, il est indispensable de porter un regard attentif et critique sur les points suivants :

- la possibilité pour des matériels de constructeurs différents de travailler ensemble ; en effet, le respect des protocoles n'est souvent pas suffisant et il faut également étudier les comportements de matériel en présence d'anomalies ou de pannes partielles – ce comportement doit être cohérent d'une machine à l'autre ;
- la tolérance aux pannes des éléments centraux qui constituent des points uniques de défaillance, tels que les commutateurs directeurs ;
- la possibilité ou non de diversifier les chemins d'accès entre l'origine et la destination, afin de se prémunir d'une panne sur un chemin ;
- la souplesse de passage d'un chemin à un autre en cas de panne du premier : est-ce automatique ou manuel ? Peut-on utiliser deux voies en parallèle ou de manière alternée ?
- le comportement des matériels en cas de redémarrage suite à divers types d'interruption, qui doit être cohérent et rétablir un état du réseau acceptable ;
- la conservation des changements de paramètres dynamiques, afin d'éviter, en cas de redémarrage, de faire une restauration sur un état antérieur incorrect.

Construire un réseau performant, c'est aussi construire un réseau fiable. Là encore, les pannes de mode commun ne doivent pas être négligées dans l'évaluation de la fiabilité (voir le chapitre 7).

Chapitre 9

Infrastructure et poste de travail de l'employé

Tout ce qui a trait à l'environnement de travail de l'employé – téléphonie, poste de travail en réseau, bureau – doit être étudié soigneusement. Ces éléments, utilisant des technologies de plus en plus avancées, sont en effet des points vulnérables mais indispensables à la continuité de l'entreprise.

Ceci inclut dans une certaine mesure les problématiques liées aux ressources humaines, bien que ce sujet soit à la limite du périmètre de cet ouvrage. Le cas de la pandémie, qui nécessite une approche spécifique, est traité au chapitre 11.

Les réseaux

L'analyse de la disponibilité du réseau se révèle toujours compliquée, parce qu'un réseau n'est pas un « objet technique » comme les autres. En effet, ce n'est pas parce que les routeurs ou commutateurs fonctionnent que le réseau est disponible. Le bon fonctionnement d'un réseau implique en général deux acteurs – chacun à une extrémité – avec la plupart du temps un opérateur entre les deux. C'est un jeu à trois. Quant aux cas où le réseau fonctionne mal, il n'est pas toujours aisé d'en déterminer les causes. La vision de son état de fonctionnement peut d'ailleurs être différente selon l'endroit d'où on l'observe.

Par ailleurs, lorsque seul le réseau ne fonctionne pas dans une entreprise, les techniciens les plus avancés se retrouvent désemparés : aucune machine à réparer. Tout au plus peut-on essayer de basculer vers un autre réseau ou un autre opérateur en espérant que celui-ci ne sera pas victime de la même avarie.

Réseau téléphonique

En dépit de la montée en puissance des nouvelles technologies, le téléphone joue encore un rôle primordial dans la vie de l'entreprise, comme l'illustre l'exemple suivant.

Exemple : l'acheteur et le téléphone

M. Achat est acheteur chez un fabricant qui dépend fortement de ses fournisseurs en termes de délais. Un soir, de retour à son domicile, il voit au journal télévisé régional qu'un incendie s'est déclaré chez son principal fournisseur. La télévision montre des flammes et le commentaire est imprécis. Souhaitant avoir plus d'information, M. Achat essaie d'appeler le site sinistré : impossible. Le site est trop éloigné pour qu'il s'y rende en voiture.

Le lendemain matin, il cherche à joindre son commercial attitré chez le fournisseur – en vain. Par précaution, il passe commande chez un autre fournisseur, pratiquant des prix très élevés, sacrifiant ainsi à la sécurité.

Trois jours après, M. Achat apprend que le sinistre ne concernait ni l'usine ni les stocks de son fournisseur, mais uniquement des bureaux et la salle de l'autocommutateur.

Moralité :
– il peut être utile de disposer du numéro de portable de son commercial ;
– en cas d'incendie, il faut essayer dans la mesure du possible de transmettre à la télévision des informations précises, en espérant qu'elles passeront à l'antenne... ;
– la société sinistrée doit prévoir un accueil téléphonique de ses clients, dans des cas semblables de sinistre : son opérateur doit avoir des solutions.

Les réseaux téléphoniques n'ont pas été conçus en prévision que tout le monde appelle tout le monde au même moment (plus exactement, qu'une moitié des abonnés appelle l'autre moitié). Ils sont dimensionnés pour permettre le trafic de quelques pourcents d'une zone donnée (on cite souvent le chiffre de 10 % en Amérique du Nord). Cela est valable aussi bien pour la téléphonie fixe que pour la téléphonie mobile. Ainsi, en cas de sinistre régional, ou simplement d'incident ou événement attirant la curiosité générale, il est impossible de compter sur un acheminement sûr des appels.

Vu de l'utilisateur en entreprise, le réseau téléphonique peut être décomposé en trois parties, dont chacune mérite l'attention :

- les cheminements internes à l'entreprise, courant dans des goulottes, avec des connexions situées dans des répartiteurs ou armoires qu'il faut vérifier ;
- le cheminement hors de l'entreprise, dirigé vers les moyens techniques de l'opérateur (central téléphonique) en passant par la voie publique et ses aléas ;
- l'autocommutateur de l'entreprise, qui est une machine s'apparentant désormais à un ordinateur, avec sa redondance interne, sa maintenance, ses mises à niveaux et ses techniciens.

Câblage interne

Concernant le câblage interne et les armoires de répartition, il faut s'assurer que :

- les cabinets de passage des câbles sont fermés à clé ;
- les répartiteurs et sous-répartiteurs sont équipés en systèmes anti-incendie (extincteurs automatiques appropriés) ;

- rien d'autre n'est stocké sur place (si ce n'est de la mort au rats… mais pas les guirlandes de Noël !) ;
- les clés sont en possession des personnes habilitées et d'elles seules ;
- l'éclairage est suffisant dans les cabinets ;
- la séparation avec le réseau informatique, qui utilise souvent les mêmes installations, est faite correctement – en effet, ce dernier peut dégager de la chaleur car il est actif ;
- l'accès aux goulottes y est suffisamment restreint.

Le cheminement du câblage doit être connu et documenté, les entrées dans les locaux et « têtes télécom » (points d'arrivée des fils) localisées sur un plan du bâtiment.

Câbles extérieurs

Les câbles externes ne dépendent pour l'essentiel pas de la société, mais de l'opérateur télécom. C'est souvent le point faible de la chaîne qui relie l'autocom de l'entreprise au central de l'opérateur ou à divers POP (points de présence). Il faut donc surveiller certains aspects, même s'ils ne sont généralement pas du ressort de l'entreprise :

- les tempêtes, la glace ou la neige peuvent endommager les lignes aériennes : une inspection sur place permet au moins de comprendre le risque ;
- les accidents de véhicules contre des poteaux téléphoniques peuvent eux aussi affecter les lignes ;
- les lignes enterrées sont soumises aux aléas des travaux publics (voir page 280 l'anecdote du pont de Suresnes).

L'entreprise peut demander ou l'opérateur téléphonique proposer des cheminements séparés. Il faut alors étudier par où les câbles passent et comment effectuer la séparation : quelle distance y a-t-il entre les câbles, quels sont les points de regroupement, comment se font les passages de rivières, etc. ?

> **Tempêtes et dépendances**
>
> Les récentes tempêtes Klaus (en 2009) et Xynthia (en 2010) ont pointé la vulnérabilité des réseaux.
>
> – Les opérateurs de téléphonie fixe utilisent principalement des commutateurs et des dispositifs de connexion de la boucle locale (dits « NRA ») dotés de batteries de secours. Malheureusement, des pannes de courant de longue durée (plus de 48 heures) en sont venues à bout, privant de téléphone bon nombre d'usagers. Le même constat a pu être fait sur divers éléments d'opération de la téléphonie mobile.
>
> – Les usagers en mode ADSL, dotés de « box » alimentées par le courant électrique, ont évidemment été privés de téléphone lorsque le courant de leur domicile a été coupé.
>
> – Plus généralement, les réseaux de distribution d'eau et d'assainissement sont eux aussi tributaires de l'électricité, car ils nécessitent des pompes. Si les coupures de courant sont trop longues, les éventuelles batteries sont là encore épuisées.

> **Moralité** : sans précaution, une coupure de courant finit par priver les usagers de téléphone fixe et mobile et d'eau…

Le fait de passer par un deuxième opérateur n'est pas une garantie, car ce dernier peut fort bien emprunter une ligne louée auprès du premier opérateur. Il peut donc être utile de se renseigner sur tous ces points et, pourquoi pas, de parcourir en voiture le trajet emprunté par les câbles.

Quant aux opérateurs mobiles, ils encourent des problèmes du même ordre, à ceci près que certaines portions de câblage sont remplacées par des ondes hertziennes dont la fiabilité va dépendre des pylônes, des antennes, des émetteurs et d'autres matériels informatiques. La téléphonie mobile est également sensible aux intempéries, des vents forts pouvant, par exemple, endommager les antennes.

Autocommutateur

L'autocommutateur accueille les lignes téléphoniques externes et distribue les appels sur d'autres liens internes. Associés à l'autocommutateur, on trouve souvent d'autres matériels tels que des serveurs interactifs de réponse vocale, des boîtes vocales, des répondeurs, des systèmes de routage d'appels, des moyens de conférence, etc.

Il faut alors procéder comme pour une petite salle informatique, en vérifiant les points suivants :

- la liste des équipements, avec descriptions et numéros de série ;
- les contacts et numéros du service de maintenance, en cas de panne ;
- les sauvegardes qui doivent avoir été faites et leur lieu de conservation ;
- des éléments tels que les alimentations électriques secourues, les alarmes en cas de dépassements de température ou de taux d'humidité ;
- la sécurité d'accès : les clés du local de l'autocom (fermé à clé) doivent être en possession de quelques personnes responsables identifiées ;
- les systèmes anti-incendie : ceux-ci doivent être prévus et leurs tests avoir été exécutés et notés.

La similitude avec la salle informatique ne s'arrête pas là : il est en effet possible de louer un autocom de secours qui peut être amené dans un conteneur et connecté au réseau de l'entreprise. Ce type de contrat peut avoir été prévu en secours (voir le chapitre 3).

La similitude avec les pratiques des informaticiens est cependant faible, la téléphonie restant un monde à part.

Réseau informatique

Le réseau informatique du lieu de travail se décompose lui aussi en trois parties, qui présentent une analogie forte avec la téléphonie :

- le réseau local (LAN – *Local Area Network*), proche du poste de travail des employés ;
- des matériels de commutation ou de routage, des contrôleurs de réseau, des serveurs bureautiques ou d'impression, des imprimantes départementales, situés en général dans de petites salles ou des sites appropriés dans les locaux ;
- le réseau externe à l'entreprise, pour lequel les commentaires sont les mêmes que précédemment pour la téléphonie.

Le réseau fédérateur (*backbone*) de l'entreprise, présent en salle informatique, est traité dans le chapitre 8.

Réseau local (LAN)

Le *Local Area Network* (LAN) est le réseau interne aux bureaux qui connecte les postes de travail aux divers équipements utiles.

Comme on l'a vu plus haut, une partie du câblage du réseau interne à l'entreprise, de même que certains moyens de répartition, est souvent très voisine physiquement de la téléphonie. Les mêmes remarques s'appliquent donc en ce qui concerne les goulottes, les cabinets de répartiteurs, etc.

L'apparition de la téléphonie sur IP transforme le téléphone en véritable terminal Internet branché sur le LAN. Ce téléphone a toutefois besoin d'une alimentation électrique qui est souvent fournie par le LAN lui-même, moyennant des aménagements. Cela ajoute un risque dont il faut tenir compte dans les armoires de câbles.

En règle générale, il faut contrôler :

- les cheminements des câbles et leur protection ;
- les installations de répartiteurs, ou sous-répartiteurs, avec des documents à jour, des plans clairs, des terminaisons identifiées ;
- les salles ou placards utilisés, qui doivent être fermés à clé, les clés étant disponibles auprès de personnes clairement identifiées ;
- les moyens anti-incendie, inspectés régulièrement avec une preuve de l'inspection.

Serveurs bureautiques

Les serveurs bureautiques complètent le poste de travail (PC) de l'utilisateur et conservent des documents (fichiers Word, Excel, OpenOffice.org, etc.), permettant de fournir du stockage local ainsi que des moyens d'impression et de messagerie, par exemple. Leur défaillance empêche, entre autres, l'accès des utilisateurs à leurs documents, l'échange de messages et l'impression. Ces serveurs sont considérés de plus en plus souvent comme critiques par les entreprises.

La pratique qui consistait à installer ces serveurs bureautiques près des photocopieuses ou des machines à café a vécu. Les grandes orientations actuelles consistent à déplacer et consolider ces serveurs, en fonction de leur mission :

- sur des NAS (voir le chapitre 8), pour les serveurs de fichiers, souvent déplacés dans un centre informatique ;
- sur de gros serveurs de messagerie (en grappe ou redondance), situés en général dans un centre informatique ;
- sur de petits serveurs dédiés aux impressions avec une imprimante locale, départementale ou multifonction proche des utilisateurs.

Au vu de ces évolutions, les serveurs bureautiques rejoignent les serveurs de stockage associés au centre informatique. Ils bénéficient alors de toute l'infrastructure et des systèmes de sauvegarde du centre.

Si l'entreprise utilise encore des serveurs bureautiques délocalisés, il faut alors :

- identifier les administrateurs et les responsables ;
- s'assurer qu'il n'y a pas de surchauffe ou d'anomalies d'environnement (vibrations, humidité hors norme) ;
- s'il y a des sauvegardes, s'assurer qu'elles sont bien réalisées et entreposées en lieu sûr ;
- s'il y a des imprimantes, limiter la quantité de papier entreposée près des machines, qui constitue un risque supplémentaire d'incendie.

Le poste de travail

Le poste de travail de type PC a une importance variable dans l'informatique générale de l'entreprise. Historiquement, l'informatique est apparue bien avant le PC et utilisait des terminaux passifs. Les premiers PC ne servaient qu'à la bureautique et leur connexion en réseau entre eux et aux serveurs ne s'est faite que progressivement. Aujourd'hui, l'utilisateur ne connaît plus l'informatique que par son PC.

Une importance variable

Au sein de l'entreprise, plusieurs usages du PC cohabitent à des degrés divers.

- Avec les architectures dites « client-serveur », le PC a acquis une importance nouvelle : il devient dépositaire d'une partie des applications de l'entreprise, dont certaines sont critiques.
- Le PC est toujours la base des applications bureautiques (traitement de texte, tableur) qui sont de plus en plus intégrées dans le système d'information de l'entreprise.
- Le PC est très souvent aussi un « client lourd » de messagerie, dépositaire de la boîte aux lettres de son utilisateur.

- Il est quelquefois utilisé en tant que client léger ou simple navigateur web, auquel cas il peut être remplacé par des terminaux légers.
- Les données qu'il manipule sont présentes soit sur son disque dur, soit sur un serveur de fichiers local de l'entreprise (voir NAS ou serveur de fichiers dans le chapitre 8), soit sur un serveur central au centre informatique.

Le PC est donc dépositaire d'une partie plus ou moins importante des données vitales de l'entreprise. Même si cette part est actuellement en diminution, car on préfère centraliser le stockage sur des moyens plus sûrs, on ne peut pour autant l'ignorer.

Par ailleurs, en tant que poste de travail commun, les accès aux serveurs et applications centralisés de l'entreprise passent par le PC, sa perte empêchant donc tout travail sur l'informatique.

Enfin, certains utilisateurs créent, modifient et suppriment sur leur PC des données vitales pour l'entreprise. Cette pratique quelque peu dangereuse existe par exemple dans certains services financiers où des données ainsi gérées sont injectées dans des outils de reporting comptable. Ces données présentent un risque (pas uniquement en termes de continuité, d'ailleurs) qu'il faut identifier. On les appelle « données utilisateurs » (*user data*).

Se prémunir contre la perte du PC revient donc à protéger des données, protéger des applications et permettre de continuer à travailler malgré tout.

Protection des données

Trois niveaux de protection sont généralement pratiqués en ce qui concerne les données manipulées sur PC .

1. **Aucune protection** : si le PC est détruit ou si le disque dur est hors service, la donnée est détruite ou plus exactement perdue.
2. **Protection locale** : l'utilisateur dispose d'un graveur de DVD, d'un enregistreur sur cassette ; les données qu'il veut conserver sont ainsi sauvegardées localement.
3. **Protection par le réseau** : les données du PC sont conservées sur un serveur NAS ou autre, où les sauvegardes sont organisées.

En matière de continuité d'activité, il est important pour l'entreprise de s'assurer que les sauvegardes sont effectuées convenablement. Si ce n'est pas le cas, il faut modifier la manière de faire en généralisant la protection par le réseau (cas n° 3).

> **Nouveauté : les offres en « cloud »**
>
> Depuis peu se sont développées des offres de stockage accessibles aisément sur Internet, qualifiées de « stockage en *cloud* » (d'après le terme anglais *cloud computing*, qui désigne la mise à disposition de moyens informatiques divers accessibles par le réseau Internet – en français, on entendra parfois parler « d'informatique dans les nuages »...).
>
> Certaines solutions proposées permettent de sauvegarder quasi en permanence tout ce qui se passe sur le disque dur de l'ordinateur de l'usager. Ainsi, tous les documents résí-

> dant sur le disque dur sont aussi copiés et tenus à jour dans le *cloud*. Si l'usager perd son PC ou voit son disque dur détérioré, il peut très aisément, à partir d'un navigateur web, aller chercher ses données sur Internet. On peut dire ainsi que le *cloud* fait partie du plan de continuité de l'usager...
>
> Ces offres, encore balbutiantes, se cherchent en terme de tarif et de niveau de sécurité. Il est clair que c'est ce dernier point qui cristallise les réticences.

Protection des applications

Pour les applications utilisées sur PC, le même schéma se retrouve à quelques détails près.

1. **Aucune protection** : en cas de perte, l'application n'est a priori pas récupérable.
2. **Protection locale** : le CD d'installation a été conservé et on peut réinstaller localement l'application perdue.
3. **Protection par le réseau** : en cas de perte, l'application peut être téléchargée et réinstallée à partir d'un lieu de conservation central.

Il est clair que les pratiques sont à étudier pour vérifier que les applications vitales de l'entreprise se trouvent bien dans le dernier cas (sur le réseau). Une amélioration des pratiques est à envisager sérieusement si ce n'est pas le cas.

Certaines entreprises limitent la protection locale (cas n° 2) au strict minimum, voire l'interdisent, cette pratique de « bricolage » local étant jugée dangereuse. Certains outils sont capables, à partir du réseau, de détecter des applications installées localement et de les désactiver après avoir averti un administrateur.

Comment continuer à travailler ?

Pour pouvoir continuer à travailler en cas de sinistre, l'utilisateur aura besoin de récupérer ses données et ses applications locales. Cela est réalisable dans les cas suivants :

- lorsque celles-ci sont accessibles via le réseau (cas n° 3 ci-dessus) et que le réseau est en état ;
- lorsque celles-ci sont récupérables via un support correctement conservé – même si le contexte est plus difficile et aléatoire ;
- lorsqu'aucune donnée ou application n'est conservée en local (cas du terminal léger) : l'utilisateur n'a alors besoin que de se connecter au serveur.

Tout dépendra donc de la disponibilité du réseau et des accès aux serveurs.

D'autre part, l'utilisateur a besoin de récupérer son outil de travail : un PC similaire à celui qu'il a perdu, ou bien un terminal léger. Il faut donc conserver un stock de PC prêts à l'usage et assez voisins des PC qu'ils remplacent. Ce type de stock est assez souvent prévu dans les contrats de maintenance améliorée, où il s'agit de remplacer un PC en panne dans un délai rapide que la maintenance standard ne permet pas d'obtenir. Il faut alors bien vérifier que le cas du sinistre