CONSERVER LES COURRIERS ELECTRONIQUES ?
Ou comment résoudre la problématique de l'archivage des e-mails

Philippe BALLET
Jean-Marc RIETSCH

FedISA
Fédération
ILM, Stockage & Archivage

Les Auteurs

Jean-Marc Rietsch

Pilote de l'ouvrage, Jean-Marc Rietsch (jm.rietsch@fedisa.eu) est expert des métiers de la confiance et plus particulièrement de l'archivage électronique. Ingénieur Civil des Mines, Jean-Marc Rietsch a débuté sa carrière professionnelle par le développement logiciel et l'offre de services pour les PME-PMI. En 1993, il oriente sa carrière vers la sécurité et plus particulièrement la sauvegarde des données informatiques et dépose un brevet sur le sujet. En 2001, Jean-Marc Rietsch participe au lancement du premier tiers archiveur en France. Jean-Marc Rietsch est Président de FedISA (Fédération de l'ILM du Stockage et l'Archivage, www.fedisa.eu), créée en 2005 et destinée à répondre aux attentes des utilisateurs dans le domaine. Il est également le fondateur de Demateus (www.demateus.com), organisme spécialisé dans la formation sur le domaine et à l'origine d'un premier master concernant « le management de la dématérialisation et de l'archivage électronique » en collaboration avec les Grandes Ecoles.

Philippe Ballet

Philippe Ballet (philippe-ballet@alain-bensoussan.com), Avocat au Barreau de Paris, a débuté sa carrière professionnelle au sein d'une PME en charge du lancement d'un département de sécurité informatique. Il s'est naturellement rapproché de l'AFNOR, en tant qu'expert, pour l'élaboration d'une norme européenne sur les armoires ignifuges pour supports informatiques. Il a ensuite rejoint l'AFNOR comme chargé de mission pour les affaires commerciales et juridiques internationales, où il a suivi les travaux de normalisation liés à la « société de l'information » et, notamment, l'archivage électronique. Il a rejoint ensuite, en tant que directeur juridique, FranceNet, pionnier de l'accès internet en France, devenue Fluxus, puis BT France après son rachat par British Telecommunications Plc. En 2006, il rejoint le Cabinet Alain Bensoussan (www.alain-bensoussan.com) et dirige le Département Internet. Il intervient auprès de nombreux clients, du secteur public ou privé, dans le cadre d'audits de systèmes d'archivage électronique, de déploiement de procédés de signature électronique, d'externalisation des archives ainsi qu'auprès de prestataires de services de certification électronique.

Ont également contribué à ce document

Cyril Van Agt

Avant d'intégrer la société NetApp (www.netapp.fr) où il occupe actuellement le poste de responsable Avant-ventes Grands Comptes, Cyril Van Agt (cvanagt@netapp.com) a été Consultant entre 1999 et 2000 chez Ixos Software (aujourd'hui Open Text), années pendant lesquelles il a mené divers projets d'archivage électronique en environnement SAP notamment. De 1994 à 1999, Cyril a occupé chez Oracle France les fonctions de Consultant au département des Projets Avancés puis d'Avant-vente au Centre d'Expertise en Network Computing. Cyril Van Agt est diplômé de l'ISEN de Lille (ingénieur), possède un DEA Ultrasons (Valenciennes) et enfin possède un Master en Imagerie de l'ENST de Paris.

Laurent Delaisse

Avec plus d'une dizaine d'années d'expérience chez les constructeurs et éditeurs de logiciel autour de la disponibilité de la données (Sauvegarde/Restauration, Archivage, Solution de gestion du stockage, Disponibilité applicative, Reprise d'activité), Laurent Delaisse (laurent_delaisse@symantec.com) travaille actuellement pour la société Symantec (www.symantec.com) en tant que responsable Avant Ventes Alliances et Solutions Spécialiste.

Sommaire

Préface

L'archivage électronique est de plus en plus un véritables sujet d'actualité pour l'ensemble des organisations tant publiques que privées. Cette nouvelle source de préoccupation pour les entreprises trouve son origine à plusieurs niveaux :

- l'augmentation extrêmement forte du volume de données électroniques gérées au quotidien du fait principalement des évolutions technologiques
- les changements dans les processus d'entreprise, essentiellement en matière de dématérialisation
- de nouvelles obligations tant légales que réglementaires.

Cependant il ne faut surtout pas considérer la problématique de l'archivage électronique comme relevant de la simple dématérialisation des techniques traditionnelles d'archivage. Outre l'influence des nouvelles obligations, essentiellement légales, ce nouveau type d'archivage doit être pris en compte très en amont, dès l'instant où les données peuvent être considérées comme figées. C'est donc l'ensemble du cycle de vie de l'information qu'il va falloir prendre en compte, de la création de la donnée jusqu'à sa destruction, pour réaliser la mise en place d'un système d'archivage électronique efficient.

Par ailleurs le paradoxe de l'archivage électronique consiste à devoir travailler avec des technologies à l'obsolescence extrêmement rapide pour conserver des données sur du moyen, long terme voire ad vitam aeternam. Cette prise de conscience ne fait que révéler la dissociation indispensable qu'il y a lieu de faire au niveau d'un document entre le support et son contenu informationnel. Jusque là le papier permettait de s'affranchir de cette différence dans la mesure où il est bien difficile de dissocier le texte de la feuille sur lequel il se trouve. Par contre en électronique il est indispensable de faire cette différence et de s'intéresser essentiellement au contenu informationnel. De par ce simple raisonnement on s'aperçoit dès lors que le support devient secondaire dans la problématique d'archivage puisqu'il constitue seulement un moyen de parvenir à conserver ce précieux contenu informationnel.

La notion même d'archivage a changé dans la mesure où il faut totalement balayer cette vision ancienne, pourtant bien ancrée dans les esprits, de l'archive conservée dans des cartons poussiéreux. Du fait de la dématérialisation, l'information reste facilement accessible et doit le rester tout au long de son cycle de vie. Cela veut dire que même rendue au statut d'archive la donnée doit être accessible facilement, voire disponible en ligne.

Ainsi l'accès à l'information constitue incontestablement une nouvelle richesse pour toute organisation sous réserve qu'elle soit fiable et puisse ainsi être transformée en connaissance utile. Au sens électronique du terme, l'archivage peut ainsi offrir une véritable mise à disposition d'informations autrefois oubliées, voire perdues du fait de leur difficulté d'accès. Une des conséquences de l'archivage électronique est ainsi de pouvoir renforcer le système d'information de l'entreprise ou de toute organisation et par là même sa compétitivité en permettant de disposer de la bonne information au bon moment.

Enfin au delà de la technique il est également indispensable de considérer d'autres aspects très différents comme les aspects juridiques, organisationnels ou normatifs sans oublier la notion de risque propre à tout projet et un minimum de communication et de conduite du changement. Sans être compliqué cet environnement devient néanmoins vite complexe. D'où la nécessité de pouvoir effectivement sensibiliser, informer voire impliquer l'ensemble des utilisateurs potentiellement concernés.

Il s'agit là d'une des principales missions que FedISA s'est fixée sachant que le présent document fait suite à une série d'ouvrages déjà écrits sur ce thème avec ce même objectif, à savoir :

- L'archivage électronique à l'usage du dirigeant (Marie-Anne Chabin, Eric Caprioli, Jean-Marc Rietsch), adapté ensuite à la législation monégasque
- Dématérialisation et archivage électronique (Marie-Anne Chabin, Eric Caprioli, Jean-Marc Rietsch), édité chez Dunod
- Protection du patrimoine informationnel (Eric Caprioli, Paul de Kervasdoué, Jean-François Pépin, Jean-Marc Rietsch) tente de montrer que finalement la sécurité informatique, l'archivage et l'intelligence économique œuvrent dans le même sens, à savoir protéger le patrimoine de l'entreprise au sens de l'information

- L'archivage électronique en milieu hospitalier avec la participation d'Isabelle Renard constitue l'adaptation du premier ouvrage au monde médical.

L'archivage électronique, un mal nécessaire ? Absolument pas, il doit être pris comme un moyen particulièrement efficace destiné à gagner en performance et ce pour toute organisation publique ou privée quelle que soit sa taille. Les processus liés à l'archivage électronique permettent en effet un accès simplifié à une plus grande quantité d'information, totalement impossible par le passé. Au prix d'une nouvelle organisation, l'archivage électronique ne doit pas être vu comme une « simple » dématérialisation de l'archivage traditionnel, parlons plutôt d'archivage actif ou encore dynamique permettant l'accès à la bonne information et au bon moment.

Espérons que le présent ouvrage permettra au plus grand nombre de partager cet avis mais surtout d'être éclairé lorsqu'il se trouve ou se trouvera confronté à la problématique de conservation du mail.

Jean-Marc Rietsch
Président de FedISA

Introduction

Le phénomène du mail est à la fois très particulier et très représentatif de l'évolution technologique et de ses conséquences, bonnes ou mauvaises. Arrivé il y a un peu plus de dix ans, il est aujourd'hui largement répandu tant en usage professionnel que privé alors que rien ne le règlemente réellement, surtout au niveau de ce que l'on pourrait qualifier de « bon usage ». En effet chacun réagit en fonction de ses propres ressentis quant à la façon de rédiger un mail, de l'utilisation ou non de pièces jointes et des personnes à mettre en copie, simple ou cachée.

Le résultat en est une totale anarchie de fonctionnement et une augmentation gigantesque de la volumétrie à archiver que l'on nous prédit à plus de 7000 Po dès 2010 (source Gartner). Rappelons tout de même que d'un point de vue plus représentatif : 100 mégaoctets (Mo) représentent le contenu d'une pile de livres de 1 mètre de haut, 2 téraoctets (To 10^{12} octets) correspondent à tous les ouvrages d'une bibliothèque universitaire et 2 pétaoctets (Po) aux fonds de toutes les bibliothèques universitaires des Etats-Unis !

Face à cette augmentation de la volumétrie le réflexe a souvent été de l'équilibrer avec la baisse rapide des prix du stockage, même si au final le budget stockage augmentait. Or nous atteignons actuellement de tels niveaux que cette baisse n'est plus suffisante pour garantir une sorte de stabilité du budget alors même que la grande majorité des entreprises impose sa diminution. Par ailleurs la solution au problème de stockage ne répond pas pour autant à la capacité à retrouver de l'information parmi de tels volumes. Enfin pour les e-mails, il est triste de constater que malheureusement, la majorité des services informatiques, brident leurs utilisateurs en leurs imposant une taille limitée de boîte aux lettres alors même que des solutions beaucoup plus efficaces et surtout rationnelles existent que nous décrirons au cours de ce document.

Cette notion de rationalisation des espaces de stockage est essentielle en tant que véritable solution à cette problématique d'augmentation de volumétrie. On la retrouve à différents niveaux :

- Migration vers du stockage secondaire plutôt que d'exploiter du support, certes performant mais onéreux, pour des données qui ne le nécessitent pas ou plus
- Archivage au sens électronique, à savoir isoler les données figées afin de pouvoir les gérer comme archives. Le mail en représente le parfait exemple dans la mesure où il est figé dès sa création. Ce type d'organisation diminue de façon drastique (jusqu'à plus de 60%) les volumes nécessaires entre autres de sauvegarde
- Suppression des données après la durée de conservation requise, application d'une véritable politique correspondante.
- Gestion du taux d'occupation réel des baies de stockage afin de bien utiliser ce dont on dispose

Au-delà de ces aspects plutôt curatifs il est également nécessaire de pouvoir jouer sur la possible diminution des flux et des données en entrée des systèmes. Ainsi en est-il du mail dont l'usage devrait absolument être mieux organisé afin d'éviter des duplications d'information totalement inutiles et aux conséquences dramatiques : volumes qui explosent, e-mails non traités par manque de temps, information perdue car impossible à retrouver, … Précisons toutefois que malgré son importance, cet aspect préventif du bon usage du mail ne sera pas abordé dans le présent document.

Outre le vecteur de communication, le mail constitue également un support de plus en plus essentiel des relations avec ses fournisseurs et ses clients sans oublier l'outil de marketing. On est ainsi amené à lui faire jouer un rôle de plus en plus central et à devoir le considérer comme une application critique. Le Gartner estime que, en dehors des applications métier, 50% à 75% de l'information utile dans l'entreprise est échangé de personne à personne d'où l'accent sur la valeur juridique du mail et ses implications.

Rappelons enfin que la mise en place d'un système d'archivage des e-mails doit simplifier la gestion des e-mails au quotidien et leur conservation dans le temps, tant du point de vue de l'utilisateur, que du directeur informatique, du chef d'entreprise et ce tout en respectant les aspects légaux et réglementaires :

- Côté utilisateur, il y a l'exigence d'un confort maximum à pouvoir retrouver ses e-mails facilement sans pour autant être systématiquement obligé de les organiser par dossier et autre sous dossier. Cette classification montre d'ailleurs très vite ses limites lorsqu'un

mail peut être rattaché à deux dossiers différents ;

- Côté directeur informatique, les e-mails représentent vite un véritable cauchemar compte tenu de l'évolution à la fois de leur nombre et de leur volume moyen. La solution la plus souvent mise en place consiste à limiter radicalement la taille des boîtes de chaque utilisateur. La solution mise en place doit permettre de maîtriser la volumétrie sans contraintes pour l'utilisateur. Il faudra si possible être capable d'éliminer les e-mails qui ne justifient pas d'être conservés mais toutefois avec la certitude de ne pas éliminer des e-mails potentiellement utiles.
- Côté chef d'entreprise, il s'agit d'avoir la garantie de ne pas perdre d'information stratégique ou non, qu'il s'agisse d'un aspect commercial, technique, comptable ou financier voire patrimonial. Cette garantie de conservation est aujourd'hui essentiellement dictée par des obligations légales et réglementaires sachant que de plus en plus de contraintes naissent en la matière, généralement dictée par un souci d'historisation et de traçabilité de l'ensemble des opérations au sein de l'entreprise. Cette conservation devra se faire dans le respect des règles pesant également sur les données à caractère personnel.

Comme évoqué précédemment, le mail représente à lui tout seul l'ensemble des problématiques rencontrées pour tout système d'archivage électronique. L'archivage des e-mails pose ainsi des problèmes techniques dus au fait que l'on a à gérer un grand nombre d'items pour un volume donné (à l'extrême, les index d'un mail vont occuper plus de place que le mail lui-même). On doit également largement prendre en compte les aspects juridiques et réglementaires comme la conservation de la trace des échanges, sans parler des pièces jointes ou encore le respect des données à caractère personnel selon les exigences de la CNIL.

Contrairement à un archivage traditionnel, les exigences de l'archivage électronique sont multiples et il doit ainsi permettre bien évidemment au meilleur coût et avec un minimum de risques :

- D'assurer l'intégrité, la traçabilité, la confidentialité et la pérennité des données;
- De répondre aux exigences légales et réglementaires de conservation et de restitution;
- De relever le défi de l'obsolescence technologique récurrente;
- De faciliter l'accès à l'information.

Face à tous ces facteurs les responsables d'entreprise se trouvent fort démunis, ne sachant pas par quel bout prendre le problème, d'où la tentation fort compréhensible souvent d'attendre ! Pourtant les enjeux sont de taille qu'ils soient, financiers, juridiques, réglementaires, organisationnels, sécuritaires, géopolitiques, ...et surtout l'augmentation de la volumétrie fait qu'aujourd'hui et de plus en plus, il est indispensable de trouver des solutions et d'appliquer une véritable politique d'archivage, souvent en premier lieu pour les e-mails.

L'objectif de ce document est ainsi d'aider les responsables d'organisations tant publiques que privées dans cette démarche d'archivage au sens électronique du terme, sans oublier que l'un de ses principaux objectifs consiste à pouvoir retrouver rapidement une information au besoin. Appliqué aux e-mails cela n'est pas aussi simple qu'il y paraît, en effet mieux vaut avoir anticipé une recherche lorsqu'il s'agira de trouver un mail parmi plusieurs centaines de millions...

Afin de faciliter au maximum son apport et son accès, le présent document a été construit sous forme de fiches. Chacune d'entre elle a été conçue de façon à pouvoir être lue indépendamment et comporte trois parties : contexte, enjeux et recommandations. Ce choix a été dicté par un souci d'efficacité destiné à permettre au lecteur de trouver rapidement les premiers éléments de réponse aux problèmes qu'il se pose. *A contrario*, ceci provoque inévitablement certaines répétitions ou renvois le cas échéant à d'autres fiches complémentaires.

A l'intérieur de chaque fiche on pourra retrouver un certain nombre de focus (sous forme d'encadrés) au sujet de certains points importants qu'il ne nous était pas possible de traiter ici plus en détail. Par ailleurs, un référentiel documentaire à la fin du présent document permettra à ceux qui le désirent de pouvoir approfondir tel ou tel aspect.

Conserver les courriers électroniques		
Phase	**N° Fiche**	**Thèmes**
Le cadre	1	Besoins d'archivage
	2	Aspects juridiques
	3	Contraintes techniques
	4	Méthodologie et normes
Les solutions	5	Grandes familles de solutions
	6	Exemples d'architectures
	7	Tiers archiveur
	8	Risques et assurances
	9	Sécurité
	10	Principaux acteurs du marché
	11	Coûts de l'archivage
	12	Cas Clients

Les points focus :

N° Fiche	Focus
1	A propos de l'intégrité
2	A propos de la confidentialité
3	A propos de la signature électronique
4	A propos de l'identification - authentification Politique d'archivage
9	L'évolution « du WORM physique vers le WORM logique »
10	La fonction WORM à partir des disques magnétiques

Fiche 1 – Besoin d'archivage

Contexte

De façon très générique, l'archivage correspond à la mémoire de toute organisation et répond ainsi à deux nécessités essentielles, à savoir conserver l'information et surtout être capable de la retrouver facilement.

Les origines de l'archivage électronique sont par ailleurs multiples :

- La dématérialisation de plus en plus importante de bon nombre de procédures, fait que les volumes de données à conserver augmentent sensiblement ;
- La sécurisation de l'information est extrêmement importante et la conservation fait évidemment partie des éléments qui y contribuent ;
- La rationalisation des espaces de stockage est également à l'origine de l'archivage dans la mesure où il paraît naturel de faire correspondre au mieux les besoins avec les solutions disponibles. Toutes les données n'ont pas à être traitées de la même manière du fait de leur grande disparité en matière de criticité, importance ou encore valeur pour l'entreprise ;
- Au-delà de ses besoins naturels de conservation des données s'ajoute de plus en plus des obligations tant légales que réglementaires qui pèsent sur les organisations qu'elles soient publiques ou privées ;
- Enfin la notion de patrimoine concerne plus spécifiquement la notion de mémoire évoquée précédemment, destinée à garder les éléments importants pour l'histoire, la trace du passé.

En complément à ces origines, capables de s'appliquer quelle que soit la forme de l'information, données structurées ou non, images, sons, vidéos il est important de traiter ici quels sont véritablement les besoins qui en découlent en l'appliquant directement aux e-mails.

Remarque : L'e-mail peut être considéré comme un simple vecteur de transmission, un système de communication parmi d'autres qui permet d'envoyer des documents en pièces jointes. Dans pareil cas il est clair qu'il n'y a aucune spécificité *a priori* en matière d'archivage de contenu mais attention au fait qu'il peut avoir une véritable « valeur » dans la mesure où il va permettre de garder la trace d'un échange. Dans la majorité des cas, l'e-mail, en plus de cette notion de trace, véhicule de l'information en son sein même et doit donc être considéré comme un type particulier de document dont l'archivage doit être analysé avec soin compte tenu de cette dualité et des enjeux décrits ci-après.

Besoins en matière d'e-mails, réponse de l'archivage

Les volumes de données échangées grâce aux e-mails augmentent continuellement et par ailleurs il est évidemment essentiel de répondre à ses obligations. On peut ainsi relever un certain nombre de problèmes qui en résultent tels :

- Adaptation des espace disque de stockage sur les serveurs : l'archivage va permettre de pouvoir déplacer automatiquement des e-mails selon des règles pré-établies vers un stockage adapté. Très rapidement un e-mail n'est plus consulté qu'occasionnellement et il peut donc être déplacé sur des critères de date de réception, de taille, de quota dans la boite aux lettres vers un stockage moins onéreux qu'un serveur de messagerie ;
- Temps de sauvegarde et de restauration: les espaces de messagerie sont l'équivalent de bases de données à sauvegarder très régulièrement dans leur intégralité. Le fait d'archiver va permettre de très largement optimiser les sauvegardes tout en conservant en ligne les éléments ainsi archivés ;
- Performance des serveurs : le fait d'archiver les e-mails va soulager d'autant les serveurs de messagerie et ainsi éviter d'augmenter leurs performances en quasi permanence. En effet lors d'une consultation, d'une réponse ou d'une transmission d'une archive, le serveur principal de messagerie ne sera pas sollicité, l'information sera ainsi directement transmise à partir du système d'archivage ;
- Gestion anarchique de fichiers d'archive (en général en mode PST) en local sur le poste de travail : en général et plutôt que de mettre en place une organisation rationnelle des e-mails, ont été mis en place des quotas sur les boîtes aux lettres dont la principale conséquence a été de créer de nouvelles contraintes du simple fait que les utilisateurs se sont rabattus sur d'autres solutions approximatives afin de conserver l'ensemble de leurs e-mails. Le recours à une

solution d'archivage et à la définition de règles d'archivage permet de supprimer des boîtes aux lettres les e-mails et pièces jointes automatiquement. Suivant les solutions proposées, il est également possible de créer des raccourcis pour permettre aux utilisateurs d'afficher facilement les éléments d'origine dans leur environnement. Les utilisateurs bénéficient ainsi d'un accès instantané à tous leurs e-mails, sans problème de coût ou de gestion ;

- Retrouver l'information : sans système dédié à cet effet, il est relativement difficile de retrouver des données parmi des e-mails du simple fait de leur grande quantité mais aussi du fait en général de la création de plusieurs dossiers et sous dossiers destinés à classer mais ayant pour conséquence que l'e-mail recherché ne se trouve en général jamais dans le bon dossier. Un système d'archivage efficace permet l'indexation des e-mails et des pièces jointes offrant ainsi une recherche et une extraction de données aussi faciles que rapides ;
- Accès à ses e-mails à distance : si l'on procède à l'archivage des e-mails sous forme de fichiers PST il s'agit là d'un véritable frein au nomadisme dans la mesure où de tels fichiers ne peuvent être retrouvés autrement qu'en mode local. Une solution d'archivage permet au contraire d'accéder aux e-mails archivés à partir de n'importe quel lieu pour peu que l'accès puisse se faire au travers d'une interface web ;
- Risques de perte d'information : en cas de changement, perte ou destruction du poste de travail l'ensemble des e-mails qui s'y trouvent peut être perdu, que les e-mails soient en mode natif ou sous forme de PST (très souvent mal ou pas du tout sauvegardé). La situation la plus aberrante consiste pour les utilisateurs à sauvegarder leurs PST sur des serveurs de fichiers centraux (serveurs de ressources), procédure qui conduit à gérer de multiples versions des fichiers PST aussi bien sur les serveurs de fichiers que sur les supports de sauvegarde. La mise en place d'une solution d'archivage permet d'éviter ce risque par une gestion centralisée des e-mails archivés couvrant entre autre la problématique de la sauvegarde de façon tout à fait optimisée ;
- Répondre à ses obligations (légales et réglementaires) : de plus en plus les entreprises doivent conserver un certain temps toutes leurs données électroniques dont les e-mails et les messages instantanés. Une solution d'archivage s'impose alors afin de servir de référentiel sécurisé pour les éléments exigeant un délai de conservation donné.

Enjeux

La mise en œuvre d'une solution d'archivage d'e-mails doit permettre d'offrir à l'utilisateur une importante capacité de stockage de ses messages, tout en garantissant leur conservation dans le temps et en optimisant leur gestion. L'archivage des e-mails répond ainsi à de multiples enjeux :

- Organisationnel : la messagerie est devenue indispensable et incontournable dans la vie quotidienne de toute organisation. Les serveurs se multiplient ce qui entraîne forcément une complexité de l'exploitation. L'archivage des e-mails doit permettre une exploitation efficace des échanges et du système informatique de l'entreprise ;
- Sécuritaire : la volumétrie des e-mails est importante, croît fortement et continuellement tant en nombre qu'en volume. Si les procédures de sauvegarde sont rendues difficiles, c'est donc la sécurité des données qui est remise en cause et l'archivage des e-mails doit entre autre permettre une rationalisation de leur sauvegarde ;
- Juridique : en complément au point précédent, le principal risque est de ne pas pouvoir produire en cas de besoin les données requises dans une forme recevable. Rappelons à ce sujet que les données doivent être archivées en respectant a minima les caractéristiques d'identification, d'intégrité et d'intelligibilité leur permettant ainsi d'être retenues comme élément de preuve valide ;
- Financier : au niveau financier l'enjeu est multiple avec en premier lieu la conséquence sous forme d'amende ou de condamnation, liée à la non production de données en cas de litige. En second lieu nous attirons également l'attention sur un autre phénomène à ne pas négliger qui relève du temps passé à la recherche d'information ou encore d'investissements perdus dans des outils non maintenus dans le temps. Enfin de façon plus classique la mise en place d'un archivage d'e-mails permet un gain direct au niveau des espaces de stockage et des procédures de sauvegarde ;
- Technique : l'enjeu technique est également double avec les problèmes d'interopérabilité entre systèmes, et le défi de pérennité des données sur le long terme, face à l'obsolescence rapide des supports et des formats.

Recommandations

Outre les besoins globaux et génériques exprimés précédemment au sujet des e-mails et pour lesquels l'archivage apporte une véritable solution, il n'en reste pas moins vrai que la première tâche consiste à évaluer ses besoins en détail, c'est-à-dire archiver quoi, pourquoi et pour combien de temps ? Afin d'aider à cette définition de besoins, il est recommandé de répondre de manière appropriée aux questions suivantes :

1. Quels sont les e-mails à archiver parmi l'ensemble géré ?	Les e-mails à archiver représentent en général une minorité de l'ensemble de ceux qui sont produits et reçus dans le cadre des activités de toute organisation. Il faut donc si possible parvenir à classifier les e-mails afin de pouvoir décider de ceux qui entreront dans le processus de conservation et si possible élaborer des priorités par rapport à des notions comme, la valeur de l'information, le caractère légal et réglementaire, les données à caractère personnel ou encore la mémoire historique.
2. Quelle est la criticité des données véhiculées par les e-mails?	Il s'agit si possible d'évaluer et de préciser : - la sensibilité de l'information (confidentielle, difficile à reconstituer), ou au contraire information courante ; - la disponibilité, c'est-à-dire les conditions de la consultation (fréquence et rapidité) selon les types de données.
3. Quelles sont les exigences de conservation ?	Le système d'archivage doit assurer la maintenance des données jusqu'à la fin du cycle de vie de l'information. Cette durée peut aller de quelques mois à plusieurs décennies, voire ad vitam aeternam. La durée de conservation est déterminée soit en application des textes légaux et réglementaires, soit par analogie avec ces textes en fonction du risque de contentieux, soit par métiers en fonction de la réutilisation prévisible de l'information ainsi archivée.
4. Quelles exigences d'intégrité et de sécurité doit-on assurer ?	Si les données doivent être restituées dans un environnement juridique ou dans le cadre d'un audit, il est impératif qu'elles respectent certaines conditions. En fait la loi de mars 2000 (voir fiche 2 Aspect légal de l'archivage numérique) fait ressortir quatre éléments fondamentaux : - Intelligibilité de la donnée ; - Intégrité du contenu depuis son origine (voir focus ci-après); - Identification de l'auteur ou des auteurs de l'information ; - Pérennité de l'information.
5. Quelle est la volumétrie à traiter ?	Au niveau des e-mails il est important de faire la distinction entre le nombre d'e-mails et la volumétrie en termes d'espace de stockage. La maîtrise de ces éléments est indispensable afin de pouvoir estimer correctement les besoins.
6. Quels accès ?	La question de l'accès comporte plusieurs aspects : - les droits d'accès, définis en fonction du profil des utilisateurs (notion d'habilitation) : accès à tout ou partie des informations, restrictions d'accès, évolution dans le temps ; - la possibilité de recherche d'information via des mots-clés (indexation automatique ou manuelle) ou à l'aide d'un moteur de recherche, assorti ou non d'un thésaurus.

A propos de l'intégrité

Ne pas recueillir d'information constitue un problème d'indisponibilité, tandis qu'obtenir des informations fausses ou mutantes est un souci d'intégrité. Ce dernier point est très important et à traiter avec d'autant plus d'attention que la durée de conservation des données sera longue et donc les risques plus nombreux.

L'intégrité est ainsi définie comme la propriété qui assure qu'une information n'est modifiée que par les utilisateurs habilités dans les conditions d'accès normalement prévues. On recherche donc par l'intégrité, l'absence de modification volontaire ou involontaire des flux et des traitements.

L'article 4.f du Règlement CE n° 460/2004 du Parlement européen et du conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information définit l'intégrité des données comme : *« la confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas été modifiées* »

Si l'intégrité représente un critère de sécurité de base, il en est néanmoins le plus diffus et donc le plus difficile à mettre en œuvre sur la totalité de la cible du traitement de l'information.

L'intégrité se subdivise normalement en deux sous ensembles distincts pour s'approcher davantage de la mécanique du traitement de l'information :
- L'intégrité des flux de données,
- L'intégrité des traitements.

En général, les atteintes à l'intégrité sont d'origine malveillantes. Les cas d'accidents ou d'erreurs sont beaucoup plus rares. Selon le CLUSIF (Club de la Sécurité des Systèmes d'Information Français), sur une période de plus de 10 ans, la malveillance s'accroît de près de 15 % par an, principalement au détriment de l'intégrité des données et des traitements. Le monde de l'Internet est en effet un champ d'expérimentation mondial pour l'atteinte à l'intégrité des données, des messages et des traitements.

Cependant il existe plusieurs interprétations possibles de l'intégrité suivant que l'on se place du côté purement technique ou plutôt du côté organisationnel et juridique. Par principe l'intégrité technique d'un document électronique est mise en cause dès l'instant où un seul des bits constituant le document est modifié. A l'inverse l'intégrité au sens juridique d'un document consiste à conserver le sens de l'information qu'il contient sans s'attacher nécessairement à la forme. Ainsi le fait de modifier un accent dans un texte ne va pas en changer fondamentalement le sens alors que cela suffira à lui faire perdre son intégrité technique.

Afin d'apporter une solution à cette difficulté d'interprétation, le Forum des Droits sur l'Internet et la Mission Économie Numérique ont recommandé dans leur rapport 2006 que la notion d'intégrité du document telle que prévue par l'article 1316-1 du Code Civil soit assurée par le respect cumulé des trois critères suivants :
- Lisibilité du document,
- Stabilité du contenu informationnel,
- Traçabilité des opérations sur le document.

Les enjeux de l'intégrité des flux et des traitements sont fondamentaux, spécialement à l'heure d'Internet dans la mesure où il est indispensable de pouvoir faire « confiance » aux données constituant l'élément essentiel du patrimoine informationnel. En effet la perte d'intégrité peut présenter des dangers vitaux comme par exemple des mutations de données du groupe sanguin d'un dossier médical partagé (stocké dans un centre d'hébergement des dossiers médicaux) ou bien d'un identifiant patient etc. Les cas pratiques donnant lieu ou non à des recours juridiques sont très nombreux et inquiétants, du fait de leur croissance exponentielle depuis plus de quinze ans.

Fiche 2 – Aspects juridiques du mail

Contexte

Le courrier électronique est défini par l'article Ier IV de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) comme « tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ».

La LCEN ne distingue pas entre courrier électronique professionnel et courrier électronique privé.

L'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, un message à caractère personnel est un usage généralement et socialement admis.

La Cour de Cassation, a notamment jugé, dans un arrêt Nikon du 2 octobre 2001, que « le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique le respect du secret des correspondances ; que l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».

De même, dans un arrêt du 17 mai 2005, elle a décidé que « sauf risque ou évènement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ».

La Cour de cassation précise également, dans un arrêt du 18 octobre 2006, que les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence.

Afin que le courrier électronique soit identifié comme personnel, il doit comprendre dans son objet la mention « privé » ou « personnel ».

Le rôle de l'administrateur de réseaux doit par ailleurs être rappelé dans la mesure où il a pour fonction d'assurer le fonctionnement ainsi que la sécurité du réseau, ce qui implique qu'il puisse accéder aux messageries voire à leur contenu, ne serait-ce que pour les débloquer ou éviter des démarches hostiles.
Toutefois, la Cour de cassation a précisé, dans un arrêt du 17 décembre 2001, que si « la préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait, (…) par contre, la divulgation du contenu des messages ne relevait pas de ses objectifs ».
Aux termes de l'article L. 211-1 du Code du patrimoine, les archives sont l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité.

L'archivage peut répondre à deux finalités:
- probatoire (pour sauvegarder la preuve d'un droit ou respecter une obligation légale de conservation) ;
- patrimoniale (à des fins historiques ou statistiques, pour la mémoire de l'entreprise).

Enjeux

Aucune disposition légale générale n'impose de durée de conservation pour les correspondances individualisées, même à caractère professionnel.

Néanmoins, la conservation de ces courriers peut s'avérer nécessaire à des fins de preuve voire patrimoniale, dans le cadre du contrôle interne qui s'impose aux établissements financiers ou encore au titre de l'administration électronique.

La durée de conservation des courriers doit être déterminée en fonction du contenu du message et de l'objet du courrier, mais également des pièces attachées au courrier.
La conservation de documents à des fins probatoires nécessite le respect de certaines

exigences légales, qui se traduisent notamment par des exigences techniques. Ces exigences s'appliquent aussi bien en droit privé qu'en droit administratif car, si en droit administratif la preuve est libre, il faut néanmoins emporter l'intime conviction du juge.

Ces exigences doivent être modulées en fonction de règles spécifiques applicables à certains types de documents ou secteurs d'activité, et des conventions de preuve passées entre les signataires d'un acte, puisque ces conventions ont pour objectif de définir les modes de preuve admis entre les parties, sans porter atteinte aux règles d'ordre public, notamment celles issues de la loi du 17 juin 2008 portant réforme de la prescription qui encadrent les conventions relatives aux prescriptions extinctives et la législation relative aux clauses abusives.

Qu'un document comportant des engagements ait été passé par écrit sous forme électronique pour des raisons liées à des finalités probatoires, ou que cet écrit soit le fruit d'une obligation légale, les modalités de son établissement et de sa conservation sont les mêmes : il convient de respecter les dispositions des articles 1316-1 et 1316-4 du Code civil.

En effet, en cas de contestation d'un écrit ou d'une signature électronique, l'article 287 du Code de procédure civile dispose que le juge doit vérifier si les exigences des articles 1316-1 et 1316-4 du Code civil sont satisfaites.

L'article 1316-1 du Code civil dispose que l'écrit électronique est recevable à titre de preuve, au même titre que l'écrit papier, sous réserve :

- qu'au moment de son établissement, la personne dont il émane puisse être dûment identifiée et qu'il soit établi dans des conditions de nature à en garantir l'intégrité ;
- qu'il soit ensuite conservé dans des conditions de nature à en garantir l'intégrité.

L'archivage sécurisé d'un document électronique qui n'a pas été établi dans le respect des dispositions légales ne pourra faire preuve parfaite et n'aura qu'une simple valeur de « renseignement ».

La signature électronique permet d'assurer l'identification de l'émetteur d'un courrier électronique. En effet, l'article 1316-4 du Code civil prévoit que la signature a pour fonction d'identifier celui qui l'appose.

SIGNATURE ELECTRONIQUE

La signature électronique peut être simple ou sécurisée, ces deux types de signature ayant la même valeur juridique, la différence résidant dans la personne sur laquelle pèse la charge de la preuve de la fiabilité du procédé de signature.

En cas de signature simple, la charge de la preuve de la fiabilité du système pèse sur celui qui se prévaut de la signature ; en cas de signature sécurisée, la charge de la preuve de l'absence de fiabilité pèse sur celui qui conteste cette valeur à la signature électronique.

La signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

Un procédé d'identification est présumé fiable lorsque :

- la signature électronique est créée ;
- l'identité du signataire est assurée ;
- l'intégrité de l'acte est garantie,

dans les conditions fixées par les décrets n°2001-272 du 30 mars 2001 et n°2002-535 du 18 avril 2002.

La signature électronique doit être établie grâce à un dispositif sécurisé de création de signature électronique certifié puis vérifiée au moyen d'un certificat électronique qualifié qui doit lui même répondre à une double exigence portant sur les informations qu'il doit contenir et sur le prestataire de services de certification électronique (PSCe) qui le délivre[1].
L'ensemble des éléments permettant d'établir la validité de la signature apposée doit être conservé.

Les formalités connexes imposées pour la validité des actes sous forme de courriers électroniques (LRAR, double original…) devront également avoir été réalisées lors de la réalisation de l'acte, en amont de l'archivage.

Quant à l'intégrité, cette notion concerne l'intégrité du contenu, ce dernier devant rester intègre depuis sa création et jusqu'à la fin de sa conservation. L'intégrité est nécessaire à la validité de la signature électronique puisque l'article 1316-4 du Code Civil pose également cette exigence, outre celle d'identification.

[1] Art. 6 I et II du décr. du 30/03/2001.

Il convient donc d'opérer une distinction entre la forme électronique et le support électronique, le législateur n'ayant posé de conditions à l'équivalence avec l'écrit sur support papier qu'en ce qui concerne cette même forme.

E-DISCOVERY

Le concept « e-discovery » désigne le processus consistant à satisfaire une demande légale de production de messages électroniques archivés, généralement en tant que preuve dans une affaire civile ou pénale.

Alors que les outils d'archivage de courriers électroniques permettent de stocker et de conserver les messages, le processus d'e-discovery permet la recherche et récupération de documents électroniques sur des disques durs, des serveurs avec pour objectifs la production de preuve dans une information judiciaire.

Un plan d'e-discovery doit être mis en œuvre afin de pouvoir produire des courriers électroniques dans une affaire civile ou pénale.

ARCHIVES PUBLIQUES

La conservation des archives publiques est régie par des principes spécifiques.

A l'expiration de leur période d'utilisation courante ou à l'expiration de la durée de conservation nécessaire si elles constituent des données à caractère personnel, les archives publiques font l'objet d'une sélection pour séparer les documents à conserver des documents dépourvus d'utilité administrative ou d'intérêt historique ou scientifique, destinés à l'élimination.

La liste des documents ou catégories de documents destinés à l'élimination ainsi que les conditions de leur élimination sont fixées par accord entre l'autorité qui les a produits ou reçus et l'administration des archives.

Pour les organismes visés par le Code du patrimoine, la politique d'archivage dépend d'un accord entre l'autorité qui a reçu les documents ou les a émis et l'administration des archives.

Une obligation de conservation d'une durée imprescriptible peut s'appliquer.

ARCHIVAGE DE DONNEES PERSONNELLES

L'archivage de documents contenant des données à caractère personnel doit faire l'objet des formalités requises par la loi du 6 janvier 1978.

A ce titre, l'entreprise doit :

- soit effectuer de nouvelles formalités préalables relatives à la gestion de l'archivage électronique ;
- soit modifier les formalités préalables qui avaient déjà été effectuées en vue d'y introduire l'archivage des données.

Toutefois, en vertu de l'article 36 II de la loi du 6 janvier 1978, les traitements dont la finalité se limite à assurer la conservation à long terme de documents dans le cadre du livre II du Code du patrimoine sont dispensés des formalités préalables à la mise en œuvre des traitements.

En vertu de l'article 32 de la loi Informatique et Libertés, l'entreprise doit notamment informer les personnes concernées par le traitement de son identité en tant que responsable du traitement, des finalités poursuivies par le traitement, et des destinataires des données, sous peine de sanctions pénales.

En outre, l'entreprise doit prévoir la possibilité d'une demande de droit d'accès et de rectification des données archivées; cependant, ainsi qu'il résulte de l'article 39 II de la loi de 1978, dès lors que le traitement des archives se limite à assurer la conservation à long terme des documents, sans aucun risque d'atteinte à la vie privée des personnes concernées, le responsable du traitement n'est pas tenu de donner suite aux demandes d'accès aux données archivées. Ainsi, le client doit être en mesure d'assurer que les moyens d'archivage employés sont de nature à exclure manifestement tout risque d'atteinte à la vie privée des personnes concernées.

Par ailleurs, l'entreprise doit conserver les données à caractère personnel archivées sous une forme permettant l'identification des personnes concernées pour une durée n'excédant pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées (article 6-5° de la loi de 1978) sous peine de sanctions pénales.

En matière d'archivage probatoire, c'est la durée de prescription applicable au document qui va déterminer la durée de conservation.

La loi du 17 juin 2008 a modifié les délais de prescription en matière civile. Le délai de droit commun de la prescription est désormais de 5 ans à compter du jour où le titulaire du droit a connu ou aurait dû connaître les faits lui permettant de l'exercer.

Au-delà de la durée de conservation légale, il convient de mettre en œuvre des procédures d'anonymisation en particulier lorsque la finalité de l'archivage est patrimoniale.

L'entreprise doit enfin prendre toutes précautions utiles pour préserver la sécurité et la confidentialité des données (voir focus ci-après) conformément à l'article 34 de la loi de 1978, sous peine d'entraîner sa responsabilité pénale.

La Commission Nationale de l'Informatique et des Libertés (CNIL) précise que les principes visés ci-dessus s'appliquent aux trois catégories d'archives précitées, courantes, intermédiaires et définitives[2].

La CNIL recommande à ce titre que :

- s'agissant des archives intermédiaires, que l'accès à celles-ci soit limité à un service spécifique et qu'il soit procédé, a minima, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) ;
- s'agissant des archives définitives, que celles-ci soient conservées sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'archives ;
- afin de garantir l'intégrité des données archivées, soient mis en œuvre des dispositifs sécurisés lors de tout changement de support de stockage des données archivées ;
- soient mis en œuvre des dispositifs de traçabilité des consultations des données archivées ;
- soient utilisées des procédures d'anonymisation.

[2] Délibération n°2005-213 du 11 octobre 2005.

A propos de la confidentialité

En matière de sécurité la confidentialité est une caractéristique très importante abordée également au niveau du contrôle d'accès. En fait la confidentialité revêt à la fois la notion de secret et de diffusion restreinte à un petit nombre de personnes.

La confidentialité représente une propriété qui assure que dans les conditions normalement prévues, seuls les utilisateurs autorisés (ou habilités) ont accès aux informations concernées.

La principale limite de la confidentialité tient au fait qu'une personne ne peut être tenue pour responsable d'aucune divulgation si les éléments révélés étaient déjà dans le domaine public ou si elle en en avait déjà connaissance ou pourrait les obtenir de tiers par des moyens légitimes.

Les informations confidentielles sont évidemment importantes : confidentialité médicale (personne atteinte du VIH etc.), confidentialité de votre code de carte bancaire, mot de passe personnel pour le contrôle d'accès physique et (ou) logique dans l'entreprise, secrets liés à la tactique militaire, etc.

Comme évoqué précédemment la confidentialité intervient également au niveau du contrôle d'accès. Il peut être ainsi judicieux d'anticiper la situation où des personnes non autorisées parviendraient néanmoins à accéder au système d'information. Dans ce dernier cas la confidentialité des données peut cependant être préservée grâce à la mise en oeuvre d'un système de chiffrement. La caractéristique principale d'un tel système est de rendre les données illisibles par toute personne ne possédant pas la clé pour les déchiffrer. Cependant la connaissance et l'accès à cette clé peuvent poser beaucoup de difficultés, surtout au bout de nombreuses années.

Suivant la situation, la confidentialité des informations doit être plus ou moins bien maîtrisée. Ainsi dans le cas de l'outsourcing ou de l'info gérance par exemple, on devra porter une attention toute particulière à la confidentialité. De même selon la sensibilité des données traitées tant à l'intérieur qu'à l'extérieur de l'entreprise il y aura lieu d'être particulièrement vigilant quant au respect de la confidentialité desdites données. En fait il existe trois principaux moyens pour assurer la confidentialité :
- La mise en place d'un système de contrôle d'accès ;
- Le chiffrement des données ;
- L'externalisation des données. De part les engagements et les responsabilités prises par l'hébergeur, une solution externe doit permettre d'éviter tout problème de confidentialité en interne dans l'entreprise. Rappelons à ce sujet que près des 2/3 des délits informatiques ont des origines internes. Pour un maximum de sécurité on pourra avoir recours à une externalisation de données chiffrées.

POLITIQUE D'ARCHIVAGE (voir focus PA fiche 3 Méthodologie)

La mise en œuvre d'une politique d'archivage n'est pas sans poser un certain nombre de difficultés, qu'il s'agisse de l'archivage lui-même ou de la suppression de certaines données et informations.

En ce qui concerne la suppression des données et des éléments électroniques et tout particulièrement des courriers électroniques, il importe de respecter les dispositions de l'article 226-15 du Code pénal qui protège le secret des correspondances.

Cet article évoque notamment l'interdiction de « supprimer » des correspondances.

La suppression est tout acte ayant pour effet de priver, même momentanément, les destinataires des correspondances qui leur sont adressées.

Même si l'alinéa 2, qui vise plus particulièrement le domaine des communications électroniques dont le courrier électronique fait partie, ne reprend pas la « suppression » comme élément matériel de l'infraction, il convient de conserver la correspondance pendant une durée raisonnable, comme l'impose la loi du 6 janvier 1978, puis de le supprimer sans risquer de tomber sous le coup de cette infraction.

Pour ce faire, il importe de qualifier les courriers électroniques émis ou reçus par les salariés en distinguant les courriers relevant des activités professionnelles, des échanges privés.

Ces règles de qualification et de gestion des courriers électroniques doivent nécessairement être portées à la connaissance des salariés, cette information prenant généralement la forme d'une charte d'utilisation des systèmes d'information, assimilée à une adjonction au règlement intérieur.

Il importe enfin de gérer le risque relatif à la dissimulation ou la destruction de preuve réprimée par l'article 434-4 du Code pénal.

Recommandations

1. Définition de la finalité de l'archivage	Bien faire la distinction entre : - archivage probatoire - archivage patrimonial
2. Guide de l'archivage	L'absence de réglementation générale de l'archivage nécessite d'identifier, dans un guide de l'archivage, ses contraintes spécifiques, telles que - Administration Electronique - Agroalimentaire - Archives publiques - Commerce électronique - Compatibilité informatisée - Etablissements financiers - Facture électronique - Santé
3. Charte d'utilisation du système d'information	Les règles de gestion des courriers électroniques doivent intégrées dans la Charte d'utilisation du système d'information destinée au personnel, en renvoyant à une charte de l'archivage, tout en organisant le tri des e-mails : - professionnels - privés
4. Charte de l'archivage	Compte tenu des règles sectorielles spécifiques, une charte de l'archivage doit permettre d'organiser la conservation des courriers électroniques professionnels en fonction des réglementations spécifiques applicables, en veillant : - au nommage - à l'enregistrement des courriers électroniques eux-mêmes - à l'enregistrement des pièces jointes
5. Code de l'archivage	Elaboration d'un code de l'archivage, tenant compte - des durées de prescription - des durées légales de conservation - des finalités patrimoniales (conservation au-delà des prescriptions)
6. Données à caractère personnel	Effectuer les formalités préalables - Droits des intéressés - Assurer la sécurité et la confidentialité des données - Mettre en œuvre des procédures d'anonymisation
7. Droit du travail	L'adoption ou la modification de la charte d'utilisation du système d'information étant susceptible de constituer une adjonction au règlement intérieur, il convient de respecter les règles suivantes : - information individuelle des personnels - information et consultation du Comité d'entreprise voire du Comité d'hygiène, de sécurité et des conditions de travail (CHSCT) ou du Comité Technique Paritaire - formalités préalables auprès de la Cnil en cas de traitement de données à caractère personnel - dépôt - affichage

8. Procédures	Il convient de vérifier que les procédures sont décrites et répondent aux critères technico-juridiques suivants : - Intégrité, - identification, - intelligibilité, - pérennité
9. Sécurité	Le système d'archivage doit intégrer la politique de sécurité, afin de tenir compte des contraintes réglementaires, issues de la loi Informatique et Libertés mais également sectorielles pouvant imposer le recours à un plan de continuité d'activité (voir Fiche Tiers archiveur)
10. Audit et MCO	Le système d'archivage doit être régulièrement audité tant en ce qui concerne sa mise en œuvre que sa conformité afin de veiller à la prise en compte des évolutions réglementaires.
10. Mentions obligatoires	Toute personne immatriculée indique sur ses papiers d'affaire : - la dénomination sociale suivie de la forme de la société ; - le numéro unique d'identification de l'entreprise; - la mention RCS suivie du nom de la ville où se trouve le greffe où elle est immatriculée ; - son capital social ; - le lieu de son siège social ; - le cas échéant, qu'elle est en état de liquidation ; - le cas échéant, la qualité de locataire-gérant ou de gérant-mandataire ; - si elle est bénéficiaire d'un contrat d'appui au projet d'entreprise pour la création ou la reprise d'une activité économique, la dénomination sociale de la personne morale responsable de l'appui, le lieu de son siège social, ainsi que son numéro unique d'identification.
11. Disclaimer (désengagement de responsabilité)	L'insertion de disclaimer dans un e-mail ne s'inscrit pas dans le cadre d'une obligation légale. Cette pratique vise à prévenir d'éventuels risques de violation des secrets des affaires et la création d'obligations de la part de salariés n'ayant pas pouvoir pour engager la société, dont l'efficacité doit être relativisée compte tenu notamment de la théorie du mandat apparent.

Fiche 3 – Contraintes techniques

Contexte

Les objectifs auxquels doit répondre l'archivage des e-mails sont multiples (voir définition des besoins fiche 1 et exigences juridiques fiche 2). Ils ne pourront être atteints qu'avec le respect d'un ensemble de mesures dont une grande partie repose sur des aspects purement techniques. Il en est ainsi de l'intégrité, de la sécurité et de la pérennité des données pour lesquelles il faudra savoir gérer et anticiper le principe de l'obsolescence technologique récurrente tout en facilitant leur accès.

Les différentes contraintes peuvent se résumer ainsi :

- retenir un format logique de document par rapport à différents types (image, vectoriel, traitement de texte, éditique, ...) en fonction de divers critères de choix (pérennité, conversion, coût) ;
- choisir un support de type WORM (write once read many, voir focus fiche 9 sécurité), magnétique ou optique selon différents critères (pérennité, conversion, coût) ;
- analyser les possibilités de migrations tant du point de vue des formats logiques que des supports physiques ;
- prendre en compte certaines spécificités comme celles liées à la signature électronique (voir ci-après) et s'assurer de pouvoir la vérifier ou apporter la preuve de cette vérification au besoin ;
- avoir en permanence à l'esprit les aspects de performance.

Les contraintes technologiques sont d'autant plus importantes qu'une fois en place, un système d'archivage inefficace aura beaucoup de mal à être corrigé compte tenu du volume d'information à traiter.

A propos de la signature électronique

Les données de base

Sans entrer dans le détail de la cryptographie, le principe de signature électronique nécessite la délivrance d'un bi-clé constitué d'une clé publique et d'une clé privée. Cette dernière doit absolument rester secrète à la connaissance de son seul détenteur. A l'inverse la clé publique peut être divulguée, en général assortie d'autres renseignements, le tout étant contenu dans ce que l'on a coutume d'appeler un certificat électronique.

Certificat électronique

Il s'agit d'un document sous forme électronique attestant du lien entre les données de vérification de la signature électronique telles que les clés publiques et un signataire. Equivalent d'un passeport dans le monde physique, le certificat électronique joue véritablement le rôle de pièce d'identité électronique.
Un certificat personnel contient notamment les informations suivantes :
- le nom de son propriétaire ;
- l'adresse e-mail ;
- la clé publique ;
- la date d'expiration du certificat ;
- le numéro de série (unique) du certificat ;
- le nom de l'Autorité de Certification qui a délivré le certificat électronique ;
- la signature de l'Autorité de Certification qui a délivré le certificat électronique (dans la mesure où l'on possède la clé publique de l'organisme émetteur il est dès lors possible de vérifier directement que le certificat est authentique)

L'Autorité de Certification atteste de la véracité de l'ensemble des informations contenues dans le certificat.

Il existe trois grandes classes de certificats électroniques. La distinction entre ces différentes classes se situe au niveau du contrôle des informations contenues dans le certificat.
Le certificat de classe I : ne garantit pas l'identité du titulaire du certificat mais seulement l'existence de l'adresse mail de celui-ci.

Le certificat de classe II : les informations concernant le titulaire et son entreprise sont contrôlées par l'autorité de certification sur la base de pièces justificatives qui sont transmises en général par voie postale. On parle de contrôle sur pièces.
Le certificat de classe III : par rapport à la classe II, un contrôle supplémentaire de l'identité du titulaire est effectué physiquement par un agent de l'autorité de certification. On parle de contrôle en face à face.

Principe de fonctionnement

Signature d'un document

Pour signer un document, on commence par en prendre une empreinte numérique. On chiffre ensuite cette empreinte au moyen de la clé privée. Le résultat de ce chiffrement correspond véritablement à la signature numérique du document. Ce dernier est ensuite transmis au(x) destinataire(s) accompagné de sa signature et du certificat électronique correspondant.

Vérification de signature

La clé publique transmise dans le certificat permet de déchiffrer la signature numérique et donc de retrouver l'empreinte originale du document. On compare cette dernière avec une empreinte que l'on prend du document reçu. Si les deux empreintes sont identiques le document transmis est authentique et émane bien du possesseur de la clé publique, tel que défini dans le certificat électronique. En effet, seule la clé publique contenue dans le certificat est capable de déchiffrer la signature obtenue avec la clé privée correspondante du bi-clé, attestant du même coup de son origine. Reste cependant à vérifier la validité dudit certificat auprès de l'autorité compétente.

En ce qui concerne la signature électronique, il existe une multitude d'informations, souvent malheureusement contradictoires. De même les terminologies différentes ne sont pas là pour aider à la compréhension. C'est ainsi que l'on parle de scellement, de signature, de signature sécurisée, de certificat qualifié, de signature avancée,…Afin de clarifier quelque peu cette situation,seule une approche s'appuyant sur l'aspect juridique de la signature le permet. En effet, il ne faut pas oublier que la finalité de la signature électronique est avant tout de faire en sorte qu'un document puisse être au besoin retenu comme élément de preuve.

Dès lors deux stratégies sont possibles. La première consiste à utiliser un procédé de signature lambda et à avoir la charge d'apporter la preuve de la fiabilité de ce procédé le moment venu. La deuxième façon de procéder revient à employer un procédé possédant une présomption de fiabilité et dans ce cas ce sera à la partie adverse d'apporter la preuve que ce procédé n'est pas fiable.

Enjeux

Le principal enjeu revient ici à pouvoir répondre efficacement aux contraintes techniques posées par l'archivage électronique afin de répondre aux autres enjeux, décrits au niveau des besoins, posés par l'archivage des mails tant technique, que sécuritaire, organisationnel, juridique ou réglementaire et financier.

Face à ces enjeux, la prise en compte des différentes contraintes techniques doit ainsi contribuer à la mise en place d'un système d'archivage répondant aux attentes et, entre autres, à celle de pouvoir augmenter sans pour autant remettre en cause l'existant, grâce à une bonne anticipation des besoins et le choix d'un système aussi évolutif que possible et surtout interopérable.

Recommandations

Devant l'ensemble des ces contraintes nous donnons ci-après un certain nombre de recommandations qu'il nous parait primordial de respecter.

1. Choix du format logique	Compte tenu du besoin de pérennité, nous recommandons de façon générale d'utiliser un format aussi standard (normalisé) et ouvert que possible destiné à permette l'intelligibilité, soit en lecture directe (exemple du TXT), soit par utilisation d'un interpréteur relativement facile à écrire en cas de besoin. S'agissant des e-mails on aura soin de prévoir éventuellement deux formats différents en fonction de la durée de conservation, par exemple un format quasi natif pour des durées relativement courtes et sa transformation en HTML ou autre pour de plus longues périodes. En ce qui concerne les documents on privilégiera une norme comme celle sur le PDF/A, même si elle a tendance à augmenter la taille des documents d'origine.
2. Choix des supports	La garantie minimale que devra offrir le support est la notion de WORM (write once read many). Cette garantie pourra être obtenue soit par le support lui-même, cas des disques optiques, soit par une logique associée à des supports traditionnels. Le type de support sera ensuite choisi en fonction d'autres critères comme la durée de conservation, l'accessibilité, la volumétrie, les contraintes de migration et le coût. Sur ce dernier point on aura soin de faire une comparaison de coût sur une exploitation globale de plusieurs années et non pas uniquement sur l'achat d'une baie de disques.
3. Migration	Compte tenu de l'obsolescence rapide de la grande majorité des supports, leur migration est inéluctable. Il peut également en être de même au niveau des formats logiques. En matière de migration il est indispensable d'évaluer aussi précisément que possible les implications tant en matière de coûts qu'en matière du temps nécessaire et de l'indisponibilité éventuelle du système.
4. Performance continue du système d'accès	Rappelons ici qu'un système d'archivage et tout particulièrement d'e-mails doit permettre de retrouver efficacement une donnée suivant un niveau de performance quasi constant quelle que soit la volumétrie. A ce stade il s'agit plus de considérer le nombre d'e-mails que le volume total. Un système d'indexation classique pourra ainsi se trouver limité en termes de performance. De même un moteur de recherche peut se révéler totalement inefficace à cause du phénomène de « bruit » renvoyant systématiquement une multitude de réponses à chaque recherche, totalement inexploitables.
5. Sécurité, préservation des données	Le système d'accès doit aussi être conçu dans le respect des droits dont dispose chaque utilisateur. De façon plus globale il est indispensable de veiller à la confidentialité des données archivées, à leur intégrité qui impose de plus la mise en place d'un système de traçabilité efficace. Enfin en matière de sécurité doit on assurer la préservation de l'information en mettant en œuvre une logique de sauvegarde traditionnelle ou mieux un système de redondance permettant en cas de sinistre de ne pas perdre de données.
6. PCA/PRA	En complément au point précédent il sera sans doute nécessaire de disposer d'un plan de continuité assorti d'un plan de reprise d'activité en cas d'un quelconque sinistre. Il est en effet impensable de penser que les utilisateurs puissent être privés trop longtemps de leurs e-mails.
7. Evolutivité	Compte tenu de l'augmentation constante des volumes de données à traiter, il est essentiel de prévoir dès la mise en place d'un système d'archivage son évolution afin d'anticiper les augmentations de capacité des différents matériels et plates formes, voire d'envisager à l'origine, déjà certaines migrations de supports.
8. Interopérabilité	Si l'évolutivité du système est importante son interopérabilité l'est tout autant. On retrouve cette notion en matière de construction du système lui-même de telle sorte que l'on puisse changer une de ses composantes sans remettre en cause son intégralité. L'interopérabilité consiste également à pouvoir transférer des données archivées d'un système d'archivage vers un autre.
9. Réversibilité	Enfin la réversibilité doit permettre de pouvoir récupérer efficacement des données archivées dans un système quel qu'il soit sans être obligé de mettre en place des procédures lourdes, voire développer des traitements spécifiques.

Fiche 4 – Méthodologie et normes

Contexte

Comme déjà évoqué, les solutions techniques qu'elles soient logicielles ou matérielles ne suffisent pas à gérer à elles seules la problématique de la gestion des e-mails et par extension de leur archivage. En effet, une grande partie du processus d'archivage électronique s'appuie sur des outils méthodologiques destinés à clarifier les besoins, à organiser le périmètre documentaire et à accompagner le cycle de vie des informations archivées. Pour avoir un système d'archivage efficient et organisé, encore faut-il que ce qu'on lui envoie soit organisé au départ. Il est important à ce niveau de faire attention aux idées fausses comme quoi avec la technique on arrive à tout faire. Même un moteur de recherche si sophistiqué soit-il, est soumis au phénomène de bruit consistant à vous fournir pléthore de réponses sur une recherche pour peu que les informations d'origine soient mal organisées, voire pas organisées du tout.

Il est ainsi essentiel de se poser un certain nombre de questions avant de décider de la mise en place de tel ou tel système. Pour les e-mails on devra répondre avant toute chose à des questions comme :

- Faut-il conserver tous les e-mails ?
- A quel moment sont-ils considérés en position d'archive, y a t-il une procédure de validation ?
- Pendant combien de temps les conserver ?
- La même durée de conservation s'applique t-elle à l'ensemble des e-mails ?
- Comment les retrouver au besoin ?
- Y a-t-il des contraintes de délais pour produire des e-mails ?
- Seront-ils recevables en cas de litige et ne pas être remis en cause ?

De nombreux travaux ont été entrepris et réalisés depuis plusieurs années afin d'aider à répondre à l'ensemble de ce type de questions, au-delà des e-mails. Des normes, modèles et méthodes existent (voir ci-après) dont il est utile de s'inspirer pour certes gagner du temps mais surtout fiabiliser l'archivage et optimiser la gestion de l'information.

Remarque : En ce qui concerne plus particulièrement l'e-mail, il peut être traité en tant que tel comme un type particulier de document ou au contraire être vu comme un document lambda, partie intégrante d'un dossier. Dans ce dernier cas il est clair qu'il entre alors dans un processus plus classique d'archivage de documents dont les règles correspondent à celles du dossier de rattachement. Dans la suite du document nous nous intéresserons essentiellement au traitement des e-mails en tant que type particulier de document.

Enjeux

L'enjeu essentiel consiste à pouvoir retrouver une information qui soit fiable, faute de quoi l'archivage ne sert absolument à rien. Il est ainsi nécessaire de maîtriser tant la forme et le contenu informationnel de ce que l'on archive que les moyens de le retrouver. Encore une fois le cas des e-mails est très représentatif, en effet archiver des messages incomplets ou incompréhensibles parce que rédigés en style télégraphique ou ambigu, présente un intérêt somme toute très limité. A quoi servirait-il de stocker pendant des années des tera octets d'e-mails voire désormais plutôt des peta octets sachant que plus de 80 % sont soit non représentatifs, soit périmés, soit ne produisent que du bruit dans les requêtes. Quant aux autres 20% ils doivent être conservés et répondre aux exigences de pérennité et de fiabilité déjà largement évoquées.

Comme indiqué dans l'introduction nous ne traitons pas ici de la gestion amont des e-mails. Néanmoins il est clair que si dès leur création les e-mails étaient soumis à des règles de gestion précises et rigoureuses, il serait beaucoup plus facile d'identifier les e-mails dits « sensibles » et ainsi faciliter l'organisation de leur archivage.

L'enjeu « légal » de l'archivage étant essentiel nous en rappelons ici les exigences principales en matière de fonctionnalités, issues de la loi ou d'autres textes normatifs.

Les critères légaux

Ceux-ci, on l'a vu, sont définis par l'article 1316-1 du code civil, il s'agit :

- De la capacité à identifier l'origine du document (voir focus identification-authentification ci-après), c'est-à-dire son imputabilité à un auteur désigné, personne physique ou morale. En pratique, il est conseillé d'assurer cette fonctionnalité en associant à l'enregistrement

numérique une méta donnée qui comprendra, entre autre, cette information sur son origine ;
- De la garantie d'intégrité du document tout au long de son cycle de vie. Le Forum des Droits sur l'Internet décline cette qualité en trois fonctions (voir focus intégrité dans fiche 1) :
  - la lisibilité,
  - la stabilité du contenu informationnel (c'est-à-dire sa fidélité par rapport au document d'origine et la capacité de détecter toute modification des documents stockés),
  - la traçabilité des opérations effectuées sur le document, c'est-à-dire la capacité d'enregistrer toutes les opérations effectuées sur les documents stockés (auteur de l'opération, date et heure de l'opération).
- De l'intelligibilité du document afin de permettre son interprétation par quiconque et non seulement par la machine, d'où l'importance des formats ;
- De pérennité, à savoir respecter les durée de conservation en fonction des exigences portant sur le document en question en fonction de son contenu informationnel.

A propos de l'identification – authentification

Authentifier une personne procède d'une démarche élaborée consistant à certifier le lien entre la personne et son identification. Il est important de pouvoir protéger l'information en identifiant aussi parfaitement que possible les personnes y ayant accès afin entre autres de respecter la confidentialité des données.

Identifier quelqu'un consiste à établir l'identité de la personne c'est à dire son caractère permanent et fondamental tandis qu'authentifier revient à certifier l'exactitude de son identité.

L'article 4.e du Règlement CE n° 460/2004 du Parlement européen et du conseil du 10 mars 2004 définit l'authentification comme « *la confirmation de l'identité prétendue d'entités ou d'utilisateurs* ».

La dualité de ces deux notions d'identification et d'authentification est chose importante en matière de contrôle d'accès afin d'authentifier la personne après l'avoir identifié. Cela touche le système d'information mais aussi le contrôle d'accès physique à tel ou tel bâtiment.

Au sujet du terme authentification
En réalité, le terme authentification ne s'applique qu'aux objets et l'on parle régulièrement, par exemple, d'authentifier une œuvre d'art. Ainsi, l'usage de ce terme en informatique est souvent employé à tort pour signifier « identification ». L'origine de cette erreur provient d'un anglicisme lié au terme anglais authentication, faux ami qui veut dire à la fois « identification » et « authentification ». Mais en français, seul le terme « identification » convient pour déterminer si un objet ou une entité est bien untel ; il s'agit d'une certaine façon d'un véritable contrôle d'identité. À l'inverse, l'« authentification » sert à déterminer si un objet, et non plus une personne, a les caractéristiques prétendues.

Le principe est en général d'identifier la personne grâce à un système d'identifiant (login) assorti d'un mot de passe. Malheureusement rien n'indique de façon certaine qu'il s'agit bien de la bonne personne. En effet même si l'identifiant et le mot de passe sont corrects, il se peut très bien que l'utilisateur qui se connecte les ait dérobés à leur propriétaire. Afin de pallier cet inconvénient majeur en terme de sécurité, on aura en général recours à ce que l'on a coutume d'appeler un système d'« authentification forte » consistant à vérifier avec quasi certitude que la personne qui s'identifie est bien celle qu'elle prétend être.

Nous reprenons ci-après les sept systèmes d'identification/authentification les plus utilisés, à savoir :
1. Identifiant (login) et mot de passe (password) : dispositif le plus courant mais très peu sûr.
2. Identifiant et OTP (One-Time Password) : l'utilisateur dispose d'un token ou « calculateur » qui lui fournit un mot de passe (à usage unique et à durée limitée) au moment où il se connecte. Pour pouvoir utiliser son calculateur, il doit tout d'abord y introduire un mot de passe.

3. Le certificat électronique sur carte à puce ou clé USB : L'utilisateur dispose d'un certificat électronique stocké sur son support et activé grâce à un code PIN. Cette solution nécessite l'existence d'une infrastructure PKI afin de pouvoir délivrer et suivre la vie des certificats.
4. La clé « Confidentiel Défense » : Il s'agit en fait d'une déclinaison particulière du cas précédent. En général le support est multifonctions et permet ainsi le stockage de certificat X509, de données, de ressource cryptographique (pour le chiffrement à la volée du disque dur et des flux applicatifs). Afin de contrer les risques des « key loggers » (enregistrement des touches frappées à l'insu de l'utilisateur), le code PIN doit être composé directement sur la clé sans passer par le clavier (exemple du dispositif utilisé par la Gendarmerie Nationale où la souris fait office de lecteur de carte et dispose d'un clavier numérique pour frapper le code PIN).
5. La carte à puce avec identifiant et mot de passe : Ce système correspond à une version allégée de la troisième solution dans la mesure où elle ne nécessite pas d'infrastructure PKI. L'authentification de l'utilisateur est faite directement à partir de l'annuaire d'entreprise (par exemple en s'appuyant sur le protocole LDAP (Lightweight Directory Access Protocol).
6. Les solutions biométriques qui utilisent des lecteurs biométriques (iris de l'œil, index, configuration de la face, contour de la main, etc.) pour contrôler les accès. Cependant le critère choisi est plus ou moins facile à mettre en œuvre et présente une force variable. De fait la configuration de l'index avec ses points de contrôle reste encore aujourd'hui le mécanisme biométrique le plus abouti. La police scientifique de la fin du XIXème siècle avait fait le bon choix avant que des lecteurs électroniques du doigt ne soient mis au point, cent ans plus tard ! Trois possibilité sont offertes afin de conserver les données à comparer au moment de la lecture biométrique, à savoir : au niveau du poste de travail, au niveau d'une carte cryptographique ou au niveau d'un serveur (se pose alors le problème légal du stockage de données biométriques centralisées en un seul endroit).
7. Le RFID (Radio Frequency Identification) actif : Cette technologie permet d'identifier l'utilisateur sans contact physique, à quelques mètres de distance. Le badge de l'utilisateur possède une alimentation propre qui lui permet de dialoguer avec une antenne connectée au poste de travail. Ce dernier détecte alors l'arrivé ou le départ d'un utilisateur sans aucune autre action particulière de sa part si ce n'est d'indiquer son mot de passe, au moins une fois.

En résumé, l'authentification d'une personne est basée sur l'un au moins des trois critères suivants :
- Ce que sait la personne, par exemple un mot de passe ;
- Ce que possède la personne, un token ou un certificat électronique ;
- Ce qu'est la personne, aspect biométrique.

Les critères normatifs

Le recours à une norme d'archivage a des conséquences importantes au plan juridique. En effet, d'après la jurisprudence (*Cour de cassation, Chambre civile, 4 février 1976, Bull. civ, II, n°49*), l'existence d'une norme dans un domaine est représentative d'un état de l'art. Or, l'état de l'art est la notion à laquelle les tribunaux se réfèrent en cas de litige portant sur une matière technique : la mise en place par une entreprise de systèmes techniques qui sont à l'état de l'art caractérise sa diligence, et est de nature à atténuer sa responsabilité en cas de litige.

Il existe à ce jour de nombreuses normes relatives à l'archivage (voir liste ci-après). Certaines de ces normes précisent les spécifications techniques à respecter et explicitent les critères légaux précédemment identifiés, d'autres (comme MOREQ) sont relatives à l'organisation de l'archivage.

Les normes insistent notamment sur une fonctionnalité essentielle de tout système d'archivage sur le long terme, qui est la pérennité de celui-ci, qui implique l'utilisation de standards indépendants des applications et des environnements informatiques.

Les principales normes ou guides pour l'archivage

- guide de l'archivage électronique sécurisé, Association Ialta France, juillet 2000 : recommandations pour la mise en œuvre d'un système d'archivage interne ou externe utilisant des techniques de scellement aux fins de garantir l'intégrité, la pérennité et la restitution des informations, ouvrage collectif sous la direction de Michel Lesourd (Directeur Adjoint des Etudes Techniques au CSOEC) ;

- recommandations du Forum des Droits de l'Internet relative à la Conservation électronique des documents (secteur privé), publié le 1er décembre 2005 en partenariat avec la Mission pour l'Economie Numérique ;
- modèle OAIS (système ouvert d'archivage d'informations), devenu la norme internationale ISO 14721 ou modèle OAIS (Open Archival Information System) de la Consultative Comittee for Space Data System, décrit l'organisation et le fonctionnement d'un centre d'archivage pour la pérennisation des données numériques ;
- ISO 15489 - Records Management, stratégie globale pour la traçabilité de l'information et des responsabilités. Cette norme est souvent associée à la méthodologie DIRKS (Design and Implementation of Record Keeping Systems) d'implémentation en 8 étapes d'un système global d'archivage :
    1. enquête préliminaire ;
    2. analyse des activités ;
    3. identification des exigences archivistiques ;
    4. évaluation des systèmes existants ;
    5. identification de la stratégie pour la satisfaction des exigences ;
    6. conception d'un système d'archivage ;
    7. mise en œuvre ;
    8. contrôle.
- ISO 19005-1 sur le format PDF/A ("A" comme archive), format de conservation des documents ;
- AFNOR NF Z42-013 Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes, révisée fin 2008 ;
- NF Z43-400 Archivage de données électroniques - COM/COLD
- modèle MoReq (Model Requirements for the Management of Electronic Records / Modèle d'exigences pour l'organisation de l'archivage électronique), publié par la Commission Européenne en 2001, révisé en 2008 ;
- série des normes ISO 27000 : Technologies de l'information -- Techniques de sécurité :
    - ISO 27001 : Systèmes de gestion de la sécurité de l'information -- Exigences ;
    - ISO 27002 : Code de bonne pratique pour la gestion de la sécurité de l'information ;
    - ISO 27005 : Gestion du risque en sécurité de l'information ;
    - ISO 27006 : Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information.
- ISO 23081 : Information et documentation -- Processus de gestion des enregistrements – Méta données pour les enregistrements ;
- TRAC (Trustworthy Repositories Audit & Certification) : méthode d'audit des systèmes d'archivages développée par le RLG (Research Libraries Group) et la NARA (National Archives and Records Administration), traduit en France par FedISA (Fédération Européenne de l'ILM du Stockage et de l'Archivage) ;
- ISO TR (technical report) 15801guide pour la conception et l'exploitation d'un système d'archivage ;
- Référentiel « coffre fort électronique » : Il a été élaboré par quatre associations : FNTC (Fédération Nationale des Tiers de Confiance), APROGED (Association des Professionnels de la GED), FedISA (Fédération Européenne de l'ILM du Stockage et de l'Archivage) et l'ADAP (Association pour la Dématérialisation des Achats Publics). La DAF (Direction des Archives de France) et la DGME (Direction Générale pour la Modernisation de l'Etat) y ont également apporté leur concours.

La politique d'archivage (voir focus PA ci-après)

La politique d'archivage est le document qui décrit les objectifs attendus du système d'archivage et l'ensemble des procédures mises en œuvre pour atteindre ces objectifs et garantir la fiabilité du système.

La PA peut être présentée comme l'interface indispensable entre les données avec les exigences légales et réglementaires qui pèsent sur elles et un système d'archivage électronique quel qu'il soit. La PA doit ainsi être capable de transformer ces exigences en différents niveaux de services qu'il faudra ensuite traduire en architecture technique et processus. Ces derniers seront également détaillés dans les déclarations des pratiques d'archivage et dans la mise en œuvre opérationnelle.

La conformité finale de l'archivage en sera ainsi grandement facilitée car pouvant se scinder en deux étapes :

- Etape 1 : Vérification de la conformité de la politique d'archivage aux obligations légales et réglementaires ;
- Etape 2 : Vérification de la conformité du système d'archivage électronique à la PA et aux exigences traduisant les niveaux de service requis.

Ainsi la politique d'archivage et la déclaration des pratiques d'archivage associée décrivent :

- les contraintes juridiques et réglementaires associées à chaque type d'information archivée ;
- les choix structurants qui ont été opérés ;
- les moyens qui permettent d'assurer la traçabilité des opérations et l'intégrité des archives et de façon plus large, la sécurité de l'ensemble du système et du service d'archivage.

La politique d'archivage est une pièce indispensable de la défense de l'entreprise en cas de litige, en ce qu'elle démontre les diligences mises en œuvre pour s'assurer de sa qualité et de sa fiabilité, et qu'elle guide la démarche de l'expert qui serait le cas échéant mandaté pour analyser les aspects techniques du litige. La politique d'archivage doit être régulièrement mise à jour.

Recommandations

On peut distinguer quatre outils méthodologiques majeurs pour un bon système d'archivage que nous décrivons brièvement ci-après :

1. Référentiel de conservation	Il se présente sous forme d'un tableau qui indique pour chaque type ou catégorie de données/documents, les règles de classement et d'archivage : durée de conservation (motivée), droits d'accès,... L'objectif de cet outil consiste à structurer les données et les documents et à les qualifier de manière à permettre leur maintenance et leur exploitation pendant toute la période requise.
2. Politique d'archivage	Il s'agit de l'énoncé par la direction générale des principes directeurs au niveau global de l'entreprise ou de l'organisation (voir focus ci-après).
3. Déclaration des pratiques d'archivage	Permet de préciser comment s'organiser pour répondre aux objectifs et engagements de la PA et ainsi définir les spécifications techniques et identifier les procédures opérationnelles et les moyens mis en œuvre correspondants.
4. Modalités opérationnelles	Correspond à la description détaillée des moyens tant techniques que procéduraux, destinés à la mise en œuvre opérationnelle du système d'archivage.
5. Tableau de bord	Ce tableau s'applique à l'ensemble des données archivées afin de disposer des informations nécessaires à une bonne connaissance globale de son archivage. Un tel tableau de bord doit ainsi permettre à tout moment de vérifier que tel type de données ou de documents existe, que tout ce qui devait être archivé l'a été, où se trouvent les données, si elles ont été détruites,...

Politique d'archivage

Comme nous l'avons déjà évoqué à plusieurs reprises, les objectifs d'un archivage électronique efficace sont multiples. De façon synthétique il s'agit de conserver des données sur le long terme, de les retrouver et de les restituer facilement tout en sécurisant leurs accès. Bien évidemment la durée de conservation, la disponibilité et la sécurité varient en fonction du type de donnée traité. Ainsi plusieurs niveaux de services d'archivage pourront être définis au sein d'une même entité. L'archivage électronique doit donc être vu comme un projet à part entière qui nécessite une étude précise des besoins à court, moyen et long terme ainsi que la prise en compte des besoins métiers. Le projet d'archivage doit être un projet d'entreprise avec une approche et une réflexion globales, validé par la direction générale.

En fonction de ce qui précède, la politique d'archivage apparaît véritablement au cœur du raisonnement et de la méthodologie indispensables afin de mener à bien un projet d'archivage électronique, surtout lorsqu'il s'agit de donner une véritable valeur probante aux informations gérées.

Remarque : Le terme d'« archivage sécurisé » est plutôt réservé au domaine public tandis que « archivage légal » ou encore « archivage à valeur probante » correspond plus au domaine privé. La première politique d'archivage sécurisé pour le domaine public a été établie dès 2005 à l'occasion d'une étude lancée par la DCSSI à laquelle ont également participé la Direction des Archives de France et la DGME (Direction Générale pour la Modernisation de l'Etat). L'ensemble des documents correspondants est disponible sur le site : http://www.ssi.gouv.fr/fr/confiance/archivage.html

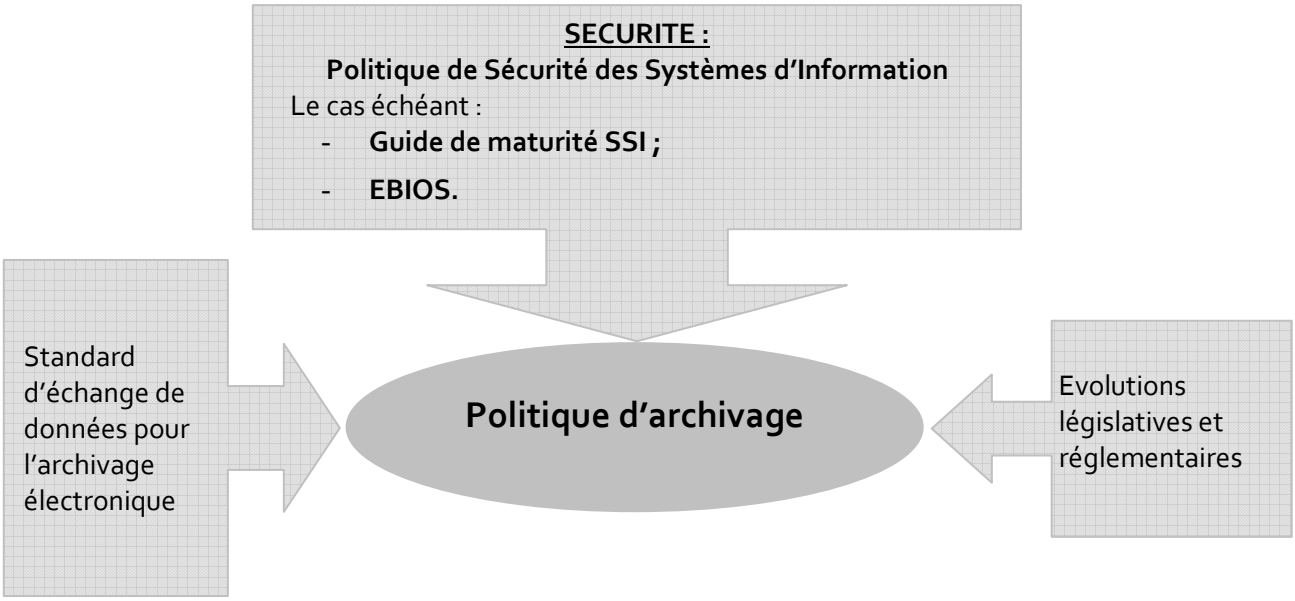
Ainsi pour mettre en place un archivage électronique à valeur probante dont la fiabilité puisse être étayée, il apparaît nécessaire de disposer d'une telle politique d'archivage destinée à décrire l'ensemble des préoccupations liées directement à la problématique de l'archivage électronique tout en tenant compte de l'environnement à la fois légal, réglementaire et sécuritaire.

Une politique d'archivage doit ainsi conduire à :
- Définir les objectifs du système d'archivage électronique en tenant compte de l'environnement sous ses aspects légaux, réglementaires mais également propres à l'entreprise. Il s'agit là des services rendus au client au sens large du terme et qui pourront faire l'objet de différents niveaux largement détaillés ;
- Préciser l'ensemble des intervenants (services producteurs, services versants, usagers, ...) et en définir clairement les obligations et les responsabilités correspondantes ;
- Définir les fonctionnalités mises en œuvre au sein du service d'archivage (versement, stockage, communication-interrogation, administration) et l'organisation fonctionnelle correspondante (liens entre fonctions, flux d'informations, ...) ;
- Présenter l'environnement sécuritaire associé (principes organisationnels, principes de mise en œuvre, principes techniques) en lien avec la politique de sécurité de l'entreprise comme présenté ci-après.

De la sorte, les personnes en charge des archives disposent d'un document posant les règles de base en matière de sécurité pour un archivage électronique à valeur probante. Cette politique d'archivage définit également les contraintes juridiques, fonctionnelles, opérationnelles et techniques à respecter par les différents acteurs afin que l'archivage électronique mis en place puisse être regardé comme fiable. Ce document, en l'absence de textes précisant les critères de fiabilité de l'archivage électronique, permettra le cas échéant, de rapporter devant le juge la preuve de la fiabilité des procédures mises en œuvre et par la même de l'archivage électronique réalisé.

Dans le cadre de la mise en place effective d'un archivage électronique à valeur probante il faut tenir compte de l'environnement dans lequel il va être opéré. A cet égard il s'agira de prendre en considération et de vérifier la cohérence avec :
- le schéma directeur des systèmes d'informations défini ;
- la politique de sécurité adoptée ;
- les technologies utilisées ;
- la structure concernée ;
- les besoins et moyens identifiés.

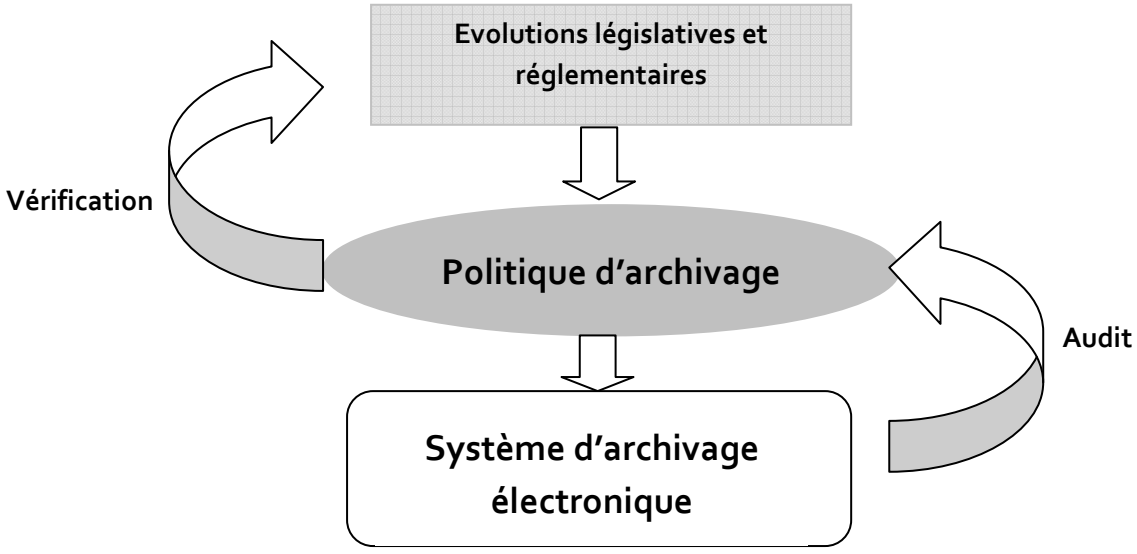
Le schéma ci-après présente une vision synthétique de ces différents environnements qu'il conviendra de prendre en compte.



Une fois la politique d'archivage établie, en découle naturellement un certain nombre d'autres éléments indispensable à la mise en place effective d'un système d'archivage efficient. En effet, à partir du moment où les besoins sont clairement définis on pourra alors facilement en déduire un cahier des charges destiné à pouvoir effectuer des demandes auprès de différents fournisseurs tant de technologies matériel que logiciel, voire de services. La politique d'archivage doit également permettre de bâtir une grille d'audit destinée à vérifier l'adéquation du système mis en place avec les objectifs poursuivis.

La politique d'archivage ne décrivant que les fonctions d'archivage, il faudra également veiller à disposer de documents précisant les moyens mis en œuvre pour réaliser ces fonctions. Ces documents sont constitués à la fois par les « déclarations des pratiques d'archivage » et par la « mise en œuvre opérationnelle » et pourront être élaborés dès l'instant où le système et l'architecture correspondante seront retenus.

Enfin il est important, voire essentiel de pouvoir vérifier régulièrement l'adéquation du système mis en place avec les objectifs de la politique d'archivage, ainsi que la conformité de cette politique par rapport aux nouvelles réglementations ou lois. Le schéma ci-après illustre cette double vérification.



La politique d'archivage apparaît ainsi bien au centre de la méthodologie à mettre en œuvre afin de proposer un service d'archivage électronique véritablement performant, évolutif et parfaitement conforme dans le temps aux exigences légales et réglementaires.

Fiche 5 – Grandes familles de solutions, fonctionnalités

Contexte

En matière de gestion et d'archivage des e-mails, nous avons identifié trois grandes familles de solutions. La première relève d'un fonctionnement manuel, l'utilisateur reste totalement maître mais aussi responsable, de ce qu'il archive. Une deuxième orientation consiste à l'inverse à archiver systématiquement tout ce qui passe par le serveur d'e-mails, tant en entrée qu'en sortie. Enfin la dernière et troisième grande famille correspond à un mixte des deux premières où seule une partie est totalement automatisée tandis que le reste est laissé au bon soin de l'utilisateur.
Le choix parmi ces grandes familles de solution doit se faire de préférence au niveau de la politique d'archivage.

Solution manuelle : l'utilisateur décide de ses archives

Comme indiqué précédemment, l'utilisateur final peut archiver directement les éléments de sa boite aux lettres de façon plus ou moins intégrée. La meilleure solution dans ce cas consiste à disposer d'un bouton spécifique directement à l'intérieur de son logiciel de gestion de mail, Outlook, Lotus ou autre.
Cette solution manuelle permet ainsi aux utilisateurs de contrôler leur archivage et de libérer de l'espace dans leur boite aux lettres à tout moment. Cependant l'efficience d'un tel archivage repose entièrement sur la rigueur des utilisateurs à appliquer les règles qui de toute façon devront être définies au niveau de l'entreprise ou de toute organisation.

Solution Automatique : tout ce qui passe par le serveur est archivé

Ce type d'automatisme doit néanmoins pouvoir s'appliquer en fonction de certains critères comme :
- L'expéditeur du message
- La taille du message
- La date du message
- Le pourcentage du quota atteint d'une boite aux lettres
- Un ensemble de boites aux lettres défini lui-même à partir d'éléments spécifiques concernant un groupe donné d'individus
- Un répertoire à l'intérieur d'une boite aux lettres
- Des mots clés dans l'objet du message
- …

Quelle que soit l'ensemble des critères utilisés, il faudra que la solution permette pour chacun d'eux de définir sa durée de conservation, le niveau de criticité, etc…

Solution mixte : en complément à l'automatisation

En fonction de ce qui précède, il paraît évident que l'automatisation totale ne s'adresse en général pas à l'ensemble des e-mails d'une entreprise. D'où dans la majorité des cas la mise en place d'une solution mixte ayant pour principale conséquence de prendre la meilleure des deux autres approches en laissant à l'utilisateur une part de liberté tout en garantissant les responsables de l'entreprise que les e-mails les plus critiques sont quant à eux systématiquement conservés. Bien sûr la difficulté de ce genre de solution sera de savoir où placer la frontière et dans ce sens choisir une solution qui permette les deux options grâce à un paramétrage approprié.

Enjeux

L'enjeu majeur quant à la solution à adopter consiste à répondre aux obligations telles que largement décrites au cours des fiches précédentes. Ainsi une approche manuelle laisse courir un risque à l'entreprise, directement lié à la discipline de ses employés en matière de respect des règles édictées.

Même si un automatisme complet peut paraître arbitraire et non justifié, il est le seul à pouvoir valablement garantir la conservation de l'ensemble des e-mails dont on pourrait avoir besoin dans le temps. Rappelons ici qu'un e-mail peut servir autant par son contenu que par la représentation de la trace d'un échange à une date donnée entre deux personnes ou deux entités. Il est clair qu'une large majorité d'e-mail ne sera jamais utilisée voire même consultée mais leur conservation entre dans un processus sécuritaire indispensable.
Par ailleurs une automatisation totale peut également procurer un véritable confort vis-à-vis des utilisateurs. En effet, partant du principe que tous les e-mails sont conservés, les utilisateurs

pourront systématiquement détruire l'ensemble de leurs e-mails sur leur poste de travail dans la mesure où ils peuvent y accéder dans une base centralisée.
Attention cependant à respecter les contraintes juridiques, directement liées à un tel automatisme, entre autre afin de respecter la vie privée des individus avec la mise en place de système de gestion des droits d'accès évolutifs et sécurisés.

La solution mixte apparaît comme un très bon compromis sachant que la principale difficulté, telle qu'évoquée précédemment, sera de choisir parmi l'ensemble des e-mails ceux à automatiser totalement en laissant les autres aux soins des utilisateurs. Ces derniers pourront y trouver une certaine contrainte alors même que l'objectif était de leur laisser une certaine liberté !

Grandes fonctionnalités

Toute solution d'archivage d'e-mails doit avant tout répondre à l'objectif principal d'un système d'archivage, à savoir permettre la recherche de contenu. En complément, les solutions proposées pourront également offrir une réduction des coûts de stockage avec une bonne rationalisation d'utilisation des espaces.

Pratiquement toutes les solutions permettent de garder les archives en ligne, de telle sorte que leur accès reste pratiquement transparent pour les utilisateurs.

En résumé, une bonne solution d'archivage d'e-mails devra permettre :
- Un accès aisé au contenu (indexation, moteur de recherche, …) ;
- L'optimisation/rationalisation du stockage (hiérarchisation, compression, …) ;
- Le respect des exigences en matière de conformité ;
- Une meilleure efficacité opérationnelle ;
- Une administration efficace comprenant d'éventuelles migrations ;
- Un environnement sécurisé (contrôle des accès, intégrité, …) ;
- Une conservation pérenne (prévoir d'autres format que celui d'origine comme par exemple HTML, voire PDF/A)
- Le suivi des durées de conservation tout en permettant de suspendre les suppressions en cas d'action en cours ;

Interface utilisateur

En plus de ces fonctionnalités, il est également très important de disposer d'une interface utilisateur offrant un accès aux messages archivés et à leurs contenus aussi transparent et intuitif que possible.

Plusieurs options sont possibles, de celles totalement intégrées dans l'utilitaire de gestion des e-mails à celles totalement dédiées web. Quelle que soit la solution elle devra également offrir une interface de recherche intégrée particulièrement conviviale.

En général une recherche s'effectue en deux temps : indication des principaux critères de recherche puis sélection dans une liste, renvoyée comme répondant aux critères initialement demandés. Les recherches doivent pouvoir s'effectuer aussi bien sur l'entête de l'e-mail que sur son contenu et les pièces jointes. Seules les pièces jointes cryptées ou protégées par mot de passe ne peuvent être indexées.

Une fois l'e-mail retrouvé, les actions possibles correspondent en général à celles dont on dispose de façon traditionnelle à savoir : réponse ou transfert.

Recommandations

Plutôt que de reprendre les différentes fonctionnalités décrites précédemment et qu'il y aura lieu de vérifier scrupuleusement, nous rappelons ci-après les principaux avantages clés à attendre de la mise en place d'une solution d'archivage d'e-mails performante.

1. Elimination des quotas sur les boîtes aux lettres	La gestion automatique des boîtes aux lettres libère l'utilisateur des quotas, sans compromettre la performance et la fiabilité de la messagerie. Les utilisateurs disposent ainsi d'une boîte de réception de taille pratiquement illimitée tout en contrôlant la croissance du nombre de messages stockés.
2. Elimination des risques liés aux fichiers .pst et autres	Les soucis liés aux fichiers de type .pst, .nsf ou autres, et les problèmes de sauvegarde, de sécurité, de stabilité et de stockage inhérents à ces types de fichiers sont éradiqués.
3. Maîtrise des temps de sauvegarde et de restauration	La gestion centralisée du contenu de la messagerie électronique accélère les sauvegardes des serveurs et assure le contrôle des restaurations après incident.
4. Rationalisation des espaces de stockage	Les espaces de stockage des e-mails en ligne sont réduits de 50 à 75 % grâce à l'archivage.
5. Conformité légale et réglementaire	L'archivage assure la récupération du contenu de la messagerie électronique et des documents d'entreprise ou de l'organisation, ce qui permet de satisfaire aux exigences légales et réglementaires de conservation. Une copie de tous les messages électroniques envoyés et reçus est conservée le temps nécessaire pour répondre à ces exigences
6. Meilleure efficacité des bases d'e-mails	Les utilisateurs gardent l'accès à l'ensemble de leur base d'e-mails et peuvent y accéder de façon efficace grâce à des outils de recherche performants.

Fiche 6 – Exemples d'architecture

Contexte

L'architecture la plus courante consiste à installer un ou plusieurs serveurs pour des raisons de sécurité ou d'évolutivité. Ces serveurs sont dédiés à l'archivage et accueille le logiciel gérant les règles issues de la politique d'archivage de l'entreprise. Cependant un composant logiciel peut être également installé sur les postes des utilisateurs dans le cas de l'utilisation d'un client lourd. Ce dernier permet ainsi de rendre totalement transparent le fait que les e-mails ont été archivés et d'automatiser leur rapatriement depuis les archives.

Les serveurs d'archivage jouent un rôle essentiel en matière de pilotage des flux d'archivage et de restauration. Surtout ils permettent de ne pas surcharger les serveurs de messagerie. La communication entre serveur d'archivage et serveurs/clients de messagerie est généralement réalisée via des API (application program interface) standards disponibles pour les produits de messagerie utilisés. Derrière ces serveurs d'archivage, on installe la partie stockage sécurisée permettant de conserver les données archivées. Bien qu'il soit en théorie possible de conserver les archives sur du disque local aux serveurs d'archivages, une bonne pratique consiste à déporter ces archives sur un stockage sécurisé, indépendant des serveurs. Ceci permet de sécuriser le stockage de façon indépendante, possibilité de sauvegarder et/ou de répliquer les archives sur un site de secours, voire y accéder directement sans obligatoirement passer par les serveurs applicatifs. Ce stockage centralisé facilite également la reprise en cas d'incident au niveau des serveurs applicatifs ou d'archivage : la disponibilité des données est indépendante de celle des serveurs.

Aujourd'hui, le rapport performance/prix/sécurité des disques magnétiques permet d'envisager des solutions de stockage basées sur des technologies de type WORM logique (voir focus fiche 9) construites à partir de disques durs. Cette fonction de WORM logique peut dans certains cas être pilotée directement par le logiciel d'archivage utilisé permettant également de définir les durées de conservation des archives.

Certaines solutions de stockage comme celles de NetApp sont suffisamment polyvalentes pour supporter différents types de disques, rapides (FC ou SAS) et lents (SATA), ainsi que tous les protocoles d'accès du marché (FC, iSCSI, NFS, CIFS). De ce fait une seule et unique baie peut éventuellement héberger les données primaires nécessaires à la messagerie (information store d'Exchange ou bases de Domino), les archives des e-mails, ainsi que les méta données nécessaires au logiciel d'archivage. Il est également possible de répartir ces données sur différents systèmes, en fonction de la taille ou des exigences du projet. Le fait d'utiliser une baie unique permet de consolider le stockage et la sauvegarde en un seul point d'où une réduction des coûts, y compris des coûts cachés.

Enjeux

Les enjeux principaux concernant l'architecture destinée à héberger les archives d'e-mails sont les suivants :

- Durabilité (sécurité & fiabilité): les messages archivés doivent être conservés et pouvoir être retrouvés pendant toute la durée de conservation requise, voire sans limitation. Le support de stockage hébergeant les archives doit donc être muni de fonctionnalités de protection contre tout type de panne, et ceci à tous les niveaux, logiciels, matériels et site.

- Intégrité : le contenu des messages archivés ne doit pas pouvoir être altéré. Cependant une modification du codage du format propriétaire de la messagerie vers un format plus pérenne est tout à fait possible en ayant soin toutefois de ne pas modifier le sens du message.

- Disponibilité (performance) : les messages archivés, extraits du système de messagerie de production, doivent rester faciles d'accès pour les utilisateurs finaux. Non seulement en période normale d'utilisation du service, mais aussi, et surtout, en période d'audit ou de nécessité de produire une justification dans un délai imposé (généralement court). L'accès aux archives doit ainsi être possible à tout moment selon un degré de performance dépendant directement des besoins de l'entreprise.

- Evolutivité : les volumétries à traiter augmentent régulièrement et les technologies

de stockage évoluent également rapidement. Le système de conservation des archives d'e-mails doit donc permettre une montée en charge en termes de capacité gérée, de nombres d'utilisateurs, mais aussi anticiper le support des technologies de stockage ou de réseau à venir.

- Pérennité : nous en revenons au paradoxe de l'archivage électronique qui consiste à devoir conserver des données pendant de longues durées en s'appuyant sur des technologies rapidement obsolètes. Si l'on considère des durées de conservation de plus de 5 ans, il est d'ores et déjà admis qu'il faudra migrer les archives électroniques vers un nouveau média, et ce régulièrement. La pérennité n'est donc pas garantie par le système de stockage en lui-même, mais pas son habilité à pouvoir facilement être migré. Il convient donc de retenir une solution la moins propriétaire et la plus ouverte possible en utilisant des briques de bases standards tant au niveau du formats de codage que des protocole normalisés, …

- Compatibilité : Cet enjeu est parfois oublié lors de projets d'archivage « tactiques » menés trop rapidement. Le système d'archivage des e-mails retenus doit bien évidemment être compatible avec les solutions actuelles du système d'information (systèmes d'exploitations, logiciel de messagerie, réseau…) mais aussi avec les solutions futures… Il doit idéalement pouvoir demeurer compatible si la messagerie X devait être remplacée par la messagerie Y ou lors d'un changement de système, passage d'Unix à Windows ou de Windows à Linux. La compatibilité d'une partie de la solution pour archiver des données provenant d'autres applications de l'entreprise, peut également être un avantage (notamment au niveau financier)

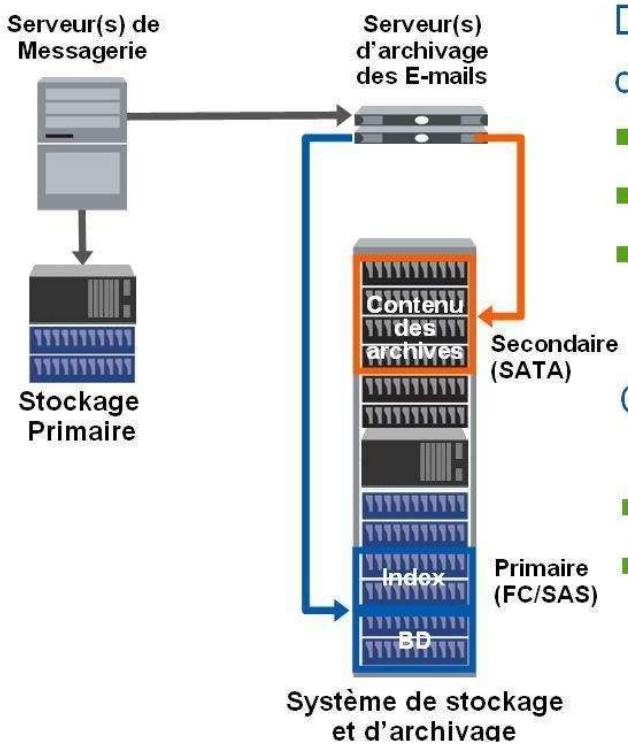
- Confidentialité : il va de soi que les e-mails archivés ne doivent être accessibles que pour les personnes autorisées (l'émetteur, les destinataires du message, auditeur, …) et doivent satisfaire aux mêmes considérations de confidentialité que les e-mails non archivés, tout en permettant une recherche et un accès en cas d'audit ou de nécessité de justification.

- Conformité légale et réglementaire: cet enjeu n'a pas la même importance suivant le secteur d'activités de l'entreprise ou de l'organisation. Les réglementations ne sont évidemment pas les mêmes pour une activité de bourse d'une grande institution financière et pour un service de support après ventes d'une enseigne commerciale. Il est essentiel de respecter l'ensemble des critères exigés par la loi et les réglementations en vigueur, sous peine de disposer d'un magnifique système d'archivage électronique gérant des données qui ne serviront à rien !

- Coût : n'oublions pas cet enjeu sans lequel, aucun projet de ce genre ne serait possible. La solution retenue doit pouvoir répondre aux enjeux précédents dans un budget de mise en oeuvre et de maintien en condition opérationnelle raisonnable. Il est recommandé d'étudier en détails tous les coûts de la solution (achat/maintenance, matériel/logiciel), même les coûts dits « cachés » (administration par exemple), afin de pouvoir déterminer le coût total de possession (TCO) et, d'anticiper dans la mesure du possible, un retour sur investissement (ROI) permettant aux Directions Générales de donner plus facilement leur accord au projet d'archivage d'e-mails.

Exemples d'architectures

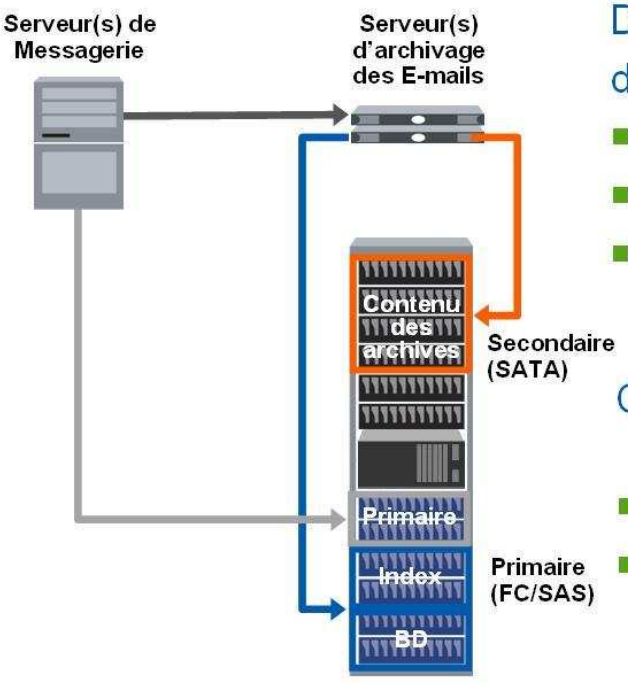
Nous donnons ci-après deux exemples d'architecture classiques. Le premier exemple reflète une situation où les données primaires (gérées directement par le serveur de messagerie) sont séparées des données d'archives :



Données du système d'archivage
- Contenu des archives
- Base de données
- Indexes plein-texte

Composant du système d'archivage
- Serveur(s) d'archivage
- Stockage sécurisé

Le second exemple représente une consolidation des données primaires et des données d'archives sur le même système de stockage (les postes clients ne sont pas figurés) :



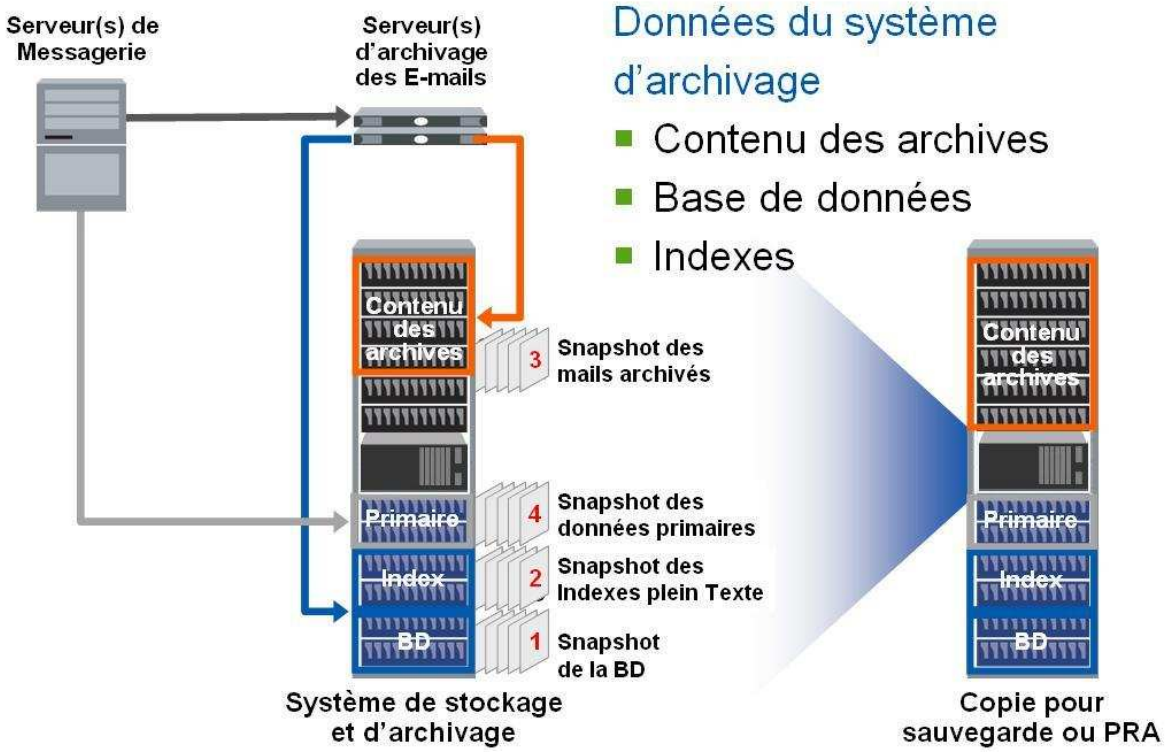
Données du système d'archivage
- Contenu des archives
- Base de données
- Indexes plein-texte

Composant du système d'archivage
- Serveur(s) d'archivage
- Stockage sécurisé

Une bonne solution d'archivage doit permettre d'accéder rapidement aux données de gestion et aux données primaires d'où l'utilisation de protocoles en mode blocs de type FCP ou iSCSI. En revanche les e-mails archivés peuvent être interrogés via des protocoles en mode fichiers tel CIFS pour Windows ou NFS pour Unix. Ces protocoles représentent des standards de l'industrie et offrent donc une véritable garantie de pérennité aux archives dans la mesure où il est possible d'y accéder au besoin sans passer par le serveur d'archivage. Ainsi en cas de disparition de la société fournissant le logiciel d'archivage, les données restent néanmoins accessibles et peuvent donc aisément être migrées vers un nouveau logiciel.

Les aspects sécurisation seront traités en détails dans la fiche 9, néanmoins le fait de centraliser les archives dans un système de stockage découplé des serveurs permet d'utiliser des solutions de réplication ou de sauvegarde disque à disque fournies au niveau de la baie.

Le schéma ci-après montre une organisation sécurisée par une logique de réplication des données secondaires :



Recommandations

Nous donnons ci-dessous la liste les critères essentiels à retenir lors du choix d'une architecture technique répondant aux enjeux de l'archivage des e-mails, tels que décrits précédemment.

1. Fiabilité	Le système retenu doit protéger le transfert et la conservation des données lors de la chaîne d'acquisition et dans la durée. Plus nombreux et fiables sont les systèmes de protection, meilleure sera la fiabilité. On peut citer comme exemple de mécanismes de protection : des caches en écritures redondés et sécurisés sur batterie, des checksums disques, une protection RAID contre les pannes disques multiples, une solution de réplication…
2. Ouverture	Plus la solution retenue sera ouverte et modulaire, meilleure sera sa pérennité dans le temps. On s'attachera à retenir un socle technique permettant des accès standards aux données, facile à migrer (du fait de l'obsolescence inéluctable des technologies) et compatible avec les applications d'aujourd'hui et de demain…
3. Evolutivité	Le système retenu doit pouvoir héberger les volumes en termes de capacité (en Tera, Peta octets) et de nombre d'objets (en millions ou milliards) envisagés pour la durée de conservation des e-mails archivés, mais aussi pouvoir répondre à l'imprévu. Il n'est pas rare en effet de sous-estimer le nombre et le volume des archives; la tendance étant en outre de plus en plus au tout numérique (après les documents, le contenu multimédia : sons, conversations, images, photos, vidéos…). Plus le système de conservation des archives sera évolutif en capacité et performance, meilleure sera la garantie d'évolutivité du système d'archivage.

4. Disponibilité	On prendra soin de choisir une solution permettant de se prémunir au maximum contre toute panne matérielle ou logicielle élémentaire, avec la redondance permettant en cas d'incident de maintenir l'accès aux e-mails archivés. Une solution de reprise d'activités peut également être envisagée. Dans ce cas, on s'attachera à vérifier que les données répliquées sur le site de secours conservent bien tous les attributs de conformité d'une archive (surtout en cas d'archivage légal), et que la bascule sur le site de secours se fasse, si ce n'est de façon transparente, au moins de la façon la plus simple et rapide possible.
5. Performance	Cet aspect est parfois négligé sous prétexte que les archives ne sont pas aussi importantes que les données au quotidien. Ce serait une erreur de ne pas garder à l'esprit ce facteur essentiel à cause de trois points principaux : - Premièrement, l'explosion des contenus électroniques en général et de l'e-mail en particulier doit être gérée également au niveau du système d'archivage qui doit pouvoir être alimenté à une vitesse ne freinant pas les performances de la messagerie elle-même ; - Deuxièmement, une réindexation du contenu archivé s'avère parfois nécessaire en fonction des contraintes métiers. Elle doit évidemment pouvoir être rapide et ne pas durer des semaines ; - Troisièmement, le e-discovery. Rappelons qu'en cas d'audit il est nécessaire de produire une preuve rapidement, et même avec une indexation performantes et à jour, cela peut s'avérer trop long si l'on ne dispose pas d'accès et de traitement rapide. On s'attachera donc à ne pas négliger cet aspect performance et à bien se renseigner sur les capacités d'alimentation, d'indexation et de réindexation, et enfin de rapidité de recherche des solutions étudiées avant d'en retenir une.
6. Conformité	Si votre secteur d'activité impose des contraintes additionnelles strictes sur les archives des e-mails, telles que traçabilité, inaltérabilité (mode WORM), confidentialité, il convient de vérifier que la solution retenue satisfait bien à ces exigences dans son ensemble, et pas seulement au niveau du logiciel d'archivage ou du système de stockage des archives, sans oublier de prendre en compte les aspects humains (procédures, administration, maintenance, …).
7. Coûts	L'ensemble des coûts doit pouvoir être connu à l'avance. Non seulement les acquisitions des différentes briques logicielles et matérielles, les éventuels coûts d'intégration le cas échéant, mais aussi les coûts de maintenance et de maintien en condition opérationnelle, sur la durée la plus longue possible (au moins 5 ans ; la plupart des éditeurs et constructeurs ne communiquant pas systématiquement leurs coûts de maintenance au-delà de 3 ans…). Il ne faut pas oublier les coûts cachés (administration notamment, sauvegardes/restaurations, indisponibilités). C'est également une recommandation importante que de valider la facilité de migration de tout ou partie de la solution (logiciel ? matériel ? brique de stockage) vers un nouveau système, et d'en estimer les coûts afin de ne pas avoir de mauvaise surprise le moment venu.

Fiche 7 – Tiers archiveur

Contexte

Il existe quelques risques afférents à l'archivage interne (effectué au sein même de l'entreprise) en matière de preuve. La Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) donne deux raisons pour lesquelles l'archivage externe est préférable :

- la mutualisation et donc le partage des coûts ;
- le professionnalisme de la solution, gage supplémentaire de la force probante des éléments archivés.

En effet, le recours à un tiers archiveur peut permettre de pallier les effets du principe de l'article 1315 du Code civil selon lequel nul ne peut se pré constituer de preuve par soi-même.

Toutefois, l'externalisation n'est pas toujours autorisée. Dans le secteur privé, il n'existe aucune restriction légale. Dans le secteur public, l'externalisation est réglementée par le décret du 3 décembre 1979 et n'est possible que pour les archives intermédiaires et définitives mais uniquement dans des dépôts d'archives relevant de la direction des Archives de France.
La notion de tiers archiveur n'est définie par aucun texte. La DCSSI le définit comme la personne physique ou morale en charge, pour le compte de tiers, de la réception, de la conservation et de la restitution de documents électroniques dont il doit garantir l'intégrité.

La loi Belge du 15 mai 2007 fixant un cadre juridique pour certains prestataires de confiance définit le prestataire de service d'archivage électronique comme toute personne physique ou morale qui offre un service de conservation de données électroniques, normalement contre rémunération et à la demande d'un destinataire du service, la conservation de ces données électroniques étant un élément essentiel du service offert.
L'intérêt se fait de plus en plus grand pour l'externalisation de l'archivage et en particulier auprès de sociétés privées. La loi du 15 juillet 2008 réglemente cette activité pour les archives publiques.

Enjeux

Dans le secteur privé, en l'absence de cadre légal, des exigences contractuelles ont été développées tenant compte des principes applicables en matière d'archivage: fidélité, durabilité, intégrité, identification.

La loi du 15 juillet 2008 relative aux archives publiques, encadre l'archivage par des prestataires privés que la circulaire du 16 janvier 1997 et du 2 novembre 2001 réglementaient à titre exceptionnel.

Le nouvel article L. 212-4 II du Code du patrimoine prévoit que les personnes soumises à la réglementation relative aux archives publiques peuvent, après en avoir fait la déclaration à l'administration des archives, déposer tout ou partie des documents qui n'ont pas fait l'objet d'une sélection, c'est-à-dire les archives courantes et intermédiaires, auprès de personnes physiques ou morales agréées à cet effet par ladite administration.

La conservation est toutefois assurée sous le contrôle scientifique et technique de l'administration des archives.

Le tiers archiveur agit pour le compte du client et en son nom en tenant compte de la spécificité du support technologique utilisé. On est donc en présence d'un mandat soumis à l'article 1984 et s. du Code civil, et d'un contrat de dépôt soumis aux articles 1927 à 1946 du Code civil.

Dans un environnement informatique, on a fréquemment recours à un prestataire ASP (Application Service Provider), en français FAH (Fournisseur d'Applications Hébergées), ou SaaS (Software as a Service). Le concept ASP prend la forme d'une mise à disposition de programmes informatiques et de services auxquels l'entreprise peut accéder à distance (via internet ou un VPN (Virtual Private Network), en français RPV (Réseaux Privés Virtuels)), moyennant le versement d'une redevance. Ce modèle ASP est amené à se développer en matière d'archivage.

L'obligation qui pèse sur le tiers archiveur est en général une obligation de moyens mais elle peut être plus lourde en fonction de la qualification prévue pour celle-ci dans le contrat. L'intérêt de prévoir une obligation de résultat est que dans ce cas la faute est présumée et la charge de la preuve

repose sur le tiers archiveur qui doit démontrer la force majeure, le fait du tiers ou le fait du client pour s'exonérer de sa responsabilité.

Le tiers archiveur est susceptible de voir sa responsabilité engagée sur le plan civil. Pour engager la responsabilité civile contractuelle de l'archiveur, le client doit prouver l'existence des trois éléments suivants :

- une faute : c'est-à-dire un manquement à une obligation contractuelle ;
- un préjudice : celui-ci pourra être constitué par la perte ou encore l'altération d'un document. Les dommages dits « indirects » (les pertes d'exploitation par exemple) sont en général exclus ;
- un lien de causalité entre la faute et le préjudice sachant que le tiers archiveur n'est pas responsable du contenu des documents archivés et notamment de leur authenticité.

En raison du risque pénal lié à la loi du 6 janvier 1978 relative à l'Informatique et aux libertés, le contrat d'archivage devra comporter les dispositions suivantes :

- identifier le responsable du traitement, défini comme la personne qui détermine les finalités et les moyens du traitement (en principe, l'entreprise ou l'organisation, cliente du tiers archiveur) ;
- convenir que le responsable du traitement garantit avoir accompli les formalités préalables requises par la loi Informatique et libertés ;
- préciser que le tiers archiveur ne peut agir que sur instruction expresse du responsable du traitement ;
- s'assurer que le tiers archiveur présente des garanties suffisantes pour assurer la sécurité et la confidentialité des données ;
- préciser quelles sont les mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité et la confidentialité des données.

Par ailleurs, dans l'hypothèse où le tiers archiveur serait établi dans un pays tiers à l'Union Européenne et n'offrant pas un niveau de protection adéquat, qu'il s'agisse d'ailleurs d'un tiers archiveur externe à la société ou d'une société apparentée, il convient :

- en cas de prestataire externe, de conclure une convention de flux transfrontières de données selon le modèle de convention de la Commission européenne organisant les relations entre le responsable du traitement et le sous-traitant (http://www.cnil.fr/index.php?id=2409);
- en cas de société apparentée, de conclure une convention de flux transfrontières de données selon le modèle de convention de la Commission Européenne organisant les relations entre deux responsables de traitement (http://www.cnil.fr/index.php?id=2409).

Recommandations

Les principales exigences que devra comporter le contrat avec le tiers archiveur sont regroupées ci-dessous :

1. Généralités relatives à l'archivage	Le prestataire assure le stockage, la conservation, la consultation et la communication des documents.
2. Politique d'archivage	Le prestataire reconnaît avoir pris connaissance de la politique d'archivage du Client ; en particulier, il déclare avoir pris connaissance de la finalité probatoire de celle-ci. Il déclare et garantit que la solution d'archivage objet du contrat est conforme à cette politique d'archivage
3. Mise en œuvre/recette	Le prestataire assure les prestations nécessaires à la mise en œuvre de la solution d'archivage électronique. La prestation de mise en œuvre fait l'objet d'une procédure de recette.
4. Services récurrents	Le prestataire assure des services récurrents d'administration, d'exploitation, de maintenance matérielle et logicielle, corrective et évolutive, de la plate-forme d'archivage, outre l'accès aux documents par le client
5. Obligation de conseil	Le prestataire est débiteur d'une obligation d'information, de conseil et de mise en garde renforcée
6. Autorisations	Le prestataire garantit avoir les autorisations légales nécessaires à l'exécution des prestations

7. Cryptologie	Le prestataire garantit ne recourir qu'à des moyens de cryptologie conformes à la législation en vigueur
8. Robustesse	Le prestataire garantit la robustesse de son système d'archivage, c'est-à-dire l'utilisation préalable du système par plusieurs utilisateurs (sous forme d'un pilote et en exploitation réelle) avant toute mise à disposition du client
9. Traçabilité	Le prestataire garantit que le système qu'il met en place est capable d'assurer la traçabilité et l'horodatage de toutes les opérations effectuées, que ce soit dans le cadre d'un usage normal (maintenance) ou anormal (fraude, malveillance, accident) du système et ce, de manière irréversible.
10. Evolutions	Le prestataire s'engage à adapter le système d'archivage aux évolutions juridiques, normatives et à l'état de l'art Le prestataire décrit de manière détaillée les modalités de modification du service et doit solliciter l'accord préalable écrit du client
11. Portabilité	Le prestataire garantit que les standards et formats utilisés sont ceux généralement préconisés par les normes et, à défaut, conformes à l'état de l'art
12. Propriété intellectuelle	La mise à disposition des documents au prestataire ne confère aucun droit d'usage ou une quelconque licence au prestataire sur les droits de propriété intellectuelle y afférents
13. Engagements de qualité de service/pénalités	Engagement général de forte réactivité. Garantie de disponibilité du système (maintenance comprise) Garantie de temps de rétablissement Garantie de temps d'intervention Pénalités à caractère non compensatoire et non libératoires
14. Maintenance	Les périodes d'indisponibilité pour cause de maintenance font l'objet d'une communication préalable
15. Normes	Le prestataire garantit la conformité aux normes applicables ainsi qu'à l'état de l'art.
16. Compatibilité	Le prestataire garantit la compatibilité de sa solution d'archivage électronique avec le SI du client
17. Politique de sécurité	Le prestataire garantit être conforme aux normes applicables en matière de sécurité de l'information (ISO/CEI 27001).
18. Accès distant	Le prestataire garantit l'accès permanent et sécurisé aux documents par le seul client par un mécanisme d'authentification forte
19. Informatique et libertés	Engagement du prestataire de n'agir que sur instruction expresse du responsable du traitement. Le prestataire garantit le respect de la sécurité et de la confidentialité des données. Il en garantit le respect par ses salariés intervenants et tiers sous-traitants éventuels. Les mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité et la confidentialité des données sont décrites. Le prestataire s'engage à ne communiquer les documents archivés qu'aux destinataires définis par le client, y compris à l'expiration du contrat. Engagement de respecter le caractère totalement sécurisé et pérenne de la solution d'archivage. Le prestataire déclare et garantit que la solution qu'il propose permet de prendre en compte le droit de rectification sans remise en cause de la valeur probante des documents La destruction éventuelle des documents ne peut être réalisée que sous le contrôle exclusif du client, selon une procédure d'authentification forte avec une traçabilité assurée.
20. Réversibilité	Engagement du prestataire quant à la réversibilité de la prestation
21. Responsabilité / Assurance	Obligation de résultat pour l'ensemble des engagements. Indemnisation des dommages directs sans pré-qualification des dommages

	indirects tels que perte de bénéfices, perte de clientèle, perte de marché. Absence de pré-qualification des cas de force majeure. Garantie par le prestataire de la souscription d'une assurance responsabilité civile professionnelle
22. Résiliation	En cas de manquement du prestataire à l'une quelconque de ces obligations, le client dispose de la faculté de résilier le contrat sans formalités judiciaire préalable. Le prestataire n'est libéré de ses obligations que sous réserve de la parfaite exécution du contrat, en particulier de la clause de réversibilité
23. Audit	Droit de pouvoir auditer ou faire auditer par un tiers les conditions d'exécution des contrats, et notamment la sécurité physique et logique de la solution d'archivage, la procédure de réversibilité
24. Restitution	En toutes circonstances, le prestataire garantit la restitution des données à première demande du client
25. Confidentialité	Le prestataire s'engage à observer la plus stricte confidentialité sur l'existence du contrat de tiers archivage et l'identité du client
26. Cession du contrat/changement de contrôle	Le contrat ne peut faire l'objet d'une cession par le Prestataire sans l'accord préalable du Client En cas de changement de contrôle, le client pourra résilier le contrat sans pénalités, ni indemnité
27. Sous-traitance	Les prestations ne peuvent être sous traitées sans l'accord exprès du client
28. Archives publiques	- agrément du prestataire - déclaration du dépôt - contrôle scientifique et technique de l'administration des archives

Fiche 8 – Risques et assurances

Contexte

Si fiable soit le système mis en place, un dysfonctionnement reste toujours possible et peut provoquer de graves préjudices pour l'entreprise ou l'organisation utilisatrice. Seule la question de l'assurance peut permettre de répondre à une telle situation. La perte d'informations constitue un risque vraisemblable et souvent peu pris en compte dans le cadre des systèmes d'information. Le système d'archivage, qu'il soit interne ou externe, devra donc être analysé pour déterminer l'impact de tout dysfonctionnement.

Le management des risques est lui-même confronté à une profonde évolution en parallèle au développement de l'économie numérique. En effet nous sommes en train de passer :

- Des architectures fermées aux architectures ouvertes ;
- Du calcul probabiliste des causes à l'approche déterministe de hiérarchisation des impacts ;
- D'une approche sauvegarde des données au cycle de vie des informations ;
- D'une responsabilité pour faute à un défaut de conformité à la norme ;
- D'une quantification des pertes assise sur le matériel à une sinistralité immatérielle.

Par ailleurs les risques sont d'origines multiples et il est essentiel de les identifier tant en regard de leurs éventualités que de leurs conséquences :

- Méthodologiques, directement liés à la gestion du projet quel qu'il soit ;
- Techniques dont la principale conséquence en est la perte d'information ;
- Environnementaux avec la destruction totale ou partielle de sites ;
- Sécuritaires (confidentialité, intégrité, …)
- Juridiques (document non recevable)

Il est donc indispensable d'avoir une évaluation précise des risques, effectuée à partir d'un « *audit des risques informatiques* » en utilisant une méthode adaptée. Certains courtiers ou compagnies d'assurance proposent également leur propre système d'évaluation des risques comme par exemple le « Netscoring » mis en place par MARSH.
L'on rejoint ici la nécessité de définir une véritable stratégie d'archivage de l'entreprise que l'on doit retrouver, au moins pour partie, dans la politique d'archivage. Il est en effet fondamental d'anticiper les conséquences de la non disponibilité de l'information, aussi bien dans un environnement réglementaire ou juridique, que dans le cadre d'une gestion saine du patrimoine informationnel de toute organisation.

La stratégie d'archivage doit ainsi être globale et :

- adaptée aux besoins de l'entreprise ou de l'organisation : si elle est sous dimensionnée, les besoins fondamentaux de restitution de l'information risquent de ne pas être satisfaits ; si elle est surdimensionnée, elle sera trop contraignante pour les utilisateurs et trop coûteuse ; de même les enjeux sont différents selon les activités de l'entreprise ou de l'organisation, son ancienneté, la taille et le flux des données et leur criticité ;
- cohérente avec la politique générale de l'entreprise ou de l'organisation: une politique de sécurité très rigoureuse ou une démarche qualité très poussée ne peuvent donner tous leurs fruits sans une politique d'archivage de même niveau ; si l'entreprise ou l'organisation a un système de gestion des connaissances très développé, il est logique d'avoir un système d'archivage en conséquence pour pérenniser ses connaissances.

Enjeux

Pour un archivage en interne

Au sein d'une organisation publique ou privée, la perte de données est tout à fait possible suite à des erreurs de saisie, de transmission, d'une mauvaise utilisation, d'erreurs d'exploitation et/ou de manipulation du système ou des supports. La question à se poser est ainsi de savoir dans quelle mesure les polices d'assurances couvrent ce type de dommages immatériels indirects.
Ces derniers sont en général garantis par un contrat spécifique appelé « *extension des risques informatiques* ». En effet, une simple « *assurance bureautique* », visant à couvrir les pertes matérielles directes (destruction, détérioration, incendie, explosion, dégât des eaux…) subies par l'assuré ne jouera pas dans le cadre d'une perte de données. Il convient donc de faire particulièrement attention au choix de la police d'assurance, en prenant garde de bien préciser dans quelle mesure les dommages

immatériels indirects sont pris en compte dans le contrat.

Archivage par un tiers

Dans le domaine des prestations informatiques de tiers archivage, plusieurs assurances semblent particulièrement adaptées :

- l'assurance responsabilité civile professionnelle couvre les dommages que peut subir le client dans le cadre de l'exécution d'un contrat de prestations de services à la suite d'une faute commise par le tiers archiveur (voir fiche 7 Tiers archiveur) ;
- l'assurance de responsabilité du Syntec informatique (Chambre syndicale des SSII et des éditeurs de logiciels) est destinée aux sociétés de services informatiques adhérentes. Cette assurance correspond bien à la problématique de l'archivage dans la mesure où elle prend en compte les dommages causés aux matériels et documents divers nécessaires à l'activité de l'assuré qui lui sont confiés pour exercer son activité professionnelle. Sont notamment garantis les dommages qui sont la conséquence directe d'une faute de manipulation des préposés de l'assuré ;
- l'assurance dommages pour compte est contractée par le tiers archiveur pour couvrir l'ensemble de ses clients en cas de perte de tout ou partie de données archivées. Dans la mesure où le tiers archiveur ne parvient pas à restituer un document archivé, l'assureur indemnise automatiquement le client, sans que ce dernier ait à établir une faute à l'encontre du tiers archiveur. Il faut cependant que le préjudice soit qualifiable et quantifiable. Un plafond est également prévu ;
- l'assurance frais supplémentaires correspond enfin à une assurance complémentaire que le client peut contracter en vue de bénéficier d'une meilleure protection en cas de sinistre. Le montant de la prime sera évidemment lié à l'évaluation des risques, faite par un auditeur qui examinera le système d'archivage du tiers qui assure le service.

L'enjeu est important dans la mesure où en ce qui concerne l'archivage d'e-mails, la perte de données pourrait causer de graves conséquences pour l'entreprise du fait même de la perte d'un élément de preuve amené à être utilisée en justice ou au cours d'un contrôle fiscal.

Des contrats permettent de se couvrir contre de tels risques, il s'agit en l'occurrence de perte d'exploitation informatique ou de contrat de type tout risque sauf. En principe dans ce dernier cas, l'entreprise est assurée pour toutes causes sauf trois : risque atomique, guerre civile et internationale, sabotage direct du mandataire social.

Recommandations

1. Audit indispensable	Un audit des risques informatiques est incontournable aux fins de choisir la police d'assurance la mieux adaptée.
2. Autres risques en regard des obligations légales et réglementaires	L'audit « technique » doit être complété par l'identification des contraintes légales et réglementaires afin d'évaluer les risques qu'il y a à archiver ou à ne pas archiver. Il y aura également lieu d'analyser les incidents qui ont pu avoir lieu en lien avec des dysfonctionnements d'archivage : données perdues, données indûment détruites, données confidentielles divulguées, document introuvable car non indexé ou mal décrit, données anciennes illisibles, etc. L'ensemble de ces informations doit permettre d'enrichir la politique d'archivage.
3. Assurance interne de perte de données	La perte de données en interne doit faire l'objet d'une assurance particulière, car elle n'a pas vocation à être couverte par les polices généralistes.
4. Assurance du tiers	La responsabilité vis-à-vis des tiers, enjeu particulièrement important dans le cadre de l'archivage, doit être, elle aussi, couverte par une police d'assurance spéciale. Rappelons que le client reste en effet le seul responsable de la non production de ses données en cas de dysfonctionnement.
5. Valeur de l'information	Il faudra également être attentif au fait que dans le cadre d'un service de tiers archivage, le client voudra connaître au préalable le montant de son indemnisation en cas de sinistre de son prestataire. Savoir à ce niveau que des assurances spécifiques existent permettant de couvrir la valeur désirée par le client, voir l'exemple cité de l'assurance frais supplémentaires.

Fiche 9 – Sécurité

Contexte

La notion de sécurité est désormais omniprésente en matière informatique et l'e-mail n'échappe pas à la règle. Par contre cette sécurité peut revêtir des aspects tant techniques que juridiques voire organisationnels. Afin de véritablement sécuriser un document pour qu'il soit par exemple recevable comme élément de preuve, qu'il s'agisse ou non d'un e-mail, il est nécessaire de prendre en compte l'ensemble de son cycle de vie, depuis sa création jusqu'à sa destruction. Or nous nous intéressons dans ce document essentiellement à la partie archivage électronique de l'e-mail et nous allons donc être obligé de déroger quelque peu à la règle afin d'apporter toutes les précisions utiles. Ainsi nous traiterons à la fois de la façon de sécuriser un e-mail, en tant que message et ensuite nous aborderons au niveau des recommandations comment garantir sa sécurité dans le temps en appliquant les règles concernant l'archivage électronique en général.

Enjeux

Les principaux enjeux sécuritaires de l'e-mail concernent la non remise en cause d'un message envoyé et/ou reçu ainsi que la garantie de l'identité de son auteur et de l'intégrité de son contenu, protégé par ailleurs de tout code malicieux. Dans certains cas on pourra également s'intéresser à la confidentialité de l'information véhiculée. Quoiqu'il en soit une très large majorité des éléments de réponse passe par l'utilisation de la signature électronique (voir focus fiche 3 A propos de la signature électronique).

Rappelons que la signature électronique constitue un procédé d'identification de l'auteur d'un document électronique et qu'elle garantie de plus l'intégrité de ce document. Pour être apposée, la signature électronique nécessite un certificat électronique qui correspond à un fichier numérique permettant de valider le lien entre une signature électronique et son signataire, personne physique ou morale. La signature électronique constitue en fait pour les entreprises un moyen fiable d'assurer la sécurité de leurs échanges sur internet ou tout autre support de communication sous réserve de respecter certaines règles essentielles.

Nous pouvons également ajouter à ces enjeux une notion importante que constitue la facilité d'utilisation de l'outil ainsi que sa disponibilité. En effet plusieurs solutions existent à ce jour permettant de fiabiliser les échanges dont certains ont recours à des services web qui obligent l'utilisateur à changer de son environnement de travail traditionnel, lui procurant ainsi certaines contraintes qui auront pour effet de l'empêcher d'utiliser plus régulièrement l'outil, si performant soit-il par ailleurs. Enfin il ne faudra pas négliger l'aspect des performances dans la mesure où la sécurité ne doit pas être synonyme de « perte » de temps. Les logiciels de sécurité nécessitent en général plus de temps que pour des traitements courants et il faut donc veiller à limiter au maximum de tels dépassements.

E-mail sécurisé

Signature d'un e-mail :

La signature d'un e-mail permet d'authentifier l'identité de l'émetteur du message et garantit que le message et ses pièces jointes n'ont pas été altérés entre le moment où ils ont été émis et le moment où ils ont été ouverts par le destinataire.

Le principe de signature d'un e-mail est relativement simple lorsqu'il est basé sur une infrastructure de messagerie traditionnelle. Les utilisateurs doivent par contre être munis de certificats sur leur poste de travail. Ces certificats doivent également être publiés dans l'annuaire de messagerie.

Le déroulement de l'opération d'émission de l'e-mail consiste pour l'émetteur à préparer son message, puis à le signer à l'intérieur de son outil de messagerie à l'aide de sa clé privée et enfin à l'envoyer à son destinataire. Ce dernier reçoit alors le message, l'ouvre et vérifie la signature de l'émetteur à la fois sous l'angle de son identité grâce au certificat électronique (qui contient la clé publique de l'émetteur) mais également sous l'angle de l'intégrité du contenu du message.

Remarque : Ce qui précède fonctionne bien dans un environnement parfaitement compatible tant au niveau de la messagerie proprement dite qu'au

niveau des différents logiciels propres à la signature électronique. Dans le doute nous recommandons toujours d'utiliser la signature électronique mais de la limiter aux pièces jointes et ainsi de n'utiliser le mail que comme un vecteur de transmission.

Chiffrement d'un e-mail :

Le chiffrement d'un message permet de garantir la confidentialité totale des informations échangées à la fois du contenu proprement dit du message et de celui des pièces jointes.

Tout comme pour la signature, le chiffrement d'un e-mail est relativement simple lorsqu'il est basé sur une infrastructure de messagerie traditionnelle sachant que les utilisateurs doivent également être munis de certificats (publiés dans l'annuaire de messagerie) sur leur poste de travail. A noter également que ce certificat électronique ne peut en général pas être le même que celui utilisé pour signer pour des raisons essentiellement de contraintes juridiques. En effet tout processus de chiffrement impose au minimum que deux personnes distinctes détiennent la clé de déchiffrement. A l'inverse la clé privée utilisée dans le cadre de la signature électronique doit absolument rester à la seule connaissance de son détenteur.

Le déroulement est également relativement simple et consiste pour l'émetteur à préparer un message, à le chiffrer (à l'aide de la clé publique du destinataire) et à l'envoyer à son destinataire. Ce dernier reçoit ensuite le message qu'il déchiffre grâce à sa clé privée.

Remarque : Tout comme pour la signature électronique, un tel mécanisme de chiffrement fonctionne très bien dans un environnement parfaitement compatible. Précisons également que le chiffrement du contenu a lieu à l'aide d'un algorithme symétrique et que le chiffrement évoqué précédemment permet en fait d'échanger la clé (identique pour chiffrer et déchiffrer) entre l'émetteur et le destinataire.

Recommandations (sécurité des archives et du stockage)

Certains aspects de sécurité ont déjà été abordés au niveau de la fiche 6 Architectures, comme le fait de découpler le stockage des archives proprement dites des serveurs d'archivage au sens de la gestion des données descriptives qui permet de maximiser la disponibilité de l'information. L'un comme l'autre devra mettre en œuvre l'ensemble des mécanismes de protection suivants :

1. Identification - authentification	L'accès à la base d'e-mails archivés par les utilisateurs doit absolument être contrôlé et évolutif. Sur ce dernier point le système doit également être capable de garder la trace des modifications intervenues quant à la définition de ces droits. Par exemple au-delà de trois ans il sera sans doute nécessaire de réduire l'accès aux e-mails aux seuls responsables de l'entreprise ou de l'organisation.
2. Disponibilité	S'agissant d'un archivage dit « actif », il y aura lieu entre autres de bien dimensionner les accès de telle sorte que les utilisateurs puissent interroger leurs e-mails de façon efficace sans perdre de temps à attendre des réponses du simple fait de l'engorgement des communications avec les serveurs. De plus, par exemple en cas d'audit, il est nécessaire de retrouver rapidement une information. L'accès aux systèmes doit donc être possible à tout moment et ces derniers devront *a priori* comporter ainsi une redondance totale des composants matériels : contrôleurs, alimentations, ventilateurs, caches en écritures,... Au niveau disque, la redondance pourra être assurée par une protection de type RAID sans impact sur les performances.
3. Intégrité	D'un point de vue technique il s'agit d'utiliser des matériels répondant à une logique de type WORM (voir focus ci-après) garantissant la non modification des informations et leur non suppression intempestive. La vérification d'intégrité doit également avoir lieu de façon régulière pendant toute la durée de conservation des e-mails. Enfin le moment venu, la suppression des informations devra pouvoir s'opérer avec un maximum de granularité, si possible au niveau de chaque e-mail archivé et non au niveau d'une archive globale.

4. Confidentialité	Le fait de sécuriser l'accès aux données par des mécanismes standard ne protège pas contre tous les soucis de confidentialité. En effet, un grand nombre de personnes au profil technique peut avoir accès aux archives (personnes de l'IT, opérateur de sauvegarde, fournisseurs, …). Afin de véritablement garantir la confidentialité, il doit être possible d'ajouter au besoin des mécanismes spécifiques (logiciel ou mieux matériel) permettant de chiffrer et de déchiffrer à la volée les données, sans impact sur les performances.
5. Sauvegardes	Il est important de prévoir plusieurs niveaux de sauvegarde de façon à répondre aux différents types de sinistres, d'un simple dysfonctionnement à des incidents majeurs. Pour les premiers on pourra avoir recours à la notion d'image instantanée tandis que pour les seconds, incidents majeurs sur site (arrêt électrique prolongé, inondation, incendie …) et en fonction du temps de reprise nécessaire lors d'un tel incident, deux solutions principales sont envisageables : la conservation de sauvegardes des archives à distance (dans ce cas, le temps de redémarrage peut être assez long, notamment si la volumétrie est importante et si le media de sauvegarde est de type bande) ou la réplication au fil de l'eau (dans ce cas, le redémarrage peut être très rapide).
6. Sauvegarde/image	Il s'agit de processus permettant la prise d' « images instantanées » destinées à se prémunir contre un effacement ou une modification accidentelle des données et surtout procéder à une restauration très rapide des données depuis un état consistant mémorisé sur disques.
7. Sauvegarde distante	Le système de gestion des archives doit pouvoir être sauvegardé, sur bandes ou sur disques. Si l'on sauvegarde sur bande, on veillera à utiliser également des bandes de type WORM en cas d'implication légales et surtout à externaliser ces bandes sur un site de secours distant et distinct du premier. Si l'on sauvegarde sur disque, on pourra éventuellement répliquer directement de la solution d'archivage source vers la solution d'archivage distante de secours, en passant par le réseau étendu (WAN) de l'entreprise ou de l'organisation. Si les e-mails archivés doivent être impérativement sauvegardés il en est de même des métadonnées associées qu'elles soient ou non stockées sur les mêmes baies de stockage. On aura également soin de vérifier régulièrement la cohérence entre données archivées et métadonnées associées.
8. Réplication	Pour garantir une reprise rapide en cas de sinistre, on peut également envisager la mise en place d'un système de réplication. Cette réplication devra bien évidemment conserver le caractère WORM des archives afin que la copie de secours conserve le caractère probant en cas de sinistre et de bascule sur le site de sauvegarde.

L'évolution « du WORM physique vers le WORM logique »

Rappelons que les exigences en matière d'archivage consistent d'une part à pérenniser l'information avec une garantie d'intelligibilité à terme mais aussi et surtout de son intégrité. Nous attirons ici l'attention quant au fait qu'il s'agit là de l'intégrité au sens « juridique » du terme agissant sur le contenu et non au sens « technique » opérant sur le format support de l'information. En effet et sur ce dernier point, dès l'instant où à l'intérieur d'un fichier un seul bit quel qu'il soit est touché, l'intégrité technique est perdue alors que pour autant l'intégrité au sens de l'information et de son contenu peut ne pas avoir été touchée. Ainsi le fait d'ajouter un seul espace entre deux mots d'un texte casse l'intégrité technique du fichier où le texte est enregistré alors qu'il est bien évident que le sens du texte n'en sera pas perturbé pour autant.

A ce jour, un grand nombre de types de supports est disponible pour la conservation des données avec deux grandes familles de supports : magnétiques et optiques. Néanmoins il est nécessaire de bien préciser une notion importante qui est celle du WORM ou « write once, read many ». Une définition élargie du WORM consiste à « *faire référence à une méthode d'enregistrement dont la propriété intrinsèque est d'être non effaçable, non réinscriptible et non modifiable* ». Par rapport à ce qui précède, le raccourci était alors facile en matière d'archivage électronique d'instaurer que les seuls supports pouvant garantir les exigences requises évoquées précédemment, devait être de type WORM. Il s'en est suivi une limitation extrêmement forte des supports éligibles pour de l'archivage, limitation levée heureusement depuis.

Si initialement, un seul type de WORM était reconnu, cette situation a largement évolué depuis. Au départ on n'imaginait pas d'autre procédé que l'optique pour répondre aux trois exigences citées précédemment de non suppression, non modification et non réécriture. N'étaient ainsi éligibles en tant que WORM que les procédés optiques non réversibles de type CD. Au moment de l'écriture, le substrat est en effet modifié (fondu) sans possibilité de retour en arrière. Ainsi un CD gravé ne pouvait pas être utilisé à nouveau pour d'autres enregistrements et garantissait par ailleurs la non modification de ce qui était gravé et par voie de conséquence sa non suppression.

Comment dès lors situer les CD réinscriptible de type RW ? De là est née toute l'ambiguïté qui consistait à assimiler un peu trop rapidement cette notion de WORM à la seule technologie optique non réversible. Sachant que par ailleurs les technologies purement magnétiques, bandes et disques apportaient de plus en plus d'arguments tendant à démontrer qu'elles pouvaient également satisfaire aux exigences précédentes, il a bien fallu proposer quelque chose. D'où la récente évolution de cette notion qui reconnaît en fait trois types particuliers de WORM :

Type 1 : transformation permanente du support, principe des disques optiques classiques avec modification du substrat ;

Type 2 : utilisation d'un micro code WORM inclus dans le support au moment de sa fabrication, reconnu par le lecteur ou le contrôleur et protégé de l'effacement et de la réécriture dans des conditions normales d'utilisation, principe des disques magnéto-optiques ou des bandes équivalentes ;

Type 3 : génération d'un micro code enregistré avec l'information et destiné à traiter cet enregistrement comme un enregistrement de type WORM par le logiciel de gestion du support, le protégeant du même coup de l'effacement et de la ré écriture dans des conditions normales d'utilisation, principe des disques magnétiques. Dans certain cas la protection de type WORM peut être limitée à une durée de conservation associée aux données à protéger.

Par rapport au troisième type, cette « reconnaissance » en tant que WORM permet ainsi aux nouvelles technologies à base essentiellement de disques magnétiques de pouvoir se positionner naturellement pour résoudre des problématiques d'archivage. Plusieurs constructeurs se sont orientés depuis vers ce type de support afin de proposer des solutions innovantes pouvant répondre aux besoins spécifiques d'archivage. On voit ainsi aujourd'hui apparaître sur le marché de nouvelles technologies combinant un ensemble d'éléments permettant d'assurer une conservation fiable et pérenne de l'information sur du disque magnétique.

Pour simplifier nous pouvons retenir qu'il existe en fait trois approches foncièrement différentes destinées à assurer cette conservation sécurisée propre aux exigences liées à l'archivage.

La première de ces approches, sans doute la plus « simple » consiste à utiliser des baies de stockage traditionnelles sur disque et à y ajouter une couche de logiciels en amont destinée à gérer cette notion de WORM logique et ainsi à bloquer toute tentative de réécriture, de modification ou de suppression.

Une autre approche, totalement novatrice contrairement à la première, fait même l'objet d'une classification à part, le CAS (Content Access System). A la place de stocker, d'extraire et de gérer les informations au travers d'un système traditionnel de fichiers ou de volumes logiques, on accède à l'information par une empreinte numérique unique créée pour chaque nouvel objet entrant. Il s'agit en fait d'une logique apparentée à celle des consignes. En effet, vous déposez un objet et en retour vous obtenez un ticket (adresse de contenu). Ultérieurement seul ce ticket vous permettra de retrouver l'objet déposé. La façon dont est conservé ce dernier est totalement prise en charge par le système.

Les avantages d'une telle solution sont multiples. Toute modification du contenu déclenche automatiquement la création d'une nouvelle adresse de contenu. A l'inverse si un même objet se présente, l'adresse de contenu étant déjà existante il n'y aura pas de doublement en matière de stockage. Les accès aux ressources sont rapides. La gestion et l'administration d'une telle solution sont considérablement simplifiées, même pour de gros volumes. Par ailleurs le système est en mesure de garantir l'intégrité du contenu à long terme. De même la confidentialité des informations peut être obtenue par un chiffrement systématique des données ainsi conservées.

Une telle logique nécessite le développement des couches applicatives en amont ou mieux, à les intégrer au sein même du micro code de la baie, destinées à permettre aux utilisateurs de retrouver les informations conservées autrement que par un simple ticket. Ces couches doivent en effet permettre de faire le parallèle entre les critères de recherche habituellement utilisés et le fameux ticket. Le fait d'être en amont et pas au sein de la baie constitue un risque car la fonctionnalité peut alors être contournée et la protection ne plus être disponible lors d'un accès direct à la baie.

Enfin la troisième approche est également innovante et répond à une logique d'organisation en cellules, faisant appel au nouveau concept de stockage en grilles ou « grid ». De telles solutions intégrées d'archivage sont plutôt indépendantes des applications mais utilisent néanmoins une méthode d'accès aux enregistrements normalisée. Comme indiqué précédemment ce type de solution utilise une nouvelle approche du stockage, le stockage dit en grille, constitué de plusieurs cellules interconnectées via un réseau ethernet. Chaque cellule participe à la solution et une demande d'archivage est ainsi répartie sur l'ensemble des cellules. Une cellule possède un processeur, un espace de stockage pour l'indexation des « contenus » et les « méta données » ainsi qu'un espace de stockage pour les données des contenus.

L'un des principaux avantages de cette approche est de permettre la réalisation facile de systèmes de stockage complexes à partir d'éléments standard. Une telle technologie permet en effet la réalisation de solutions très performantes, indépendantes du nombre d'enregistrements gérés, évitant du même coup tous les phénomènes liés aux baisses de performances que l'on peut observer au cours des montées en charge. Un autre avantage et non le moindre réside dans sa capacité à effectuer des migrations très progressives, cellule par cellule. Enfin l'exploitation de tels systèmes est simplifiée et surtout allégée à l'extrême. Ainsi même si en apparence le coût d'acquisition peut sembler plus onéreux qu'un système traditionnel, une comparaison plus complète prenant en compte les coûts d'exploitation sur trois ans ne laisse plus aucun doute. L'intérêt est encore plus évident si l'on prend en considération la notion de migration, évoquée précédemment.

Fiche 10 – Principaux acteurs du marché

Contexte

Un très grand nombre d'acteurs proposent des produits logiciels, matériels ou les deux pour répondre à la problématique de l'archivage des e-mails. Certains proposent une ou plusieurs briques de bases intégrables à une solution globale, d'autres proposent des solutions clés en main. Cette fiche, qui à pour but de lister les principales solutions, n'est évidemment pas exhaustive mais donne un aperçu assez précis des offres disponibles.

Enjeux

Une solution d'archivage comporte en fait deux principaux enjeux dont le premier consiste à sélectionner la solution présentant la meilleure adéquation possible entre ses besoins, les offres du marché et son budget. L'autre enjeu essentiel revient à surtout ne pas minimiser les aspects organisationnels de l'archivage. En effet, il n'est pas rare que les processus doivent être repensés, au moins en partie, pour que la solution technique procure toute son efficacité. Dans le cas de l'e-mail il faudrait même aller jusqu'à proposer de nouvelles règles de constitution et de gestion amont qui sont volontairement exclues du présent document. Enfin au-delà de l'aspect organisationnel propre à la solution elle-même il est également primordial de prendre en compte l'accompagnement du changement pour les utilisateurs. Cet accompagnement doit à la fois permettre un maximum d'efficacité de la part de la solution mise en place mais surtout éviter le maintien voire pire encore, le développement, de systèmes parallèles sous prétexte que la solution ne répondrait pas à certains besoins des utilisateurs, ou plus ubuesque, que les utilisateurs croient qu'elle n'y répond pas. Le meilleur exemple serait pour les e-mails, le maintien des fichiers de type PST, NSF ou autre.

Dans la mesure où une solution d'archivage d'e-mails correspond à la fois à du logiciel et à du matériel, sous forme d'un service interne ou sous forme d'un servie externalisé, nous présentons ci-après ces différents éléments avant de passer aux recommandations d'usage.

Logiciel

Le tableau présenté ci-dessous est fourni à titre tout à fait indicatif et non exhaustif, afin de montrer une approche relativement technique, destinée à comparer des logiciels du marché.

Fonctionnalités	Atempo	Autonomy	EMC	HP	IBM	Symantec
Nom du produit	Atempo Digital Archive for Messaging	Zantaz EAS	EmailXtender / DiskXtender /Archives services for Documentum	IAP	CommonStore	Enterprise Vault
Architecture logiciel ou matériel	Solution logiciel sous Windows, Linux, UNIX	Solution logiciel sous Windows	Solution logiciel sous Windows	Solution matériel fournit sous forme d'appliance	Solution logiciel sous Windows ou AIX	Solution logiciel sous Windows
Support de MS Exchange	2000, 2003, 2007	2000, 2003, 2007	2000, 2003, 2007	2000, 2003, 2007	5.5, 2000, 2003	2000, 2003, 2007
Installation d'un logiciel sur le serveur MS Exchange	Non	Non	Non	Non	Oui	Non
Import des fichiers PST (recherche via l'AD, automatisation)	Oui	Partiel	Non	Oui	Non	Oui
Support complet d'OWA	Oui	Oui	Non	Oui	Non	Oui

Fonctionnalités	Atempo	Autonomy	EMC	HP	IBM	Symantec
Support de Lotus Domino	Oui (version 2.2)	Oui (Windows)	Oui (Windows, Solaris, RedHat, Aix, AS/400)	Oui indépendant des plates formes	Oui (Windows, Solaris, Linux, AIX)	Oui (Windows, Solaris, Aix)
Installation d'un logiciel sur le serveur Lotus Domino	Non	Oui	Oui	Oui	Oui	Non
Import des fichiers NSF (recherche, automatisation, etc.)	Oui	Partiel	Partiel	Oui	Oui	Oui
Support complet de Domino Web Mail	Oui (version 2.2)	Oui	Oui	Oui	Oui	Oui
Administration de la solution	Une console	Deux consoles	Deux consoles	Une console (hardware compris)	Plusieurs consoles	Une console
Gestion des rapports	Oui	Oui	Oui	Partiel	Partiel	Oui
Support des matériels d'archivage	HDS HCAP, EMC Centera, NetApp, périphérique WORM, lecteurs de bandes	EMC Centera, NetApp, IBM DR550	EMC Centera, périphérique WORM, lecteurs de bandes	Matériel HP intégré, périphérique WORM	IBM DR550	EMC Centera, NetApp, HDS HCAP, IBM DR550, lecteurs bandes

Matériel

Avant d'aborder les offres du marché nous nous intéresserons d'abord aux types de média disponibles pour conserver des données électroniques. A ce jour nous pouvons distinguer trois différents types de support :

- La bande magnétique ;
- Le disque optique (CD-R ou DVD-R) ou magnéto-optique ;
- Le disque dur magnétique.

Depuis plusieurs années on observe une évolution du marché très nette vers le disque dur magnétique, au détriment des deux autres solutions, pour plusieurs raisons :

- Le coût au Go des disques durs de type SATA est de plus en plus bas et se rapproche de celui des bandes ;
- La fiabilité des disques durs s'améliore régulièrement. Les données sont protégées par des systèmes de grappes de disques (RAID) ou de grappes de serveurs (RAIN) et leur intégrité est vérifiable en continu. Il y a moins de composants mécaniques et ainsi pas de problème de robotique tombant en panne ;
- La rapidité d'accès à l'information : atteindre un objet est en effet beaucoup plus rapide que pour une bande. Ce facteur peut être important à différents niveaux. D'une part en ce qui concerne l'alimentation des systèmes, leur indexation ou ré-indexation. D'autre part dans le cas d'un audit où en général l'information doit être fournie dans un délai donné ;
- La granularité : les durées de conservation peuvent être gérées objet par objet afin de satisfaire au droit à l'oubli et à l'obligation de destruction (ce qui n'est pas le cas avec des bandes ou des media de type CD-R ou DVD-R) ;
- Les capacités gérées : les systèmes de disques haut de gamme du marché sont capables de gérer des milliards d'objets et des Peta-octets en ligne ;
- Les solutions supérieures de protection de données (comme la réplication dans le cadre d'un PRA ou de sauvegarde sur disque) permettant de disposer de RPO (Recovery Point Objective, la fraîcheur des données restaurées) ou de RTO (Recovery Time Objective, le temps nécessaire pour remettre en ligne les données) plus courts qu'avec les bandes ou d'autres disques optiques.

Aujourd'hui, plusieurs solutions d'archivage sur disque sont disponibles sur le marché. Bien que ces solutions intégrées (logiciel et matériel) embarquent des disques magnétiques, par nature réinscriptibles, elles sont munies d'un logiciel qui permet de travailler en mode WORM logique (voir focus fiche 9). Sans ce logiciel, le matériel et les disques sont inutilisables pour de l'archivage.

Le tableau ci-dessous, qui ne se veut pas exhaustif mais avant tout indicatif, résume les choix faits par les principaux fournisseurs pour proposer des solutions de WORM logique à base de disques magnétiques.

Fournisseur	Solutions	Option d'une baie classique	Mode RAIN / Grid	APIs propriétaires	Protocoles standards	« tout en un »[3]	Logiciel pour archivage des E-mails	Outil d'indexation et de recherche	Chiffrement Natif	Capacité Disque maximale
EMC²	Centera	Non	Oui	Oui	En option (avec *Centera Universal Access* : NFS, CIFS, FTP, http)	Avec options	*EmailXtender for Exchange/Domino* & *Documentum Archive Services for Email*	En option : *Centera Seek* & *Centera Chargeback Reporter*	Non	96 To par armoire, liables entre elles.
HDS (Hitachi Data Systems)	Data Retention Utility + HCAP (Hitachi Content Archive Platform)	Oui (DRU sur gammes WMS, AMS, NSC & USP) + solution dédiée	Non (DRU) Oui (HCAP)	Non	Oui (avec HCAP : NFS, CIFS, http(s), WebDAV)	Non	Solutions partenaires	En option (avec HCAP)	Oui	256 To par nœud jusqu'à 20 nœuds (20 Po)
HP	IAP[4] (Integrated Archive Platform)	Non	Oui (cellules en grille)	Oui ou XAM	Non	Oui	*HP Email Archiving software for Microsoft Exchange 2.0 / For IBM Lotus Domino* ou solutions partenaires	Oui, intégré	Non	447 To par système IAP
IBM	Data Retention DR550	Non	Non	Oui (SSAM)	En option (avec *DR550 File System Gateway*: NFS, CIFS)	Avec options	*IBM DB2 common store for Exchange / Lotus Domino* & *Content Manager*	En option (Exalead)	Oui	224 To
	SnapLock	Oui (gamme Nseries)	Non	Non	Oui (NFS, CIFS)			En option	En option	1176 To
NetApp	SnapLock	Oui (gammes FAS & V-Series)	Non	Non	Oui (NFS, CIFS)	Non	Solutions partenaires	En option (ISM 1200)	En option (Decru DataFort)	1176 To

Comment réaliser la fonction de WORM logique à partir de disques magnétiques

Afin de fournir la fonctionnalité WORM, les fournisseurs de stockage de type disques magnétiques ont utilisé deux approches :
- Embarquer cette fonctionnalité WORM directement au sein d'une baie de disques classique, et s'appuyer sur des standards pour l'accès aux données archivées : c'est le cas de NetApp avec sa solution SnapLock , ou de HDS (Hitachi Data Systems) avec son Data Retention Utility ;
- Construire une nouvelle solution et proposer un nouveau standard pour l'accès aux objets archivés : c'est le cas de HP avec IAP ou d'EMC² avec sa solution Centera fonctionnant en mode CAS (Content Adressed Storage).

Toutes les solutions proposées embarquent par ailleurs une horloge interne, censée être infalsifiable, servant à l'horodatage des éléments archivés et à la gestion des durées de conservation. Selon la solution, la granularité est sur l'objet, le fichier ou le LUN (Logical Unit Number). Des droits d'accès ou fonctionnalités de chiffrement permettent de gérer la confidentialité. Ainsi l'administrateur de la solution n'a pas accès aux données archivées quant à leur contenu.

[3] Le fournisseur peut proposer une solution complète pour l'archivage des e-mails, (hors serveurs & OS)
[4] Précédemment dénommé RISS (Reference Information Storage System)

Il est important de rappeler que dans le cadre d'un archivage à long terme de données électronique, les technologies logicielles et matérielles devenant obsolètes très rapidement, il sera nécessaire de migrer (recopier) périodiquement les archives (une période moyenne de 5 ans est généralement admise) et leurs méta données associées, même si elles ne sont pas conservées au même endroit. Aucun constructeur ne s'engage sur une durée de vie de plusieurs dizaines d'années de sa solution. Il convient donc de prendre bien soin de retenir un socle technique le plus pérenne possible, évidemment au niveau logiciel (format pivot, protocoles standardisés) mais aussi au niveau matériel. La simplicité de migration de la solution matérielle représente ainsi en elle-même un véritable gage de pérennité.

Certains fournisseurs de matériel sont capables de proposer la solution complète : socle matériel d'archivage et logiciel métier (comme EMC avec Documentum, DiskExtender,EmailExtender, IBM avec Content Manager, Filenet ou encore HP). D'autres préfèrent travailler en mode partenariat. On jugera aussi la pérennité d'une baie d'archivage par le nombre de solutions partenaires supportées mais aussi sa facilité d'intégration à de nouvelles solutions métiers. Un facteur d'économie majeur est la capacité de la solution à héberger différents types d'archives (et donc à supporter un grand nombre d'applications d'archivage métier) : non seulement les e-mails, mais aussi d'autres pièces importantes comme les documents métiers entrants ou sortants (factures, contrats, courriers, ...), qui sont propres à chaque activité.

Tiers archiveurs

Même s'il existe aujourd'hui sur le marché de plus en plus de tiers archiveurs, rares sont ceux qui proposent une véritable solution dédiée à l'archivage des mails. Nous pouvons néanmoins citer à titre historique la société américaine Zantaz Inc, rachetée en 2007 par Autonomy, qui dès 2000 proposait ce type de service.

Recommandations

Pour choisir une solution complète d'archivage d'e-mails incluant à la fois logiciel et matériel, plusieurs points essentiels devront être analysés soigneusement.

1. Evaluer les besoins	Les besoins concernent d'une part la volumétrie attendue, essentiellement en matière de volumétrie globale mais aussi en nombre d'e-mails à gérer, sans oublier le nombre d'utilisateurs concernés. D'autre part on aura également soin de classifier au besoin les e-mails par grandes familles pour lesquelles les durées de conservation seront clairement définies.
2. Interopérabilité et partage de ressources	Evoquée également dans la fiche 3 sur les contraintes techniques, la question de l'interopérabilité est fondamentale, à compléter par la notion d'évolutivité. On la retrouve à trois niveaux : - La capacité du système à pouvoir changer l'un de ses composants (logiciel ou matériel) sans remettre en cause l'ensemble, éviter les systèmes propriétaires ; - La possibilité d'implémenter un système d'archivage non intrusif, capable de travailler avec des ressources déjà existantes et non dédiées ; - Enfin, dans le cas d'un archivage confié à un tiers, la sécurité que ce tiers soit interopérable avec d'autres tiers afin, le cas échéant, de pouvoir leur confier les données de ses clients en cas par exemple d'arrêt de son activité.
3. Evolutivité, montée en charge et volumétrie	Concernant cet aspect il est indispensable d'obtenir des garanties de la part des fournisseurs (logiciel et matériel). Une bonne façon de s'en convaincre consiste à assister à une démonstration en exploitation chez un client. Même dans le cas du recours à un tiers archiveur les temps d'accès doivent être garantis dans le temps, surtout en fonction de l'évolution du nombre d'utilisateurs.

4. Possibilités d'indexation	En matière d'e-mail et compte tenu de leur nombre, la facilité de retrouver un e-mail sera directement fonction de la façon dont il aura été indexé, entre système classique par rapport à l'entête, système par mots-clés et moteur de recherche, appliqué au corps de l'e-mail mais également aux pièces jointes. Il sera important de vérifier que l'outil permet de hiérarchiser les résultats de recherche et autorise des recherches en cascade.
5. Accès	Même si l'on parle d'archivage des e-mails, rappelons qu'il s'agit d'un archivage dynamique et que l'accès en matière de temps doit être rapide. L'utilisateur a en général besoin de ses e-mails en ligne sans attendre et ce quelle que soit la volumétrie et le nombre d'utilisateurs. Le contrôle d'accès se retrouve également au niveau de la confidentialité sachant que les droits devront être parfaitement définis et évolutifs dans le temps afin également de respecter les exigences de la CNIL en la matière.
6. Coûts directs et associés	Voir la fiche 11 qui détaille cet aspect essentiel consistant à bien analyser l'ensemble des postes de coûts: matériel, logiciel, intégration, … mais également les coûts cachés ou associés comme la maintenance, la formation,…
7. Déploiement	La complexité d'un projet n'est pas la même pour quelques milliers ou pour plusieurs dizaines de milliers d'utilisateurs. Pour les projets avec d'importantes volumétries, il est ainsi particulièrement important d'être vigilant dés le départ sur les trois points suivants : - Complexité de la solution (complexité des profils d'archivage à mettre en œuvre, complexité d'intégration des différents composants, maintenance opérationnelle dans le temps, restauration de l'environnement complet en cas de problème) - Scénarii de déploiement (charge réelle du projet et modification des habitudes des utilisateurs) - Garanties sur les performances et sur l'évolutivité de la solution dans le temps (voir ci avant recommandation 3)
8. Pérennité du fournisseur	Même si rien ne peut véritablement garantir la pérennité des fournisseurs, il est important de la prendre en compte. Ainsi la reprise ou le transfert des données, ou au niveau logiciel la récupération des codes sources doivent être précisément envisagés en détaillant les modalités et les coûts correspondants.
9. Evolution de l'organisation	Au sein même d'une organisation, les réorganisations sont possibles et à ne pas négliger (y compris les fusions et acquisitions) dans la mesure où elles font partie des événements courants de la vie des sociétés. Il est ainsi préférable que les systèmes d'archivage retenus soient aux maximum compatibles (interopérables) ou du moins qu'on puisse mutualiser les outils de recherche. On privilégiera donc le côté efficacité des solutions plutôt que leur sophistication.

Fiche 11 – Coûts de l'archivage

Contexte

Il est indispensable d'évaluer les coûts liés à l'archivage des e-mails. Nous donnons ci-après les éléments clés à prendre en compte afin d'optimiser le retour sur investissement et minimiser les coûts de sa solution d'archivage d'e-mails, à savoir :

- Le prix d'acquisition qui comprend les coûts du matériel, du logiciel, des services d'installation et de mise en œuvre, de la formation et les coûts de maintenance.

  Remarque : Afin de pouvoir comparer différentes solutions il est intéressant de pouvoir ramener si possible ces coûts au Giga-Octet utile voire utilisé. Ceci afin de valoriser certaines solutions qui permettent d'atteindre des taux d'utilisation (rapport entre espace utilisé et espace alloué) très élevés, grâce à des mécanismes avancés de gestion de l'espace (allocation au plus fin, sur-allocation, instantanés, déduplication,…).

- Le coût d'un service de tiers archivage, à opposer au prix d'acquisition traditionnel ;
- Les coûts d'exploitation (internes) ;
  - la charge d'exploitation que génère la solution pour sa gestion au quotidien correspondant aux ressources humaines nécessaires pour préparer l'archivage, gérer les données archivées et restituer l'information aux utilisateurs. Le constat a été fait que le coût humain est toujours plus important que le coût matériel ;
  - Les coûts liés à l'espace en salle machine, la consommation électrique, les besoins en ventilation.
- Les coûts liés aux arrêts de service ;
  - Coût des arrêts planifiés ;
  - Coût des arrêts non planifiés causés par des incidents matériels, logiciels, ou dus à une erreur humaine ;
  - Coût du risque légal lié au processus de recherche (audit, …).

  Remarque : Les solutions qui nécessitent peu de plages de maintenances (nombre et durée) et qui présentent une disponibilité maximale mais aussi des temps de restauration rapides seront à privilégier dans la mesure où la disponibilité de l'archive est très importante pour permette aux utilisateurs d'accéder à leurs anciens e-mails facilement mais également pour permettre à un auditeur de trouver la pièce recherchée dans le délai imparti.

- L'éventuelle mutualisation des coûts avec d'autres solutions de stockage ou d'archivage.

En vue d'analyser la rentabilité de telle ou telle solution, les coûts précédents sont à comparer à d'autres types de coûts indirects qui résultent d'un non archivage :

- temps perdu à rechercher des informations pas ou mal archivées ;
- coût des solutions techniques mal adaptées qui provoquent des systèmes parallèles ou imposent un renouvellement prématuré des matériels ;
- les amendes, sanctions et éventuels redressements, conséquences de l'impossibilité pour l'entreprise de produire le document exigé par les autorités ou de prouver son authenticité, ou encore par suite de la conservation de données personnelles dont la destruction est réglementaire.

Enjeux

Deux objectifs sont prioritaires dans l'approche du coût de l'archivage électronique :

- Trouver le bon rapport coût / efficacité : des solutions techniques et des outils méthodologiques trop sophistiqués feront de l'archivage une contrainte trop lourde pour les utilisateurs qui seront alors tentés de contourner le système. De même, des outils sous dimensionnés en termes de volumes, de fonctionnalités ou de points de contrôle produiront un archivage qui ne sera pas fiable et qui présentera donc des risques plus ou moins élevés pour l'entreprise. A ce niveau on pourra raisonnablement se poser également la question de choisir entre faire ou faire faire ;

- Identifier et hiérarchiser les risques (essentiellement financiers) du non archivage afin de définir les données ou services prioritaires et de programmer les dépenses en fonction de ces risques.

Recommandations

Le type de recommandations que nous pouvons donner ici est avant tout guidé par une attitude de bon sens. Chaque organisation doit analyser ses coûts en fonction de ses propres besoins et par rapport à ses risques potentiels. Par contre il est essentiel qu'une étude des coûts prenne en compte tous les aspects qui entrent en jeu lors de la mise en place d'un système d'archivage électronique.

1. Exhaustivité des coûts	Afin d'être aussi exhaustif que possible nous recommandons une simulation d'exploitation complète du système d'archivage, sur au moins trois ans. Une telle simulation aura également pour mérite de pouvoir prendre en compte l'amortissement du matériel et surtout permettra véritablement de comparer une solution d'acquisition interne à une solution externalisée.
2. Migration	Une durée de simulation d'exploitation du service d'archivage supérieure à trois ans permettra par ailleurs d'anticiper et surtout de prendre en compte les coûts de migration.
3. Autres coûts	Ne pas oublier de simuler des incidents afin d'anticiper des coûts de restauration et de mettre en avant certains manques par exemple en matière d'assurance.
4. Suivi de projet	Même si l'archivage des e-mails ne représente qu'une partie d'un projet global d'archivage il doit être géré comme un projet à part entière et en ce sens il est important de prévoir d'autres coûts comme : - Communiquer sur les conséquences du non archivage au niveau global de l'organisation ; - Faire en sorte que les exigences d'archivage soient prises en compte par l'ensemble des métiers et fonctions de l'organisation ; - Accompagner le changement par des actions de sensibilisation et de formation de l'ensemble des utilisateurs concernés ; - Inclure l'archivage des mails dans la politique d'archivage (au sens électronique) existante ou en créer une au besoin.
5. Mutualisation des coûts	La mise en place d'un système d'archivage des e-mails en interne nécessite l'acquisition de matériels et de logiciels. On prendra soin avant de lancer ces achats de vérifier qu'il n'y a pas éventuellement une solution de partage avec des équipements déjà existants. A l'inverse les matériels achetés pour l'archivage pourront potentiellement être partagés avec d'autres applications.
6. Valeur de l'information	En fonction par exemple de la disponibilité à assurer, les coûts peuvent être très différents. Par ailleurs il est clair que toutes les données n'ont pas la même valeur ou criticité pour l'organisation en regard entre autres, des conséquences financières qui en découleraient si ces données étaient perdues. On aura donc soin de définir différents niveaux de service d'archivage de telle sorte que l'archivage de données vitales coûte légitimement plus cher que d'autres.
7. Mesurer son archivage	Même s'il n'existe pas à ce jour d'indicateurs spécifiques destinés à l'évaluation de la performance d'un système d'archivage d'e-mails, il est néanmoins recommandé de le mesurer en calculant par exemple son coût annuel incluant l'identification, la capture, la gestion, la maintenance, l'accès et la destruction des e-mails, ainsi que l'évolution de ce coût au fil des ans.
8. Faire ou faire faire	La logique de mutualisation peut, poussée à l'extrême, conduire à choisi une solution externalisée. En fait chaque organisation est soumise à ses propres contraintes et l'analyse du faire ou faire faire doit être abordée avec soin en prenant en compte un ensemble de critères pas seulement quantitatifs. Par ailleurs il est également parfaitement possible de recourir à plusieurs solutions articulées en fonction de la nature des données. Certains e-mails stratégiques pourraient par exemple être externalisés pour des raisons de confidentialité alors que les autres seraient archivés en interne. Enfin l'important est de garder une vision globale des solutions utilisées afin d'en maîtriser les coûts.

Fiche 12 – Cas Clients

Centre hospitalier universitaire de Louvain (UZ Leuven)

Le cadre

Avec plus de 2000 lits, le centre hospitalier universitaire de Louvain, en Belgique est l'un des plus grands centres hospitaliers d'Europe et le premier de Belgique. Les 9.000 employés de l'hôpital possèdent tous un compte de messagerie sous Microsoft Exchange. Pour eux, l'e-mail est un moyen de communication aussi important que le téléphone. Il est utilisé à peu près pour tous les besoins métiers sauf l'information médicale propre à chaque patient.

Le problème posé

Les défis pour la direction informatique concernant la messagerie électronique sont multiples :

- assurer la disponibilité du service à un bon niveau de performance,
- monter en charge pour permettre un doublement du nombre des utilisateurs,
- simplifier la gestion des boîtes aux lettres,
- réduire les appels au helpdesk interne,
- accélérer les temps de restauration du système de gestion des e-mails.

Deux points de vue s'opposaient, celui du département informatique qui désirait conserver une « petite base » Exchange afin de garantir les performances, la disponibilité, et restaurer rapidement le système en cas d'incident, et celui des utilisateurs qui voulaient disposer d'une grande boîte aux lettres, quasiment illimitée afin de pouvoir conserver tous leurs messages. Jusqu'alors le département informatique avait imposé ses vues en mettant en place une solution basée sur des quotas. De leur côté les utilisateurs avaient évidemment contourné cette contrainte en utilisant des fichiers au format PST en local sur leur machine. Il en résultait un grand nombre d'appels au helpdesk et des utilisateurs mécontents du fait de ne pas pouvoir accéder à l'ensemble de leurs e-mails facilement.

La Solution

Avec la mise en place d'une solution d'archivage des e-mails, la base de données principale reste désormais d'une taille tout à fait gérable, les utilisateurs ne sont plus limités par des quotas et l'opération s'est avérée totalement transparente pour eux. Bien que « sortis » de l'application Exchange et stockés sur un media d'archivage secondaire, les e-mails restent visibles depuis l'interface utilisateur, une fonctionnalité de recherche rapide en plein texte est également fournie ainsi qu'un mode déconnecté. Le système est également prêt pour l'archivage « légal ».

Architecture retenue

Les boîtes aux lettres sont gérées avec le système Exchange 2003 de Microsoft, pour une taille totale de l'ordre de 1 To, stockées sur des baies NetApp performantes (disques fiber channel rapides, en accès iSCSI). Des snapshots (clichés instantanés) sont pris régulièrement sur la production et répliqués sur un stockage secondaire dans un second centre de données, pour assurer une reprise rapide en cas de nécessité et répondre ainsi au besoin de disponibilité.

La gestion des e-mails archivés est assurée par le logiciel Enterprise Vault de Symantec. Les e-mails archivés sont conservés également sur des baies NetApp mais économiques (disques SATA sécurisés en RAID double parité). La taille totale de l'archive est de l'ordre de 1,7 To (avec utilisation du mode single-instance et de la compression). Les e-mails archivés sont également répliqués vers le second centre de données.

Les règles d'archivage retenues sont les suivantes :

- Archiver systématiquement les mails datant de plus de 7 jours, sauf pour l'inbox (30 jours), la poubelle et le dossier SPAM (jamais) ;
- Remplacer dans la base Exchange chaque mail archivé par un raccourci comprenant les méta données originales, les 500 premiers caractères du corps du message et la liste des pièces jointes.

Lorsque l'utilisateur clique sur le raccourci pour accéder au mail complet, la donnée est automatiquement rapatriée depuis l'archive.

Le TCO et les bénéfices

Une étude effectuée par une société d'audit externe a montré que le retour sur investissement de la mise en œuvre de l'archivage sera de 189% au bout de 5 ans et que le ROI était atteint en 27 mois.
En outre, le stockage nécessaire aux e-mails a été réduit de 49% et les appels au helpdesk ont baissé

de 75%. Le niveau de service assuré permet un RTO inférieur à 30 minutes. Le doublement du nombre des utilisateurs de la messagerie n'a généré qu'une surcharge de 25% au niveau des équipes en charge du système. Avec l'ancien système, il aurait fallu environ 150% de personnel supplémentaire (rien que l'effet positif de l'archivage sur ce poste a généré une économie de 90K€).
Enfin, la taille du stockage primaire peut être maîtrisée et la croissance se faire principalement sur le stockage dédié à l'hébergement des archives, plus économique que le disque primaire.

L'archivage « légal »

La législation européenne n'impose pas aux hôpitaux d'archiver les e-mails en mode WORM. Cependant si cela s'avérait nécessaire et compte tenu de l'architecture actuelle, il serait aisé d'activer la journalisation ainsi que le mode WORM optionnel embarqué dans le stockage NetApp (fonctionnalité SnapLock).

Ecurie de F1 affilié à un grand groupe automobile

Le cadre

Véritable vitrine technologique du constructeur cette écurie F1 conçoit, construit, maintient et gère l'écurie de course du même nom dont les voitures sont régulièrement engagées sur les circuits de Grand Prix de Formule 1 aux quatre coins de la planète. L'équipe F1 emploie environ un millier de personnes travaillant sur des stations de travail Unix ou des postes Windows.

Le problème posé

Afin de rester compétitif, l'équipe F1 dépend autant de la disponibilité et de la performance de ses applications critique, de l'intégrité des informations conservées, que de l'expertise de ses pilotes. Elle avait le besoin crucial de pouvoir gérer la véritable explosion du volume de ses données, non seulement les informations issues de la CAO (conception assistée par ordinateur) de conception des bolides (notamment des modèles 3D Catia), les données de calculs de dynamique des fluides (CFD), les télémesures prises sur le terrain (plus de 200 capteurs auditent 12.000 composants sur chaque véhicule) mais également la volumétrie gérée par les e-mails et par conséquent la taille des boîtes aux lettres.

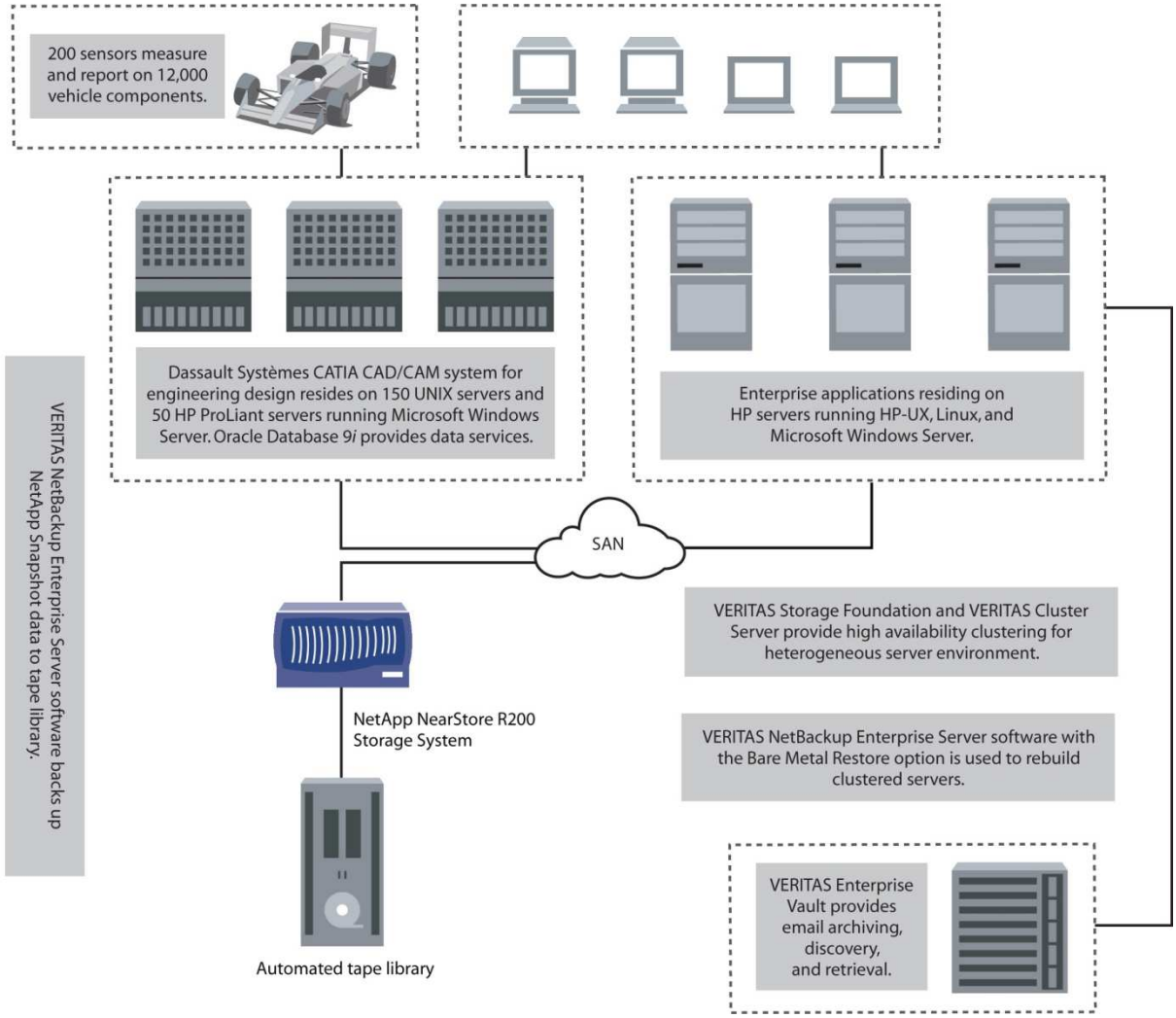
La Solution

Le logiciel Enterprise Vault a été choisie dès 2004 par l'équipe de Direction afin de permettre l'évolutivité de l'infrastructure Microsoft Exchange, de conserver les processus de workflow actuel des employés, tout en améliorant la fiabilité globale de la messagerie. La solution permet de limiter désormais le stockage local à 500 Mo (sept fois moins que la situation précédente) et fournit une fonctionnalité d'archivage transparente, basée sur du disque mais également sur des bandes, pour permettre d'accéder à des années d'e-mails en ligne, directement depuis l'interface Outlook.

Architecture retenue

Il s'agit d'une architecture très consolidée. Les serveurs déposent leurs données applicatives et leurs archives sur une baie NetApp via un réseau de stockage spécialisé (SAN). Les logiciels de Symantec gèrent la haute disponibilité des applications, la protection des données ainsi que le processus d'archivage.

Server and Storage Management and Email Management Architecture



Le TCO et les bénéfices

Une étude interne montre que la mise en œuvre de l'archivage des e-mails pour l'équipe F1 a permis de réduire de 50% le coût total de possession de l'infrastructure de messagerie, notamment grâce au fait d'avoir acheté moins de serveur, mais aussi du temps gagné dans la recherche des e-mails perdus ou effacés.

Initialement installé dans un seul site, ces solutions ont été récemment adaptées également par d'autres usines du groupe, augmentant ainsi significativement la contribution de NetApp et Symantec aux succès de l'équipe F1. Les systèmes de stockage NetApp voyagent maintenant à travers le monde avec les équipes de courses et d'essais de l'équipe F1.

L'archivage « légal »

Contrairement à ce que l'on pense l'archivage des e-mails n'a pas systématiquement une connotation légale ou réglementaire. Le cas qui vient d'être rapidement présenté illustre bien cette nécessité de devoir conserver ses e-mails, ne serait-ce qu'à des fins internes d'exploitation, sans même aller jusqu'à la notion de patrimoine.

Conclusion

Nous espérons au travers de ce document avoir suffisamment attiré l'attention des responsables d'entreprise ou de toute organisation tant publique que privée de la nécessité de véritablement gérer les e-mails. Au-delà de cette mise en garde nous avons tenté d'apporter les principaux éléments de réponses destinés à résoudre la problématique de plus en plus pressante d'archivage des e-mails.

A noter également que d'autres matériels communiquants prennent également de plus en plus d'importance et l'accès à l'information se doit d'être au même niveau d'exigence quel que soit l'outil. Ainsi une solution d'archivage doit aujourd'hui permettre aux utilisateurs l'accès à leur base d'archive aussi bien à partir de leur poste de travail au bureau que via un PC portable ou d'autres terminaux de type PDA (personal digital assistant), BlackBerry ou autre.

Enfin, en termes de communication, d'autres systèmes se développent comme la messagerie instantanée (Microsoft Live Communication Server, Lotus Sametime, Windows Live Messenger, Yahoo ! Live Messenger, Google Talk, etc…). En plus de l'e-mail il s'agit là bien évidemment d'une nouvelle contrainte dans la mesure où les entreprises doivent conserver leurs données électroniques, quel que soit l'outil à partir desquelles elles ont été générées. Les solutions d'archivage doivent donc de plus inclure également dans leur périmètre ce type d'outil.

Référentiel documentaire

- Textes relatifs à l'écrit numérique : articles 1316 à 1316-4 du Code Civil, Article 287 du Nouveau Code de Procédure Civile
- norme ISO 14721 ou modèle OAIS (Open Archival Information System) de la Consultative Committee for Space Data System, organisation et fonctionnement d'un centre d'archivage de données
- norme ISO 15489 - Records Management, stratégie globale pour la traçabilité de l'information et des responsabilités
- norme ISO 19005 – PDF/A format de conservation des documents
- norme AFNOR NF Z42-013 Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes
- modèle européen MoReq (Model Requirements for the Management of Electronic Records)
- Recommandations du Forum des Droits de l'Internet relative à la Conservation électronique des documents (secteur privé), publié le 1er décembre 2005 en partenariat avec la Mission pour l'Economie Numérique
- Délibération CNIL n° 2005-213 du 11 octobre 2005 relative aux modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.
- Guide de l'archivage électronique sécurisé, publié par l'EDIFICAS
- L'archivage électronique à l'usage du dirigeant publié par le CIGREF et FedISA
- Dématérialisation et archivage électronique publié chez Dunod par Jean-Marc Rietsch, Marie-Anne Chabin et Eric Caprioli.
- Protection du patrimoine informationnel publié par le CIGREF et FedISA
- GUIDE de l'E-MAIL, guide de la bonne utilisation de l'e-mail dans l'entreprise, MEDEF 2008

FedISA
Fédération
ILM, Stockage & Archivage

55 avenue Victor Hugo 75116 Paris
Tél./Fax : +33 (1) 44 17 91 45
info@fedisa.eu
www.fedisa.eu