Accompagner

Guide pratique

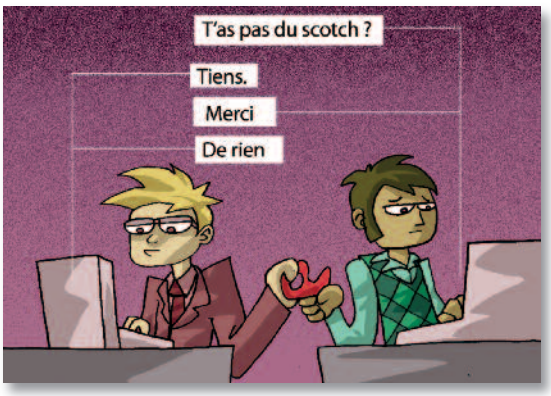
La bonne utilisation de l'e-mail dans l'entreprise

MEDEF

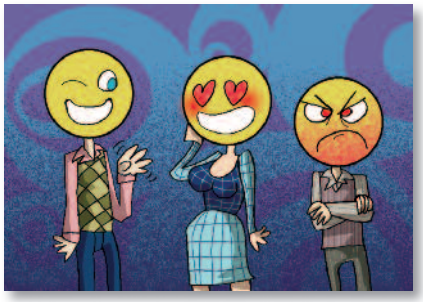
Sommaire

Avertissement

Le présent document a pour unique vocation de sensibiliser à la bonne gestion des e-mails. Le MEDEF décline toute responsabilité en ce qui concerne l'utilisation des solutions préconisées par ce guide. Ce guide ne peut aucunement se substituer aux conseils avisés de spécialistes techniques ou juridiques de la sécurité des systèmes d'information.



Partie 3
Fondamentaux techniques



Préface

Ce guide est à destination des dirigeants d'entreprise

Son objectif est de **donner un aperçu de l'ensemble des sujets liés à l'usage de l'e-mail** et des points clés correspondant à chacun des niveaux impliqués (dirigeants, collaborateurs et service informatique gérant l'outil mail, prestataires), tout en permettant un dialogue entre ces diverses populations autour de ce sujet.

Outre cette introduction qui présente ce qu'est l'e-mail, les points-clés du bon usage, et un glossaire des principaux termes du domaine, le guide est organisé en fiches, accessibles séparément selon les besoins.

Les fiches sont organisées comme suit :

1. Bon usage de l'e-mail

- **Fiche 1 :** Les règles de bonnes pratiques de l'e-mail afin d'augmenter sa productivité
- **Fiche 2 :** Les limites de l'usage de l'e-mail, au profit des autres outils de communication et de collaboration
- **Fiche 3 :** Les usages en mobilité, en se connectant via un ordinateur à l'extérieur de l'entreprise ou via un téléphone permettant de récupérer ses e-mails
- **Fiche 4 :** les aspects juridiques liés à l'utilisation de l'e-mail

2. Bonne utilisation de l'e-mail pour la performance de l'entreprise

- **Fiche 5 :** l'intérêt de l'e-mail comme outil marketing
- **Fiche 6 :** e-mail et archivage : correspondances dématérialisées et mémoire d'entreprise

3. Fondamentaux techniques

- **Fiche 7 :** que faire face au détournement du bon usage : le SPAM, le PHISHING, les contenus malveillants, les attachements malveillants, les BOTNETs
- **Fiche 8 :** l'utilisation de l'e-mail sécurisé : chiffrement, signature
- **Fiche 9 :** les architectures nécessaires, ainsi que les choix possibles.
- **Fiche 10 :** Les smileys !!

Un **glossaire** présente les termes les plus couramment utilisés dans le guide. On trouvera également la liste des contributeurs à sa rédaction.

Le terme le plus couramment utilisé d'e-mail sera privilégié dans ce guide à des fins d'homogénéité de lecture mais d'autres termes existent pour le désigner : messagerie électronique, courrier électronique, courriel, email, mail, mel...

Ce guide ne remplace pas les conseils de spécialistes : n'hésitez pas à voir votre responsable informatique et/ou un juriste spécialisé.

Introduction

Utilisation de l'e-mail en entreprise

L'e-mail est un outil de messagerie, communication électronique par l'écrit, de nature asynchrone comme l'est la lettre envoyée par la poste. **Il s'est imposé comme l'outil le plus utilisé en entreprise car il permet de :**

- **multiplier les communications indépendamment du nombre de correspondants et de leur disponibilité immédiate,**
- **assurer la traçabilité et le suivi des échanges,**
- **gérer la diffusion de l'information, personnelle ou au sein d'un groupe, directe ou indirecte (destinataire en copie),**
- **classer, archiver et rechercher les communications réalisées.**

Sa progression en volume est constante d'année en année notamment au détriment du courrier papier, du fax mais aussi du téléphone. Une étude IDC de 2005 montre un doublement du volume des e-mails entre 2002 et 2005. Cette tendance se poursuit, sans ralentir, tant en nombre de boîtes e-mail qu'en volume comme l'illustrent les projections des études du Radicati Group de 2006 (croissance de 20% par an en moyenne et doublement entre 2005 et 2009).

La facilité d'utilisation, le caractère universel et les bénéfices de l'e-mail expliquent largement cette adoption massive.

La messagerie est également souvent liée à des usages complémentaires concernant la gestion du calendrier et des contacts. De plus, l'organisation et le suivi des réunions impliquent souvent des échanges de messages et pièces jointes.

Son développement accompagne et soutient les évolutions managériales des entreprises (organisations mixant hiérarchie et rattachement fonctionnel, organisation par projet, organisation multinationale, accent mis sur la collaboration, processus transversaux, communautés transverses, relation clients, etc…).

Il constitue aussi un support clé de relation avec ses fournisseurs et ses clients et un outil de marketing.

Cette prédominance de l'e-mail dans l'activité de l'entreprise conduit, de plus en plus, à lui faire jouer un rôle central et à le considérer comme une application critique. Le Gartner estime ainsi que 50% à 75% de l'information utile est échangée de personne à personne (par opposition aux applications métier et aux référentiels documentaires d'entreprise). **Cette situation met ainsi l'accent sur l'enjeu de la valeur juridique de l'e-mail.**

La croissance constante du volume des e-mails s'accompagne aussi, logiquement, de l'augmentation du temps consacré à les traiter. Cette activité prend des proportions significatives du temps total de travail.

Les salariés américains reçoivent en moyenne 44 e-mails par jour, en envoient 17 et passent 1H35 par jour à traiter leurs e-mails (Work Productivity Council, 2003). Une étude réalisée en France a fait ressortir des chiffres similaires (Microsoft, 2006). Elle met aussi en évidence l'existence en proportions significatives de populations à haute intensité d'utilisation de l'e-mail (plus de 100 e-mails reçus par jour et plus de 2 heures passées par jour à traiter ses e-mails). Recevoir 100 e-mails par jour ne constitue plus aujourd'hui une situation exceptionnelle dans des grandes entreprises internationales. Des situations extrêmes peuvent même être observées : Marissa Mayer, vice-président de Google confiait ainsi dans un entretien "How I work" (Fortune, 2006) qu'elle recevait 700 à 800 e-mails par jour !! (Elle ajoute qu'elle peut consacrer 10 à 14 heures par jour à traiter ses e-mails !!).

La popularité de l'e-mail et son développement constant conduisent aussi à l'extension de ses utilisations, au-delà de ses fonctions premières, **l'e-mail devenant le « couteau suisse » du travail intellectuel :**

- conversations par enchainement d'allers et retours d'e-mails,
- prise de note et de mémo dans le corps d'un e-mail,
- espace de stockage de fichiers de référence en pièces jointes des e-mails,
- …

L'e-mail, par son caractère différé (asynchrone) et traçable, complète utilement le téléphone.

En revanche, l'e-mail a souvent tendance à être utilisé à la place d'autres outils de communication plus pertinents pour certains usages, mais ces derniers sont encore trop peu connus dans l'entreprise.
En effet **l'e-mail ne constitue pas l'outil le mieux adapté à tous les contextes. Ainsi, le travail collaboratif sur des documents relève d'outils collaboratifs ou de gestion de contenu. De même, le suivi des demandes, travaux ou affaires est réalisé beaucoup plus efficacement par des outils dits de « workflow » (processus de traitement des tâches). Au-delà de ces outils de communication, messagerie par mail ou instantanée, téléphone et site collaboratif, se positionnent des outils de communication enrichis :**

- sites de partage de documents ou d'applications,
- sites de publication de contenu en intranet et workflow,
- messagerie instantanée,
- webconferencing : conférence utilisant Internet et intégrant voix, image et flux de données,
- vidéo-conférence,
- collaboration intégrée dans des applications métiers.

La messagerie instantanée est aujourd'hui peu développée en entreprise, mais y est introduite notamment par les générations de jeunes employés qui importent l'usage qu'ils font des messageries instantanées grand public, ainsi que via de nouveaux usages de communication d'entreprise basés sur la notion de disponibilité (« gestion de présence » selon l'expression anglo-saxonne).

L'importance prise par l'e-mail dans la vie de l'entreprise est telle qu'elle nécessite de pouvoir y accéder n'importe où et n'importe quand.
Cela conduit à développer des solutions de consultation à distance.

Cela pose aussi la question des règles d'usage entre la sphère professionnelle et la sphère privée (l'accès à distance de l'e-mail s'effectuant aussi à la maison).

L'e-mail constitue donc un enjeu à différents niveaux :

- Le chef d'entreprise doit définir la politique d'utilisation et les investissements nécessaires pour en tirer les bénéfices optimums.
- Les utilisateurs doivent mettre en œuvre les usages les plus adaptés pour garantir leur productivité personnelle.
- Les équipes informatiques doivent définir et opérer les solutions correspondantes.

Il constitue donc, du fait de sa prééminence dans la communication, le partage d'informations et le travail d'équipe, un sujet à part entière dans le management et la productivité de l'entreprise qui réclame l'attention du chef d'entreprise.

Le chef d'entreprise a ainsi intérêt à définir une politique de la bonne utilisation de l'e-mail :
- règles de bon usage,
- questions juridiques,
- archivage,
- sécurité, …

Il veillera à sensibiliser et former régulièrement ses collaborateurs sur ces sujets.

Au-delà de cette étape, selon les usages dans son entreprise, il pourra explorer deux pistes :
- Mise en place d'autres outils complémentaires de l'e-mail (messagerie instantanée intégrant le partage de documents et les web-conférences, espaces de partage de documents, workflow,…).
- Intégration de l'ensemble des moyens de communication (téléphone, messagerie, messagerie instantanée) dans un seul outil numérique (messagerie unifiée).

Les 12 points clés à retenir pour le bon usage de l'e-mail

[A] Faciliter l'exploitation des e-mails pour les destinataires

1. Faciliter le traitement des e-mails par les destinataires :
Destinataire = pour action, Copie = pour information, Répondre à tous : non systématique !

2. Favoriser la lecture des e-mails : titre explicite, message court et clair,
synthèse des e-mails longs retransmis.

[B] Être productif dans le traitement des e-mails reçus

3. Réaliser une action pour chaque e-mail consulté : traiter, supprimer, marquer (pour suivi ou traitement ultérieur), déléguer.

4. Organiser des plages horaires dans son agenda pour consulter ses e-mails.

5. Savoir rapidement retrouver un e-mail particulier, en organisant des dossiers de classement (arborescence structurée) des e-mails par type d'activités et/ou en utilisant une fonction de recherche (moteur de recherche).

6. Utiliser des règles de classement ou repérage automatique des e-mails entrants (e-mail direct, en copie, venant de son supérieur direct, liste de diffusion,…).
N'imprimez pas systématiquement vos mails.

7. Faire une sauvegarde régulière de ses e-mails pour protéger son capital informationnel de risques physiques (incendie, vol de PC, …) et logiques (virus, …), penser à utiliser l'archivage, maintenir une taille de boite mail acceptable.

[C] Utiliser l'e-mail à bon escient

8. Pour les conversations simples ou urgentes, préférer les échanges directs (téléphone et messagerie instantanée). Pour partager et converger sur un document, conserver un certain nombre de réunions.

9. Éviter les e-mails « ping-pong » (pas plus de 2 allers-retours à partir du même e-mail de départ).

10. Ne pas utiliser l'e-mail pour résoudre des conflits.

11. Veiller au nombre et à la mise à jour des membres de vos listes de diffusion.
Eviter d'envoyer des e-mails à trop de destinataires.

12. Relire votre e-mail avant envoi. Eviter l'envoi précipité. Vérifier la liste des destinataires, le titre, le contenu, les pièces jointes.

Partie 1

Fiche 1

Les règles de bonnes pratiques de l'e-mail afin d'augmenter sa productivité

Sommaire

Le problème de l'e-mail, ce n'est pas que l'on en reçoit trop, c'est que l'on nous en envoie trop !

De ce constat découlent les principes de bon usage et d'efficacité de l'e-mail :

- Limiter les e-mails envoyés en communiquant pertinemment et en utilisant les moyens de communication les plus adaptés par rapport au contexte.
- Envoyer des e-mails en prenant en compte la manière dont vos interlocuteurs vont les traiter pour faciliter leur exploitation.
- Traiter efficacement les e-mails reçus en utilisant les règles de productivité de l'e-mail.

Deux autres bonnes pratiques peuvent être définies :

- Optimiser l'organisation et le suivi des réunions à partir du calendrier.
- Favoriser l'utilisation des espaces collaboratifs.

Communiquer pertinemment et utiliser les moyens de communication les plus adaptés par rapport au contexte

Trois contextes principaux de communication peuvent être caractérisés :

1 - Conversation

Caractéristiques :

- Réponse immédiate attendue (urgence, criticité) : par exemple dans une relation client ou une prise de décision.
- Demande ponctuelle instantanée : par exemple une expertise sur un point (souvent lié à la notion de disponibilité).
- Sujets ou problèmes peu structurés nécessitant une succession d'échanges interactifs liés les uns aux autres.

- Sujets complexes ou sensibles nécessitant une communication riche (intonation de voix, langage corporel,...).
- Sensibilité au temps de réponse et à la disponibilité de l'interlocuteur.
- Interlocuteurs généralement connus.
- Pas de traçabilité.

2 - Message

Caractéristiques :

- Réponse différée.
- Sujets ou problèmes structurés pouvant être formalisés dans un court message avec des points identifiés.
- Interlocuteurs généralement connus et en nombre restreints.
- Traçabilité.

3 - Diffusion

Caractéristiques :

- Communication unidirectionnelle ; pas de réponse nécessairement attendue.
- Sujets ou problèmes structurés pouvant être formalisés.
- Interlocuteurs non forcement connus et potentiellement en nombre important.
- Mise à disposition du message potentiellement au-delà du groupe de diffusion et dans la durée.
- Message long (plus d'une page).

Les moyens de communication les plus adaptés par rapport à ces contextes de communication sont, de manière générale, les suivants :

1 - Conversation

- Téléphone.
- Messagerie instantanée.
- Face à face.

2 - Message

- E-mail.

3 - Diffusion

- E-mail (liste de diffusion).
- Site collaboratif.

Comme indiqué en introduction, la facilité d'utilisation de l'e-mail en fait l'outil de communication privilégié au détriment d'autres moyens, parfois jusqu'à l'excès.

À titre d'exemple, voici quatre cas d'utilisation non optimale de l'e-mail dans des contextes de « conversation » (ce qui ne veut pas dire que l'e-mail doit être systématiquement proscrit dans ces contextes) :

- **E-mail « ping-pong »** (voir ci-après) : Echanges multiples d'e-mails par allers et retours aggravés par la multiplication des correspondants et les relances multiples sur des sujets secondaires. L'utilisation de l'e-mail conduit à des difficultés à converger et des risques de non conclusion par rapport à une conversation réelle caractérisée par un début et une fin, un fil conducteur et une interactivité riche permettant de mieux focaliser l'échange.

- **E-mail « flamme »** (voir ci-après) : Utilisation de l'e-mail pour exprimer une réaction vive « à chaud » (langage familier, utilisation des majuscules, contenus non maîtrisé). Autant une réaction vive peut être compréhensible quand elle reste informelle et liée à un contexte que partagent l'ensemble des interlocuteurs présents autant elle risque d'être mal comprise lorsqu'elle est réalisée sur un support permanent dans le temps et susceptible de diffusion en dehors du contexte initial.

- **E-mail « d'évitement » :** Envoi d'un e-mail pour éviter de discuter d'un problème ou pour en transférer la responsabilité à une autre personne. Ce type de communication requiert des interactions « riches » peu compatibles avec le caractère « impersonnel » de l'e-mail notamment en ce qui concerne la résolution des conflits.

- **E-mail « d'échanges répétés des versions d'un document » :** L'échange et la convergence sur un document sont réalisés de manière beaucoup plus rapide à travers un échange simultané et interactif sur un document partagé (via messagerie instantanée, web-conférence ou réunion par exemple) plutôt que par des échanges répétés et successifs de multiples versions d'un document pour chaque modification individuelle.

L'optimisation de l'utilisation de l'e-mail consiste donc d'abord à :

- Communiquer de manière pertinente en s'assurant que le contenu de sa communication est bien approprié par rapport aux interlocuteurs qui la recevront.

- Limiter le recours à l'e-mail lorsque d'autres moyens de communication s'avèrent plus adaptés.

Dans un contexte de « diffusion », il est préférable de mettre à disposition des informations de référence d'entreprise (message d'entreprise, note de service,…) sur des sites intranets largement et facilement accessibles et consultables dans le temps, quitte à ensuite en avertir une population limitée en fournissant le pointeur sur l'information.

Le choix du meilleur moyen de communication peut aussi dépendre du statut de disponibilité ou du moyen de contact préférentiel affiché par le correspondant (cela implique généralement l'utilisation de la messagerie instantanée couplée au calendrier). Par exemple, pour une personne affichant un statut « disponible », le meilleur moyen de communication est la messagerie instantanée ou le téléphone alors qu'une personne affichant un statut « non disponible » ou « en réunion » le sera par e-mail.

Rappelons que le bénéfice d'une communication rapide et universelle attribué à la messagerie ne peut être réalisé que si l'ensemble des membres de l'entreprise disposent de la messagerie. Dans le cas contraire, la diffusion des notes de services, des messages d'entreprise, voire la dématérialisation et la circulation des formulaires (demandes RH,…) nécessitent des circuits complémentaires coûteux (réunion de service, diffusion papier,…) pour les personnes non équipées.

Maîtriser et mettre en forme les e-mails émis pour faciliter leur exploitation

Ce paragraphe, volontairement pratique, est destiné à être lu en face de votre ordinateur.

Le bon usage de l'e-mail s'applique aux points suivants :

- **Adressage**
- **Transfert et réponse**
- **Titre et « descripteurs »**
- **Rédaction**
- **Formule de politesse et signature**
- **Pièces jointes**
- **Vérification avant envoi**

Adressage

« A: » (« To ») : A l'attention de

- C'est là que vous indiquez l'adresse e-mail de votre correspondant. Il s'agit généralement du destinataire « pour action ». En règle générale, ne mettez QU'UN SEUL correspondant.

« Cc : » En copie

- C'est la que vous indiquez l'adresse e-mail des personnes que vous mettez en copie, c'est-à-dire que vous souhaitez informer de votre e-mail sans pour autant que ces personnes n'agissent nécessairement.

- En anglais « Cc » qui signifie « carbon copy », et est un héritage du monde papier lorsque l'on demandait à sa secrétaire de taper une lettre en 3 exemplaires, celle-ci insérait un papier carbone entre les feuilles de papier de sa machine a écrire pour créer les copies requises.

- Chaque personne en copie doit l'être pour une raison définie. De manière générale, dans un contexte de faible volume de communication et de coordination hiérarchique forte, la mise en copie systématique est supportable. Elle le devient beaucoup moins dans un contexte de surcharge du volume des e-mails et de coordinations multiples (hiérarchique, fonctionnelle, matricielle, par projet, transverse).

« Cci (« Bcc »): » Copie carbone invisible ou Copie cachée

- En anglais « Bcc» « blind carbon copy » ou copie cachée, est une facilité à utiliser avec soin ; elle permet de mettre quelqu'un en copie SANS que les correspondants ou les personnes en copie officielle en soient informés.

- Notez que 2 personnes mises en « Cci » ne sauront pas réciproquement qu'elles sont mises en copie. Vous pouvez également vous mettre vous-même en « Cci » pour vérifier que votre courrier est effectivement délivré et sous quelle forme il est reçu.

- Utilisez avec circonspection les « copies cachées ». N'oubliez pas que le destinataire peut les transférer ou faire « répondre à tous ».

Listes de diffusion : [liste de contacts. par exemple, liste de membres d'un groupe de travail, d'un projet,…]

- Elles peuvent être utiles mais elles constituent une source potentielle d'adressage inadéquat et ne doivent donc être utilisées qu'avec précaution dans un contexte de surcharge du volume des e-mails. L'utilisation des listes de diffusion fonctionnant sur abonnement permet de gérer les échanges centrés sur des communautés dédiées.

Carnet d'adresses

- Utilisez un carnet d'adresses électroniques pour conserver toutes les adresses de vos correspondants. Cela permet un gain de temps appréciable. Vous pouvez également créer des « surnoms » à partir des initiales du correspondant, par exemple : Jean Dupond a une adresse e-mail jean.dupond@masocieteamoi.fr et peut se voir associer un surnom « jd ».

Transfert et réponse

« Transférer » (« Forward »)

- Précisez s'il s'agit d'un transfert pour info (FYI : « For Your Information ») ou pour action, si possible dans le titre de l'e-mail.

- Résumez un échange d'e-mails transférés s'il est très long pour éviter de faire lire 12 pages. Sinon, le transfert s'apparente à un délestage (à toi de jouer !)

- Attention à la confidentialité des informations d'un échange d'e-mails transférés. Il se peut que

le bas de l'échange ne concerne pas les personnes à qui vous transférez l'e-mail.

« Répondre » (« Answer »)

- Prenez en compte le délai de réponse (évitez l'e-mail urgent le vendredi soir à 22h00).
- Répondez selon les règles de la charte d'entreprise. Par exemple dans les 48 heures ouvrables pour les e-mails internes qui vous sollicitent personnellement et explicitement et dans les 24 h pour les e-mails provenant de l'extérieur.
- Pensez à mettre s'il le faut l'assistant(e) du Groupe / Division en copie s'il s'agit de quelque chose d'important dont le suivi est impératif.
- Si vous n'avez pas les éléments d'information pour répondre, répondez tout de même en indiquant que vous n'avez pas l'information mais que vous prévoyez de l'avoir pour le tant, ou qu'il faut contacter telle personne.
- Si vous n'êtes pas la personne concernée, ne faites pas le mort ; orientez votre correspondant vers la personne adaptée ou répondez lui que vous n'êtes pas la personne adéquate.
- Répondez aux e-mails pour lesquels vous n'êtes qu'en copie que si vous avez une vraie valeur ajoutée à apporter. Encore une fois, si vous êtes en copie, cet e-mail vous est normalement adressé pour information uniquement. Si vous répondez, vous tomberez dans le « ping-pong » (voir ci-après)

« Répondre à tous » (« Answer all ») :

- Repositionnez les personnes en destinataire et en copie.
- N'abusez pas du « Répondre à tous » pour dire « merci », ou « je ne pourrai pas assister à la réunion », faites une réponse juste à l'émetteur.
- Pensez à réduire systématiquement le nombre de personnes destinataires dans un « répondre à tous ».
- Modifiez le titre des e-mails dès que le contenu des e-mails change.
- Lorsque vous êtes investi de la responsabilité associée à un échange d'e-mails qui commence à être long, faites un résumé avant de poursuivre. D'ailleurs, là aussi, il vaut mieux changer le titre de l'e-mail. Par exemple avec « SUJET chose : Point au 29/10/1999)

E-mails « Ping Pong » :

- L'e-mail ping-pong consiste en un envoi successif d'e-mails au sein d'un groupe d'individus sur le même sujet ou avec des relances multiples sur des sujets secondaires avec à chaque fois quelques commentaires personnels et souvent peu de valeur ajoutée. Dans le pire des cas, l'e-mail ping-pong finit avec des participants qui n'étaient pas présents au début des échanges.
- Il faut arrêter à la troisième itération, passer ensuite au téléphone ou à la messagerie instantanée ou planifier une réunion. Voire, s'abstenir de participer.
- Utilisez la fonction de la messagerie qui permet de regrouper tous les e-mails d'un même échange pour faciliter leur suivi.

E-mails « Flamme » (« Flame ») :

- Les e-mails « flamme» sont des e-mails contenant beaucoup d'adrénaline, de mise en cause d'autrui. Ils sont créés spontanément lorsque quelqu'un a quelque chose à reprocher à quelqu'un d'autre. Ils interviennent également dans le cadre de discussions qui s'enveniment.
- La mauvaise interprétation du contenu de ces e-mails et la forte probabilité que le destinataire de l'e-mail réponde violemment exacerbe souvent la situation. Dans une discussion en face à face ou au téléphone, on peut jouer avec l'intonation de la voix. Au contraire les e-mails « flamme» contiennent souvent des tentatives d'humour, de l'ironie, du sarcasme qui sont souvent mal interprétés. Les e-mails impulsifs peuvent circuler dans les boîtes aux lettres, être imprimés, et acquérir un degré d'importance qui n'était pas prévu au départ. Ils constituent une réelle barrière à une communication efficace et peuvent avoir un impact négatif sur la productivité et les relations interpersonnelles.
- Si vous vous apprêtez à envoyer un e-mail « flamme» en réponse à un autre e-mail, prenez cependant la précaution de bien lire l'e-mail que vous avez reçu et qu'il n'y a pas de risque de mauvaise interprétation. Si vous utilisez de l'humour ou de l'ironie, faites en sorte que ce soit clairement identifié comme tel, par exemple avec des « smileys » (☺).

- Avant d'envoyer un tel e-mail, assurez-vous de plusieurs choses. D'abord qu'il n'y a pas d'autre moyen efficace de communiquer (téléphone, réunion). Ensuite, après avoir écrit votre e-mail, laissez-le reposer quelque temps. Revenez dessus ensuite pour voir si vous ne regretteriez pas de l'avoir envoyé. Vous pouvez aussi le faire lire par un proche. Une fois assuré, vous pouvez l'envoyer.

Titre et « descripteurs »

Titre:

- Indiquez clairement le titre de votre e-mail de façon la plus concise, compréhensive et claire. Pensez que votre interlocuteur reçoit beaucoup d'e-mails chaque jour. Donnez lui envie de lire votre e-mail.

- Le titre doit favoriser le repérage de l'e-mail dans une liste lorsque le contenu n'est pas dévoilé. Il doit donc résumer le contenu (du type : points clé, contexte, objectif,…) par exemple « préparation réunion client du XX » et non pas « problème » ou « discussion ».

- Ne traitez qu'un seul sujet par e-mail. S'il y a deux sujets distincts, faites deux e-mails séparés.

- Expliquez si nécessaire l'action à faire : « pour action », « pour information » (FYI : « For Your Information »)

« Descripteurs »

- Utilisez les descripteurs (drapeaux de signalisation, suite à donner) notamment « urgent » que dans les cas réellement prioritaires.

Rédaction de l'e-mail

« Corps » de l'e-mail :

- Dans le corps de votre e-mail, soyez également clair et concis. Faites des paragraphes (3 paragraphes maximum doivent pouvoir expliquer la teneur de votre message). En règle générale, ne dépasser pas une page d'écran.

- Faites une synthèse des e-mails longs retransmis.

- Ceux qui se sentent plus prolifiques peuvent rédiger un mémo ou un compte-rendu, même court.

Forme / style :

- L'e-mail est un outil de communication. Toute forme de communication comprend une « étiquette ». Rédigez donc les e-mails. Le destinataire ne doit pas avoir à faire des efforts pour lire et comprendre l'e-mail. Celui-ci doit être facilement exploitable en consultation ultérieure ou par d'autres destinataires différents de ceux d'origine.

- Ecrivez en bon français

- Faites attention à un style trop télégraphique ou trop directif

- Evitez les abréviations ou les raccourcis orthographiques (style « SMS »)

- Soyez neutre, factuel et explicite

- Les mots et phrases en majuscule correspondent à une hausse de ton. Par exemple, du bon usage des CAPITALES : Vous pouvez écrire « Je vous demande de revoir votre prix » ou « JE VOUS DEMANDE DE REVOIR VOTRE PRIX ». Dans le deuxième cas, vous indiquez que vous CRIEZ ! Ce qui n'est peut être pas votre intention !

- Si vous utilisez l'humour ou l'ironie qui ne seront pas forcement identifiés comme tel dans un message formel utilisez des smileys (☺) pour le préciser.

Formule de politesse et signature des e-mails :

Formule de politesse

- Utilisez les marques de considération de la correspondance (Monsieur / Madame, Cordialement, Merci par avance). Soyez bref dans vos formules de politesse. Vous pouvez également indiquer des formules plus développées si les circonstances s'y prêtent.

Signature

- Les signatures automatiques e-mails sont très utiles. Elles doivent cependant être courtes (maximum 2/3 lignes) et sans fioritures excessives. Le basique est d'indiquer vote nom, votre titre, votre e-mail et votre téléphone.

- Une notice légale doit compléter la signature

- L'adresse du site Internet de votre société peut compléter la signature

- Vous pouvez ajouter un « disclaimer » (clause d'exclusion ou de limitation de responsabilité)

- Evitez d'insérer une image trop volumineuse dans votre signature

Pièces jointes

- Vous avez l'opportunité de joindre des fichiers à vos e-mails (photos, feuilles de calcul, etc.). Cette fonction est souvent représentée par un « trombone » dans la plupart des logiciels de messagerie.

- Lorsque les pièces jointes sont trop volumineuses (plus de 1 à 2 Mo), privilégiez des solutions de travail collaboratif.

Vérification avant envoi

- Relisez vos e-mails avant de les envoyer.

- N'oubliez pas que si votre message est soporifique et que vous l'envoyez à 10 personnes, vous forcez 10 personnes à perdre leur temps ! Quelle mauvaise publicité ! Evitez ce désagrément et RÉ-ÉCRIVEZ votre e-mail.

- Un e-mail n'est jamais entièrement confidentiel : évitez de répondre sous l'emprise de l'émotion ou de diffuser librement des informations confidentielles.

- N'oubliez pas que ceux qui reçoivent les e-mails peuvent les conserver ou les transmettre à des personnes autres que les destinataires d'origine. Les e-mails peuvent aussi être examinés lors de procédures judiciaires et les commentaires « informels » que vous avez fait par e-mail peuvent être mis en lumière (et apparaître sous un éclairage différent).

Utiliser les règles de productivité pour le traitement et l'organisation des e-mails

Consultation et traitement des e-mails

- Limitez la fréquence de consultation et de traitement des e-mails à des plages fixes dans son agenda (par exemple matin, midi, après-midi et soir) et supprimez l'affichage des alertes e-mails.

- Utilisez le « volet de lecture » de votre logiciel de messagerie afin de visualiser le contenu de vos e-mails en même temps que la liste des e-mails.

- Utilisez la visualisation par conversation (« thread ») pour condenser l'ensemble des échanges à partir d'un même e-mail de départ

- Réalisez une action pour chaque e-mail consulté. **Une règle applicable par exemple est celle des 4 D** : Do (faire), Delete (supprimer), Defer (différer, marquer l'e-mail pour suivi), Delegate (déléguer).

- Indiquez à vos correspondants de ne plus vous envoyer certains e-mails s'il n'est pas pertinent que vous les receviez.

- Organiser des dossiers de classement (arborescence structurée) dans la messagerie en fonction des thèmes (dossier client, dossier fournisseur,…) et de vos priorités (traitement / recherche). Une fois lu ou envoyé, un message peut être rangé dans un dossier.

- Utiliser des règles de classement automatique pour vous aider à traiter vos e-mails. Par exemple, faites des répertoires avec les e-mails adressés en direct, en copie, venant de votre supérieur direct, venant de liste de diffusion, etc…. Créez notamment des répertoires spécifiques pour les e-mails non prioritaires dans l'activité : lettres d'informations, correspondances personnelles,…

- Utilisez des marqueurs de suivi pour les e-mails à traiter ou en attente de réponse.

- Utilisez systématiquement un moteur de recherche local pour rechercher des e-mails ou des fichiers (recherche effectuée quelque soit la localisation de l'élément en bénéficiant de la puissance de l'indexation préconstituée).

Archivage (voir fiche n° 6)

- Définissez des règles de conservation des e-mails. Par exemple archivez tout ce qui a plus de 3 mois ou identifiez ce qui a une valeur juridique pour en réaliser un archivage à part.

- Définissez le mode d'archivage (un ou plusieurs fichiers archive, en local ou sur le réseau, automatisé ou manuel,..).

Délégation et absence

- Indiquez votre statut d'absence si vous n'êtes pas en mesure de consulter vos e-mails afin que vos correspondants puissent adapter leur communication si nécessaire (renvoi automatique d'un e-mail d'absence).

- Utilisez les règles de délégation si vous partagez des boites de messagerie au sein d'une équipe ou entre un manager et son assistante.

- De manière générale évitez l'utilisation de boites e-mails « génériques » du fait de la complexité introduite par la gestion et la mise à jour des règles de routage.

Optimiser l'organisation et le suivi des réunions à partir du calendrier

L'efficacité des réunions constitue un sujet clé de la performance collective. La « réunionite » est souvent décrite comme un des maux dont souffrent les entreprises françaises. Les réunions sont considérées comme trop longues, trop nombreuses, ayant trop de participants, redondantes entre elles, insuffisamment préparées et peu suivies d'effets.

Le contrôle de l'opportunité, de la pertinence et des règles de réunions relève de décisions de management totalement indépendantes du recours aux outils. L'utilisation d'outils ne fait que procurer un instrument de planification, de mesure et de suivi pour le management.

En terme de planification, l'organisation des réunions est liée à l'e-mail dans le sens où celui-ci constitue souvent le seul outil support utilisé (envoi des invitations par e-mail, retour par e-mail, replanification éventuelle de la réunion par e-mail, envoi de documents supports par e-mail).

L'utilisation systématique et généralisée dans l'ensemble de l'entreprise du calendrier pour l'organisation des réunions permet :

- *de rechercher directement des dates de disponibilités sans avoir à échanger des e-mails dans cette phase préparatoire,*
- *de mettre à jour automatiquement les calendriers des participants,*
- *de collecter directement et de manière centralisée les réponses des différents participants,*
- *de replanifier facilement une réunion en mettant à jour automatiquement les calendriers de l'ensemble des participants.*

L'utilisation du calendrier permet ainsi de limiter significativement les e-mails échangés.
Le calendrier peut aussi être utilisé, à travers les formulaires de création de réunion, pour promouvoir des règles d'efficacité des réunions fixées par le management. Par exemple, la création d'une réunion peut nécessiter de renseigner obligatoirement un objectif, un ordre du jour, une liste de participants et une salle de réunion.

Dans certains cas précis (nombre de participants important, réunion d'information), il peut être plus pertinent d'utiliser d'autres moyens de communication (publication sur un site de partage par exemple).

La publication des documents support de réunion sur un site intranet dédié contribue aussi à améliorer l'organisation et le suivi des réunions en permettant :
- La mise à disposition et la mise à jour des documents supports de réunion,
- La collecte des comptes-rendus de réunion,
- Le suivi de plan d'action dans la durée suivant la réunion,
- La conservation et la mise à disposition des contenus des réunions au-delà du groupe des participants aux réunions.

Favoriser l'utilisation des espaces collaboratifs (cf. fiche 2)

L'utilisation de la messagerie se fait souvent au détriment des sites collaboratifs de partage de documents. Favoriser l'utilisation des sites collaboratifs conduit à soulager la messagerie ainsi qu'à développer le partage des connaissances des entreprises. La création et le développement de l'utilisation des sites collaboratifs concernent notamment les sites de projets, d'initiatives, d'équipes ou portant sur des domaines ou sujets de capitalisation d'information.

Fiche 2

Les limites de l'usage de l'e-mail, au profit des autres outils de communication et de collaboration

Sommaire

Limites de l'e-mail dans le travail collaboratif

L'e-mail : un outil collaboratif « en apparence » seulement

L'envoi d'un e-mail à un groupe de travail est d'une facilité tentante. La plupart des clients de messagerie permettent en quelques clicks d'envoyer un ou plusieurs fichiers attachés à une personne, ou à un groupe de travail, dont on souhaite solliciter l'avis ou un travail de modification.

Cette facilité et ce « don d'ubiquité » (envoyer presque instantanément à plusieurs personnes dans plusieurs lieux) ont représenté un gain énorme dans les années 1995 à 2000 pour la circulation de l'information, l'échange, et le travail en équipe.

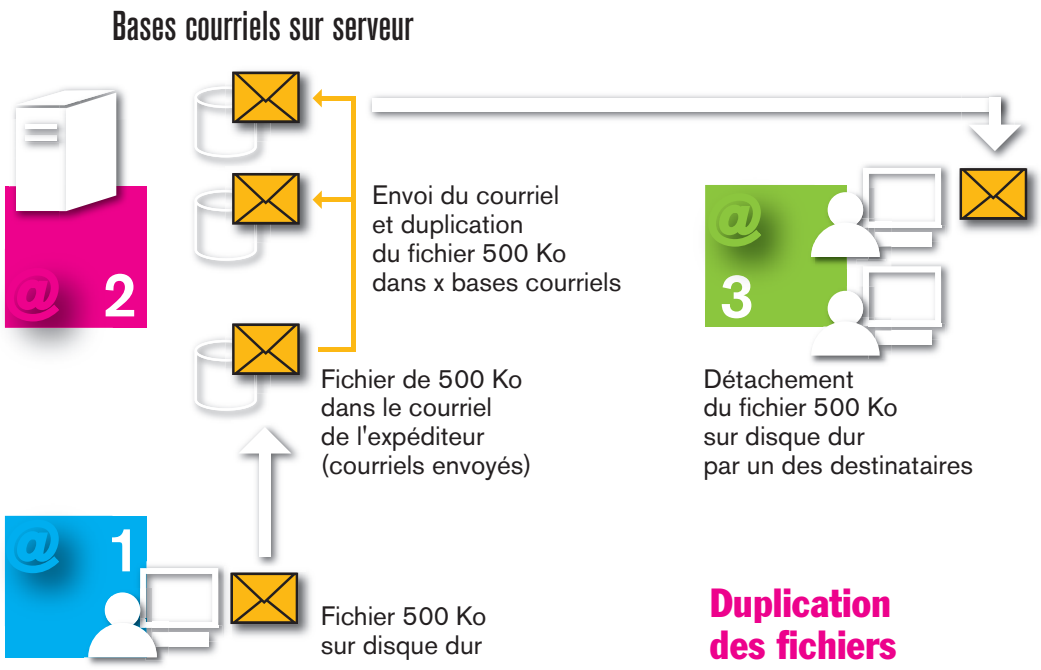
Pourtant, une étude plus détaillée des processus de travail collaboratif laisse apparaître de réelles limites de l'utilisation de l'e-mail. D'autre part, depuis les années 2000, de nouvelles applications ou technologies et des méthodes de travail collaboratif plus abouties permettent de combler de nombreuses limites développées dans ce chapitre.

Nous traiterons ici des exemples de travail collaboratif au sein d'une même organisation, c'est-à-dire pour des personnes d'une même entreprise, bénéficiant d'un même réseau d'entreprise et des mêmes outils de messagerie.

L'extrapolation des explications ci-dessous à un travail collaboratif dans une entreprise étendue (société, fournisseurs, partenaires, voire clients) reste tout à fait possible, mais nécessite quelques investissements d'infrastructure supplémentaires (zone d'échange Extranet, sécurité via une DMZ ou zone Démilitarisée, parfois interface entre applications,…)

Limites dans l'utilisation de l'e-mail

Des dangers peuvent apparaître comme : la duplication de contenu, le suivi des versions, la traçabilité des processus, la sécurité, la reprise de l'historique lors de la remise d'un dossier à un nouveau collaborateur.



Etapes du phénomène :

1- L'expéditeur attache un fichier de 500 Ko de son disque dur (ou de son espace disque sur le réseau) dans un e-mail à envoyer à 2 personnes. Ce fichier se retrouve alors également sur le serveur de messagerie, dans la base e-mail de l'expéditeur (section « messages envoyés »)

2- L'envoi à 2 personnes de l'e-mail dépose dans la base mail de chaque destinataire ce fichier de 500 Ko.

3- Il est souvent probable qu'un (ou plusieurs) des destinataires enregistre également le fichier sur son disque dur ou son unité réseau.

Ce scénario avec 3 personnes met en évidence qu'un simple fichier de 500 Ko finit par occuper entre 2 Mo et 3 Mo (et nous ne développons pas ici les possibles réponses et « faire suivre » avec les pièces jointes qui resteront parfois attachées).
L'effet exponentiel de cette duplication (reportons nous aux volumétries indiquées dans le dossier et aux nombres d'e-mails et de fichiers que vous recevez ou envoyez chaque jour) a forcément des répercutions techniques sur les espaces disques.
L'espace disque est aujourd'hui peu cher, mais pas gratuit…

Ces pratiques sont également préjudiciables au niveau du suivi et de l'organisation.

Derrière ces dangers se profilent des enjeux business : erreur possible, perte de temps, non-conformité aux exigences d'un donneur d'ordre …

La duplication du contenu

Au niveau technique tout d'abord, l'envoi d'un mail à plusieurs personnes avec des fichiers attachés multiplie d'autant le volume occupé sur les espaces disques.

La figure ci-dessus explique le phénomène qui se produit régulièrement au sein d'une entreprise.

La notion de suivi des versions

L'envoi d'un e-mail avec une pièce jointe peut avoir deux objectifs :

- Informer les destinataires de l'intérêt du document attaché pour lecture, classement,

etc…Dans ce cas, nous pouvons supposer qu'aucune action supplémentaire n'est requise (bien que cela soit plus subtile).

- Demander un travail de modifications ou de complément aux destinataires.

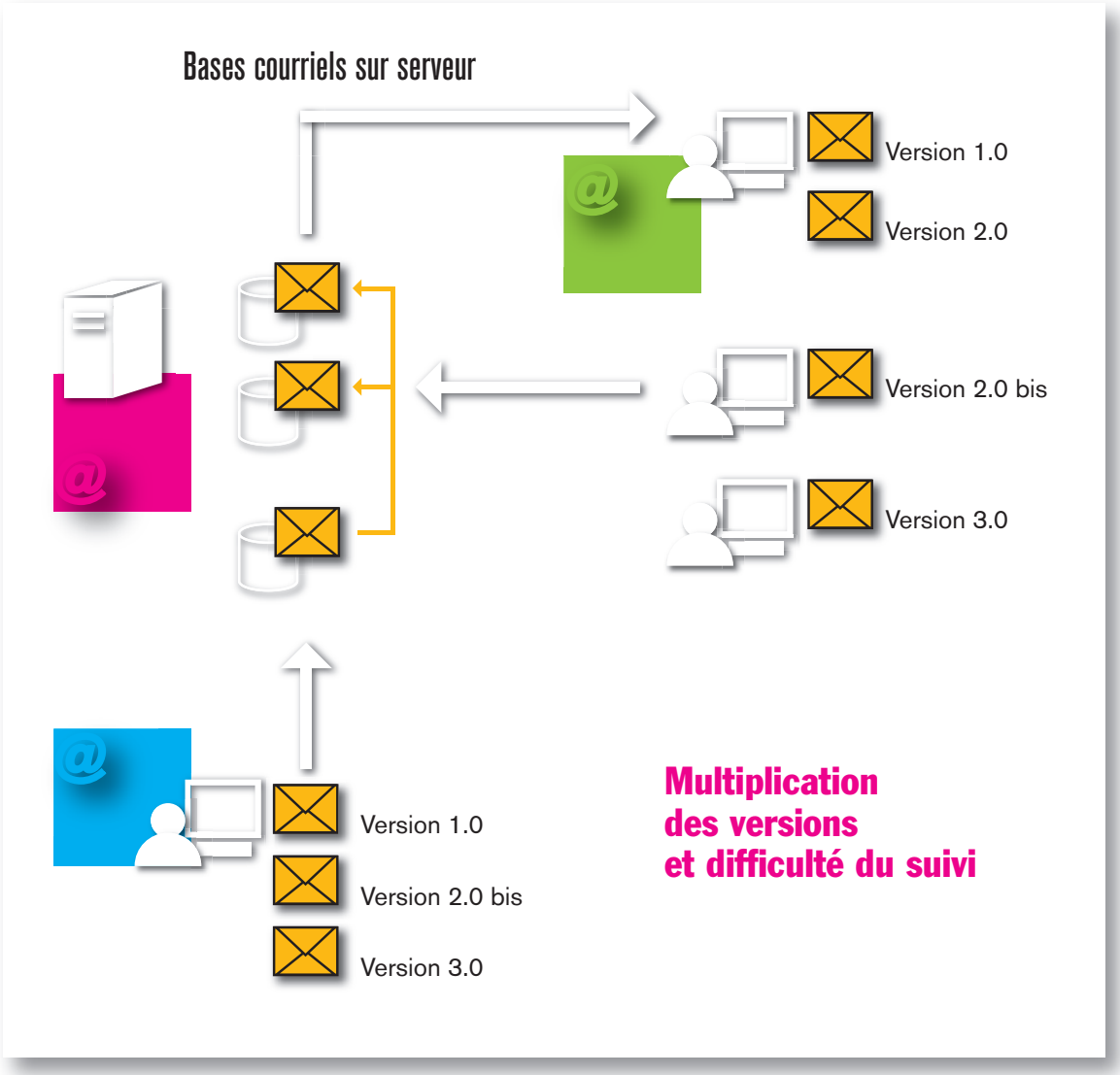
Dans le deuxième cas, les limites de la collaboration par e-mails sont clairement atteintes. La figure ci-dessous en donne un exemple.

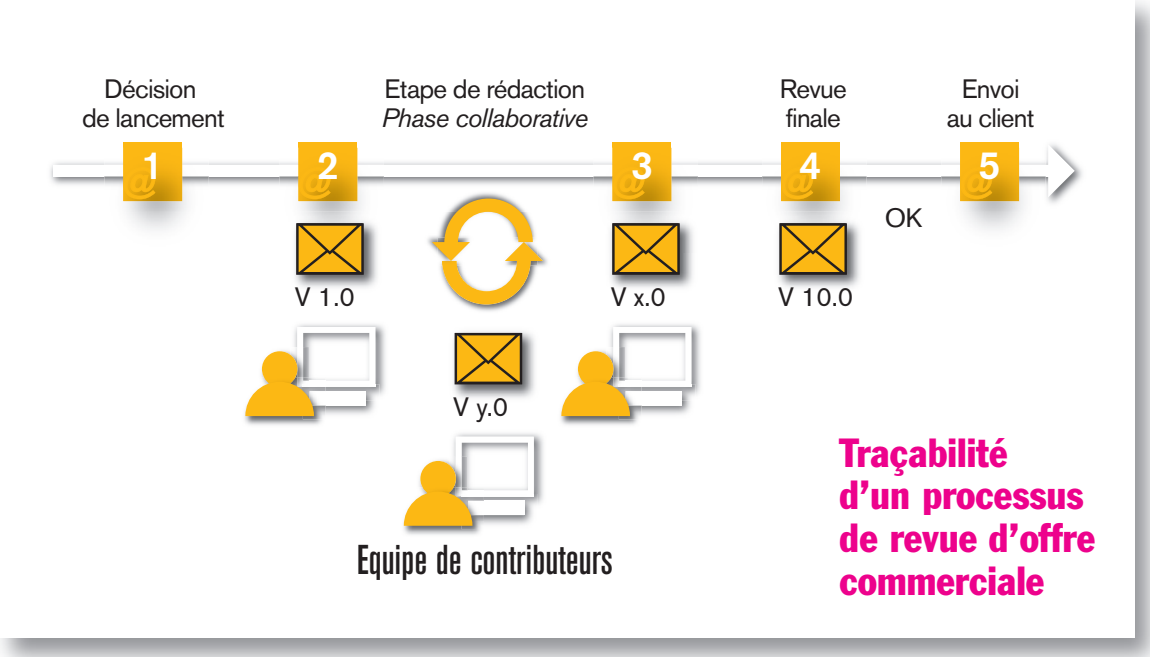
Dans le cas d'une demande de contribution de plusieurs personnes, chacun va alors enregistrer le fichier joint à l'e-mail sur son disque pour le modifier, puis retourner une version complétée à l'expéditeur initial (avec parfois en copie les autres contributeurs).

Il en résulte la circulation de plusieurs versions (version 1.0, version 2.0 ou 2.0 bis, modifiée par une autre, la version 3.0 qu'un contributeur aura modifiée à partir de la version 2.0, en oubliant la version 2.0 bis, etc...).

Nous retrouvons l'impact technique sur la duplication des fichiers, mais surtout, les chances de retrouver et utiliser une version bien mise à jour et complète deviennent limitées.

Pour un document complexe avec 3 ou 4 contributeurs et une durée de rédaction collaborative de 2 ou 3 semaines, donc plusieurs mises à jour et compléments (un contrat commercial complexe, un document technique pointu, …), la plus grande rigueur des participants aura du mal à venir à bout du risque de présenter une version incomplète à la fin.





Le déroulement d'un processus et la traçabilité

Le processus de revue de contrat ou de revue de proposition commerciale est un processus classique dans les entreprises, surtout depuis la norme ISO V2000.

Il s'agit de démontrer que les différentes étapes du processus sont bien respectées. Ce processus reprend en général les étapes suivantes (voir figure ci-dessus) :

- décision de lancement de la proposition,
- étape de rédaction,
- phase de revue finale,
- décision d'envoyer le document final et validé au client,….

La notion de processus est très importante aujourd'hui dans le travail collaboratif (s'assurer que tous les acteurs déroulent une méthode de travail maîtrisée aboutissant à une bonne qualité du document).
Après plusieurs semaines de travail, la collaboration de 4 ou 5 contributeurs compétents, il est souvent délicat de consolider toutes ces étapes et de s'assurer qu'elles ont toutes été respectées. Cela est d'autant plus délicat lorsque tout le processus s'est déroulé par envoi d'e-mails, réponses, échanges de pièces jointes, via le système de messagerie.

Même si tous les mails sont conservés précieusement (voir par exemple fiche 6), il sera toujours difficile de s'assurer que toutes les étapes d'un processus sont bien respectées, en raison de la multitude des e-mails échangés, mais aussi parce que le mail ne garantit pas le respect d'une étape ou un envoi par erreur avant l'étape de validation finale (lorsque c'est un envoi par erreur au client, les impacts peuvent être importants…). C'est une des limites majeures du mail dans le mode collaboratif : la « non traçabilité » et le manque de fiabilité des étapes.

La sécurité

La sécurité est également le point faible de l'e-mail en mode collaboratif.

Une proposition doit circuler entre les personnes nécessaires, mais ne pas forcément être accessible par d'autres personnes de l'organisation.

Bien que la plupart des serveurs de messagerie proposent des fonctions anti-copie, anti « faire-suivre », la plupart des utilisateurs ne les utilisent pas.

Ainsi, le fichier attaché ne profite d'aucune sécurité en particulier et peut tout à fait être envoyé à d'autres personnes, en dehors de l'équipe de travail.

Le mail n'assure pas de sécurité propre au document et même un document word avec mot de passe n'est pas suffisant. Un mot de passe se communique aussi… par e-mail…

La remise du dossier à un nouveau collaborateur

Paradoxalement au fait que la sécurité soit très pauvre dans une organisation collaborative fondée uniquement sur le mail, il est souvent délicat, dans ce mode de fonctionnement, d'intégrer un nouveau collaborateur.

Lorsqu'un nouveau membre arrive dans l'équipe qui travaille sur un sujet, comment lui donner une bonne compréhension du travail en cours et du dossier ?

La seule solution est souvent de lui faire suivre les multiples e-mails contenant fichiers attachés et remarques en essayant de ne pas oublier un e-mail important.

Ces quelques exemples concrets d'une équipe de travail fondant le travail collaboratif uniquement sur l'utilisation de l'e-mail démontre combien l'outil de messagerie a ses limites dans ce contexte.

Il existe aujourd'hui d'autres applications plus adaptées, qui utilisent l'e-mail en mode « notification », c'est-à-dire pour avertir les contributeurs, sans que l'e-mail ne porte un contenu trop important.

Des solutions collaboratives possibles :

Les applications de Gestion Documentaire Collaborative

Le marché des applications collaboratives est aujourd'hui assez vaste, tant au niveau des applications dites « Middle-Market », donc pour PMEs, que des applications adaptées à des entreprises multinationales. Pourtant, ce marché a atteint une certaine maturité et on peut trouver quelques propriétés communes :

- Les applications se fondent sur un système documentaire, associant une fiche documentaire à un ou plusieurs fichiers. Ces fiches permettent de définir le classement, le thème, le type et certaines propriétés du document et assurent le suivi en version et modification du document.

- Les droits d'accès et la sécurité sont explicites au niveau de la fiche documentaire et du système documentaire : qui peut modifier, qui peut avoir accès en consultation, etc…et ne dépendent pas des destinataires d'un e-mail.

- La création d'un environnement projet ou collaboratif. Les membres y sont explicitement inscrits et personne d'autre ne peut voir les documents dans cet environnement.

- L'application envoie aux membres de l'équipe des e-mails pour toutes modifications ou événements, avec un lien vers les fiches documentaires. Le mail ne porte que peu d'information, ne génère pas de duplication de contenu et peut être effacé. Il ne porte pas non plus de droits d'accès. Ainsi, même si une personne reçoit ce mail par erreur, le lien ne marchera pas si elle n'est pas connue du système.

- L'application est souvent associée à un moteur de processus, parfois très simple, permettant d'assurer que certains documents sont bien soumis à certaines étapes de validation par les bonnes personnes afin de poursuivre leur « cycle de vie ».

- Enfin, suivant les éditeurs, on trouvera des fonctions pour gérer le nomadisme (accès à certains documents depuis l'hôtel ou l'avion), du « reporting », des moteurs de recherche avancée, etc….

Le sujet n'est pas ici de mettre en avant un éditeur ou un autre, mais vous pouvez conseiller à votre responsable informatique de se rendre à certains salons sur le sujet, comme :

- Salon Documation
- Forum de la GEIDE

D'autres outils de partage et d'interaction

Il existe aussi d'autres applications permettant d'éviter l'usage de l'e-mail de manière inadaptée et d'encombrer les messageries :

- Le système de conférence audio ou vidéo, avec partage de tableau blanc et de fichier, pour une contribution de chaque participant et un travail d'équipe en temps réel.

- Les messageries instantanées pour discuter et tracer une conversation rapide sur un thème pointu.

Il existe là aussi différentes solutions avec des coûts de mise en ligne réduits (et parfois l'achat de WebCam). Cependant, prenez soin d'en parler avec votre responsable informatique car cela nécessite quelques adaptations du réseau et de la sécurité.

Le rôle de l'e-mail dans les applications métiers

Nous avons vu que dans les applications collaboratives, l'e-mail était un simple moyen de notification pour différents acteurs, et qu'il ne portait plus de contenu, ce contenu étant protégé dans l'application collaborative.

Ce même mécanisme est également utilisé dans les moteurs de processus ou moteurs de Workflows, souvent utilisés dans une approche « BPM » ou « Business Process Management ». A chaque étape du processus, l'acteur ayant à faire une activité précise reçoit un e-mail de notification par le système, avec un lien vers l'application et l'écran sur lequel il doit agir. Ainsi, l'e-mail est dans ce cas un outil que l'application de processus utilise pour prévenir et informer chaque acteur.

On retrouve ce même principe dans de nombreuses applications de GRC (Gestion de la Relation Client) ou SAV (Service Après-vente) où tout évènement sur le client inscrit dans l'application est notifié aux personnes en relation avec le client. Cela peut être une demande du client directement formulée sur un site web, un incident sur une machine vendue au client, remonté par un commercial vers le service technique, etc…

Dans ces cas de figure, l'application envoie elle-même des e-mails aux utilisateurs pour les notifier d'une action à faire. Cela évite aux utilisateurs d'avoir à se connecter régulièrement ou de faire des recherches pour savoir si un événement les concerne. Ainsi, ils peuvent se concentrer sur leurs activités, sans craindre de manquer une action, car leur messagerie recevra alors un e-mail.

Enfin, l'e-mail peut parfois être utilisé comme un robot pour qu'une application reçoive des informations. Il s'agit des mails dits « structurés ».

Prenons par exemple le cas d'un technicien de maintenance, M. Durant, en visite chez un client dans l'est de la France, la société « RapidEmballage ». Suite à analyse d'une machine chez le client, il découvre un défaut que le bureau d'étude doit analyser.

Soit il peut accéder à l'application de service après-vente pour créer un incident dans le système, soit il rédige un mail suivant un format bien défini, et il peut ainsi l'envoyer au système depuis les locaux du client, ou depuis son hôtel le soir.

Exemple de mail structuré :

« Destinataire : MailSAV@companie.fr

Titre : Incident à déclarer

Corps de l'e-mail :
Auteur de l'incident : Durant
Client : RapidEmballage
N° Machine : X409
Type de panne : fuite hydraulique
Description : « problème de fuite dans la système hydraulique n'assurant pas un bon emballage »

Fin du mail structuré

Cet e-mail sera directement envoyé à l'application qui « décodera » les différents mots clés dans le corps du texte (client, No Machine, etc…) et créera automatiquement un incident dans le système avec les bons attributs. En réponse, l'application enverra un autre e-mail avec le numéro d'incident, au destinataire, mais aussi aux différentes personnes traitant ce client. L'incident pourra alors être complété et les actions pour le résoudre seront prises dès le lendemain.

Ces exemples montrent que l'e-mail n'est pas seulement un échange entre personnes. C'est aussi un outil qui peut être utilisé par les applications pour communiquer avec différents acteurs.

Messagerie unifiée

Définition, Usages et Bénéfices

Définition

Les collaborateurs sont équipés de différents terminaux : téléphone fixe, mobile Dect ou Wifi, GSM, ordinateur, PDA, etc et de différentes messageries (vocales, sms, fax et e-mail).

Ils ont également besoin de consulter simplement leurs messages en tout lieu et à tout moment.

Mettre en œuvre une solution qui permette d'unifier les différentes messageries et de gérer ses messages par le média de son choix devient un atout pour l'entreprise et l'efficacité individuelle des collaborateurs.

Adoption de la messagerie unifiée en entreprise

La messagerie électronique maîtrisée par la majorité des employés, peut être le point de convergence des différents outils de messagerie.

Exemples et scénarios d'usage

- Disposer d'un numéro unique fax/tel/GSM ;
- Écouter un message vocal déposé sur son téléphone fixe à partir de son mobile, avec authentification automatique ;
- Ecouter un e-mail en synthèse vocale en filtrant les e-mails lus, par exemple lecture uniquement des e-mails d'un client spécifique ;
- Envoyer un fax par l'interface de messagerie électronique pour une commande, et recevoir un accusé de réception automatique d'une demande de service ;
- Réceptionner un fax confidentiel sur son poste de travail directement ;
- Envoyer des SMS de confirmation de livraison automatique via une application métier (pour limiter les appels entrants et augmenter la qualité de service) ;
- Etre prévenu par SMS de l'arrivée d'un message vocal sur mon poste fixe avec les coordonnées des interlocuteurs qui ont souhaité me joindre ;
- Transférer un message vocal par simple envoi d'e-mail.

Bénéfices pour l'entreprise

Les bénéfices d'une telle solution peuvent être appréhendés à deux niveaux dans l'entreprise : utilisateurs et exploitants.

Utilisateur

- Gestion des messages simplifiés : homogénéisation des interfaces, consultation des messages par n'importe quel terminal.
- Développement de la mobilité : capacité à recevoir, consulter et émettre des messages quel que soit sa localisation, télétravail, hôtel, hotspot et le terminal dont on dispose.

Exploitant

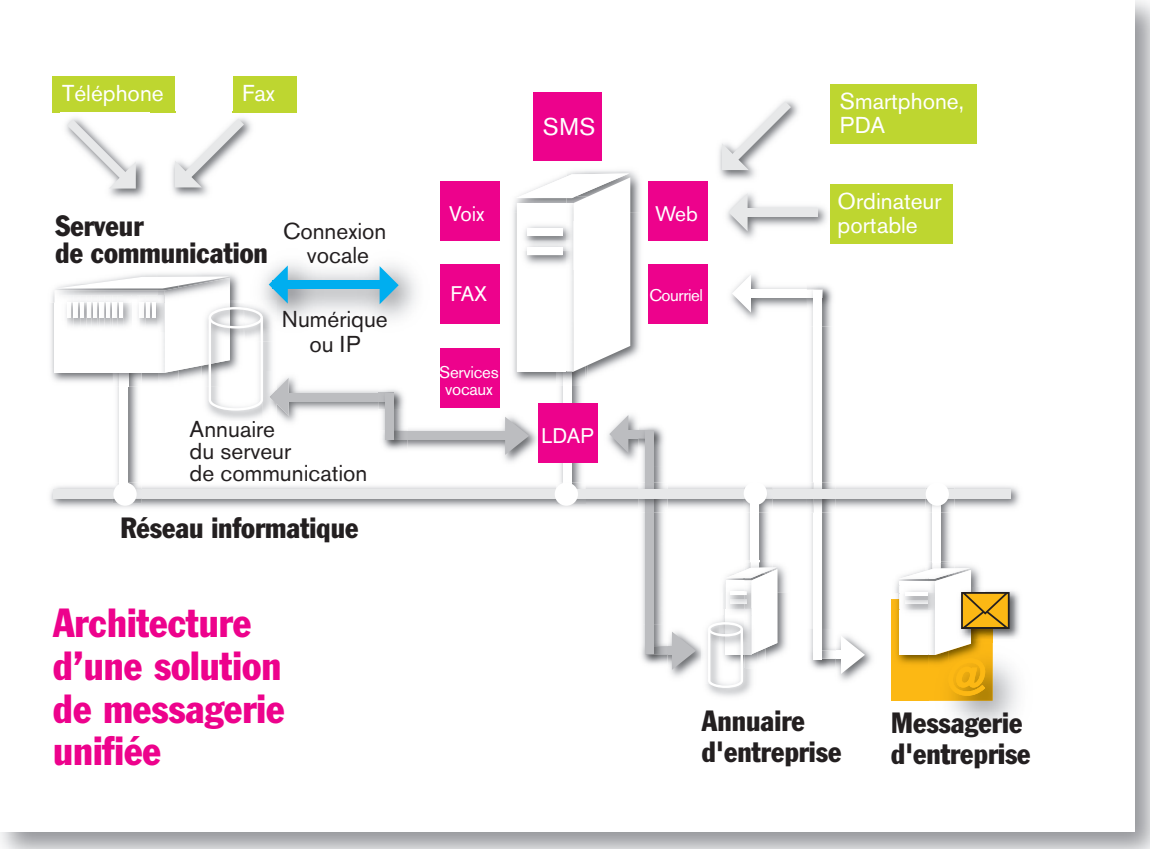
- Rationalisation des infrastructures de messagerie en regroupant les différents services sur un serveur commun (suppression des fax, un seul serveur pour gérer les messages voix, fax, sms).
- Exploitation centralisée

Au delà de ces bénéfices, la messagerie unifiée est un élément qui, associé à d'autres technologies, comme le Couplage Téléphonie et Informatique, permet une réelle intégration avec les applications métiers et devient une fondation d'une stratégie de Communication Unifiée d'entreprise.
Cette Communication Unifiée prend toute sa valeur lorsqu'elle s'intègre avec des processus métiers, ex : envoi automatique d'un fax au client lors d'une confirmation de commande, envoi automatique d'un SMS pour confirmer une intervention de service après vente ou pour notifier le retour d'un article réparé, appel téléphonique lancé directement depuis le PC en réponse à un mail…

Choix d'une solution, Architecture et Mise en Œuvre

Recommandations dans le choix de la solution de messagerie unifiée

- La qualité de l'intégration avec le client de messagerie est souvent déterminante, il est important que les nouveaux services soient présentés de façon ergonomique et cohérente pour que les utilisateurs puissent se les approprier facilement.
- Le choix de la solution se fera aussi en fonction du type de message que l'on souhaite unifier : e-mail, voix, fax, sms, toutes les solutions ne couvrent pas l'ensemble des médias.
- Les moyens de consultation des messages sont aussi à prendre en compte notamment si l'on dispose d'utilisateurs nomades : client de messagerie, web, synthèse et reconnaissance vocale.
- Dans le cadre de projet incluant une intégration de la communication dans des processus métiers, il est important de prendre en compte les possibilités offertes par la solution notamment en terme de connecteurs avec les applications métiers.
- La facilité d'administration de la solution est aussi un critère important pour optimiser les coûts d'exploitation.



Architecture d'une solution de messagerie unifiée

Mise en œuvre

Le succès de la mise en œuvre d'une telle solution repose sur la qualité de l'intégration entre deux mondes qui ne communiquent pas nativement entre eux : les télécoms et l'informatique. Pour cela il est recommandé de faire appel à une société qui a la double maîtrise des infrastructures et applications de communication.

Un autre point clef, en terme de succès d'un tel projet, est l'attention apportée à l'accompagnement des utilisateurs. Cette démarche est à prendre en compte dés les phases amonts du projet pour communiquer efficacement sur les bénéfices qu'apporte la solution de messagerie unifiée dans le travail quotidien des collaborateurs.

Panorama des offres

Les solutions de messagerie unifiée sont proposées par différentes catégories de constructeurs et d'éditeurs :

- Les acteurs du monde de la communication d'entreprise (Alcatel, Cisco, Nortel, Siemens, Avaya…) proposent des solutions de messagerie unifiée propriétaires intégrées à leurs offres, ils proposent aussi des offres de messagerie instantanée associées au service de présence.
- Des éditeurs spécialisés dans le domaine de la messagerie unifiée souvent issus de l'environnement du serveur de fax proposent des solutions indépendantes de la plate-forme de communication (Cycos, Tetco, …).
- Par ailleurs les éditeurs issus du monde du poste de travail développent aussi ces nouveaux services, c'est le cas de Microsoft avec son offre de messagerie unifiée pour Exchange 2007 ou IBM avec son offre de messagerie unifiée et collaborative Lotus Notes très présente dans le monde de l'entreprise.

Messagerie instantanée

Définition et Usages

Définition

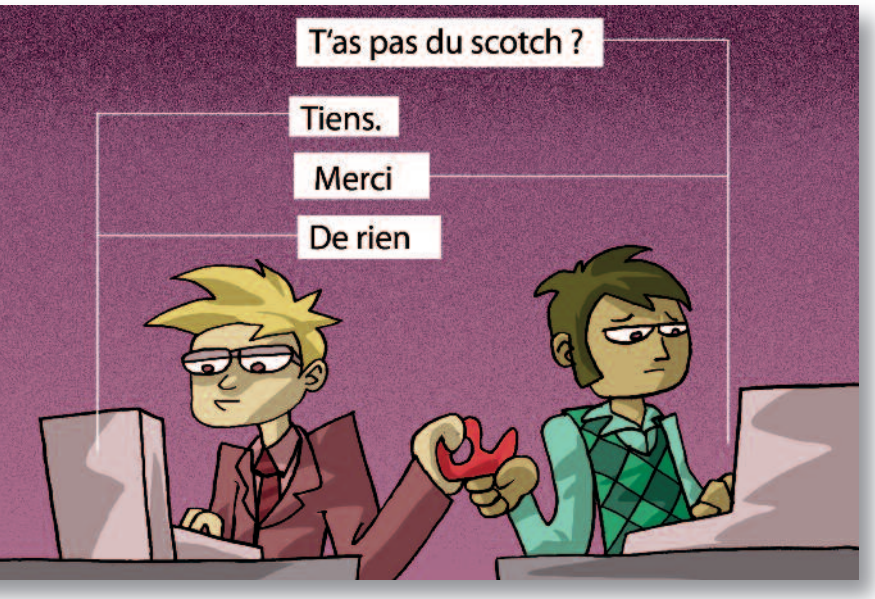
La messagerie instantanée permet de dialoguer instantanément par ordinateur avec un interlocuteur distant connecté au même réseau informatique, notamment Internet.
Cet outil permet de visualiser la disponibilité de l'interlocuteur (en ligne, occupé, …).

Différences par rapport au e-mail

À la différence de l'e-mail qui par définition est un outil de communication asynchrone, la messagerie instantanée est du domaine du synchrone, c'est à dire du temps réel. A ce titre elle est complémentaire de l'e-mail et va générer de nouveaux usages au sein de l'entreprise (détaillés ci dessous).

Adoption de cet outil

Le développement de la messagerie instantanée en entreprise est fortement tiré par l'adoption aujourd'hui massive des solutions grand public qui existent déjà depuis quelques années.
Le développement et la mise en œuvre des solutions entreprise sont associés à une volonté des entreprises de maîtriser les flux de communication échangés au travers de cet outil, un grand nombre d'employés l'utilisent quotidiennement au sein de leurs entreprises, des solutions grand public qui échappent à la politique de sécurité des sociétés.
Un autre moteur pour la mise en œuvre de solutions entreprises est leur capacité d'intégration avec les autres applications du poste de travail (agenda, applications de communication voix, vidéo, …).



Usages en entreprise

- Réaliser d'autres tâches en même temps, Ex : poser une question à quelqu'un qui est déjà en conversation sur un autre média, le téléphone par exemple, et inversement, alors que je suis en communication et que j'ai besoin d'une précision, poser une question à une personne sans interrompre ma conversation.

- Relancer quelqu'un qui n'a pas répondu par téléphone ou par e-mail.

- **Réduire les coûts des appels longue distance pour des communications simples.**

- Eviter des communications directes difficiles Ex : lever les barrières linguistiques en permettant, à des personnes ne maîtrisant pas parfaitement une langue étrangère, de prendre du recul par rapport aux questions qui leur sont posées et aux réponses qu'elles formulent en retour.

Le choix d'une solution de messagerie instantanée

Solution entreprise

- Application appropriée à une utilisation professionnelle (pas de publicité, ergonomie).

- Application de la politique de sécurité de l'entreprise (antivirus, filtrage).

- Intégration avec les infrastructures et applications de l'entreprise (messagerie, annuaire, « conferencing » (téléconférence, webconferencing, ...)...).

- Permet si nécessaire de s'interconnecter de façon sécurisée avec des solutions grand public (suivant la solution)

Solution grand public

- Manque de maîtrise de la société (flux, sécurité,…).

- Dissocié des autres outils collaboratifs de l'entreprise.

- Gratuit (mais financé par la publicité…).

- Difficulté pour dissocier l'utilisation professionnelle de l'utilisation personnelle.

Fiche 3

Usages en mobilité

Sommaire

Introduction

Avec des entreprises de plus en plus décentralisées, l'accès sans fil aux communications et aux informations est devenu une nécessité pour les collaborateurs mobiles de l'entreprise, qu'il s'agisse d'une mobilité extra ou intramuros. Les collaborateurs ont besoin de prendre des décisions rapides basées sur des informations actualisées en tout lieu et à tout moment pour des performances accrues et une augmentation de la productivité globale.

Les solutions de communication sans fil fournissent aux professionnels et aux entreprises mobiles une extension de l'ensemble de leurs besoins de communication, leur permettant de gérer rapidement et facilement leurs communications professionnelles et personnelles lors de leurs déplacements.

L'e-mail nomade est donc en constante progression, tant parmi les chefs d'entreprise et les collaborateurs lorsqu'ils occupent une fonction commerciale ou opérationnelle. D'ailleurs, ce sont souvent ces deux fonctions qui, ne disposant pas toujours d'une assistance, en sont les premiers demandeurs.

Le courrier électronique est ainsi la première application informatique en mobilité, faisant le pont entre les services de téléphonie cellulaire désormais classiques, les accès à l'Internet et le système d'information de l'entreprise en situation de mobilité. Elle est devenue indispensable à tout télétravail.

Solutions pour l'e-mail en mobilité : peut-on utiliser l'e-mail en tout lieu ?

L'e-mail au travers d'une interface WEB : le WEB mail

Depuis plus d'une décennie, le courrier électronique Internet est accessible (via un client dit « léger »[1]) au travers d'un navigateur Web au travers d'un simple couple « identifiant / mot de passe ». Cf. Le marché de l'e-mail (fiche 9).

Ce type de service adapté au nomadisme (au domicile, sur un ordinateur mis à disposition à l'exemple de web-café ou du poste emprunté par un collaborateur ou chez un partenaire…) est proposé par divers opérateurs « virtuels » d'un service mondial

(1) Par opposition à un client « lourd » : logiciel installé sur un poste pour une longue durée

(ex. Gmail, Hotmail…) mais aussi par les opérateurs d'accès Internet ou encore par un accès serveur interne d'entreprise.

Sécurité du WEB mail
La sécurité du web mail est un point sensible. Les opérateurs de service Web mail sérieux imposent automatiquement un chiffrement de la connexion (vérifier l'icône du cadenas sur le navigateur, et l'adresse web du type « https »).
Mais la menace la plus sérieuse reste le vol de mot de passe lorsque le terminal n'est qu'emprunté (cas typique mais non exclusif du « web bar »).

Même sans être assuré à 100% d'une administration anti-virus ou anti-spyware, il ne faut pas laisser le navigateur enregistrer son mot de passe. De plus, il faut surtout se déconnecter avant de quitter le navigateur.

L'e-mail sur assistant numérique de poche communicant (PDA), smartphone et BlackBerry
Le marché propose ainsi un large éventail de terminaux et de solutions de marques diverses, des assistants personnels de poche dotés d'une fonction communicante et de gestion d'e-mails aux téléphones cellulaires évolués supportant la messagerie unifiée.

L'acheminement des e-mails en nomadisme exige le recours à un **service de communication sans fil** et donc **au réseau d'un opérateur télécom mobile** (cellulaire de type 2G ou 3G) ou à celui d'un opérateur de service de données mobile. Ce dernier se charge de la fonction de télécommunication mais aussi de la gestion du serveur d'e-mails externe.

Comme pour la téléphonie mobile, ces opérateurs proposent divers « forfaits données » (data) incluant ou non la mise à disposition de terminaux, leur maintenance et leur assurance comme des services complémentaires.

Le PC mobile
Sans avoir recours aux PDA communicants, il est possible de rendre un ordinateur portable communicant :

- au travers d'un modem cellulaire (achat complémentaire d'une carte au format dit « PCMCIA » à insérer dans un emplacement du portable prévu à cet effet, ou modem externe connecté via un port USB) ;
- ou du modem incorporé dans certains téléphones portables connectés alors sur un port USB et en souscrivant un accès « données » auprès de l'opérateur. Le serveur doit dans ce cas être accessible via Internet (accès externe sécurisé ou WEB mail).

Les accès aux réseaux locaux (Wifi et bientôt Wimax) peuvent suffire dans des cas tels que réseaux urbains, campus, salles de réunions, conférences ou encore au sein d'un hôtel, si le serveur d'e-mails propose un accès Internet.

E-mail et nomadisme en pratique : comment choisir une solution selon ses besoins

Une analyse incontournable des besoins

Le vaste panorama de solutions existantes ainsi que la baisse régulière des prix rendent complexe un choix qui devra être guidé par les besoins réels individualisés, le système d'information existant de l'entreprise comme les coûts d'investissement ou opérationnels. Les professionnels mobiles peuvent gérer, à partir d'un seul appareil intégré, toutes leurs informations et leurs communications.

Les services sans fil comprennent l'e-mail mobile, la téléphonie, le SMS, le MMS, l'Internet mobile, les fonctions d'agenda et de répertoire, la messagerie instantanée ainsi que la possibilité d'accéder aux données de leurs applications-métiers et de leurs systèmes (tableaux, informations clients, données de tarification, informations de commande et mises à jour des stocks par exemple) ou non (messagerie instantanée, traitement de texte, tableau, ...). L'identification des besoins des utilisateurs, des scenarii de mobilité et des bénéfices associés permettra de faire un premier pas dans l'identification de la solution recherchée.

En plus des fonctions de téléphonie et de l'intégration d'un service d'e-mail mobile, il s'agit d'étudier les besoins de l'entreprise en matière d'applications mobiles complémentaires, de type CRM (Gestion de la Relation Client).

Pour en simplifier l'administration, la solution retenue doit s'intégrer simplement à l'architecture de l'entreprise existante et permettre une gestion centralisée. Etant donné que les utilisateurs envoient et reçoivent des courriers électroniques ou

accèdent à des données en mode sans fil, la solution doit également protéger de manière transparente les informations. Elle doit ainsi préserver l'intégrité, la confidentialité et l'authenticité des données de l'entreprise transitant entre le terminal et le système d'information de l'entreprise. Attention : si les terminaux sont multivalents (par exemple à la fois cellulaire GSM et Wifi), le coût d'usage d'un accès réseau rendu permanent peut ainsi varier de zéro à plusieurs centaines d'euros / jour (à l'international) sans que l'utilisateur n'en ait conscience !

Ainsi, la solution retenue par l'entreprise doit non seulement répondre aux principaux besoins des professionnels itinérants mais également à ceux des services informatiques. Elle doit permettre aux utilisateurs d'accéder sans effort à l'information lors de leurs déplacements tout en répondant aux besoins d'intégration, d'administration, de sécurité et de coût des entreprises.

Se connecter à ses e-mails en déplacement : comment et à quel coût ?

Par le biais d'un ordinateur fixe connecté à Internet

Au cours d'un déplacement, il vous suffit de vous connecter à Internet par le biais d'un ordinateur disposant d'un accès en lançant le navigateur Web. L'utilisation d'un logiciel de **webmail** (interface Web) rendra alors possible la gestion des courriers électroniques directement depuis ce navigateur Web au travers des protocoles d'accès à distance de votre messagerie électronique.
Si l'ordinateur ne vous appartient pas (celui d'un cybercafé par exemple), il faudra veiller à appliquer des mesures de sécurité minimum, en s'assurant notamment que le mot de passe ne soit pas enregistré automatiquement par le navigateur !

Coût : celui de la connexion Internet déjà présente (au forfait ou à la durée).

Par le biais d'un ordinateur portable ou assimilé

Vous pouvez également utiliser un ordinateur portable équipé d'un module de communication : ordinateur équipé d'une carte enfichable au format PCMCIA dite « Mobile PC Card », ou modem GPRS/UMTS externe connecté en interface USB, ou encore clé USB dite « clé 3G » ou « clé 3G+ » enfichée dans l'ordinateur. Le service de l'opérateur inclut également un logiciel de pilotage de ce matériel.

Le coût dépend du type de forfait choisi :

- soit à la durée (exprimée en heures) : de 5 à 40 heures/mois suivant la formule, compter de quelques dizaines à une centaine d'euros HT par mois ;

- soit au volume de données transférées (en mégaoctets) : de 5 Mo à 1Go par mois suivant la formule, compter de quelques dizaines à une centaine d'euros HT/mois ;

- soit formule illimitée, compter au moins 60€ et jusqu'à plus d'une centaine d'euros HT/mois.

À ces coûts doivent être ajoutés le prix du matériel et un abonnement dit « data » de l'ordre de 10€ HT/mois.

Les « PDA communicants », assistants personnels numériques intégrant des capacités hertziennes de transfert de données, sont également à classer dans cette catégorie.

Par le biais d'un terminal mobile alliant capacités vocales et transfert de données

Plusieurs solutions existent. Votre choix dépendra de vos besoins, du budget que vous souhaitez allouer et du système d'information (dont la solution email) existant dans votre entreprise. N'hésitez pas à consulter les sites web des opérateurs et constructeurs pour comparer les offres et les architectures.

En fonction des solutions, l'entreprise peut choisir entre différentes catégories de terminaux, dont le prix unitaire varie de quelques dizaines à plusieurs centaines d'euros :

- Téléphone mobile permettant de souscrire à une option data (abonnement dit « data » de l'ordre de 10 € HT/mois).

- Téléphones intelligents appelés « Smartphone », en même temps téléphone et « PDA communicant ». La tarification est en général fonction du volume de données transmises, et dégressive en fonction de la taille de la flotte de l'entreprise (gamme de prix du service : voir paragraphe précédent, de quelques dizaines à plus d'une centaine d'euros HT/mois). Pour les voyageurs désirant accéder à leur messagerie à l'étranger, une option d'extension du forfait pour les communications data effectuées depuis l'étranger est nécessaire. Elle est fonction du volume de données transférées (de quelques dizaines à une centaine d'euros HT/mois) et peut varier suivant la zone géographique dans laquelle se trouve le Smartphone (Europe, Amérique du Nord, Afrique,…).

- Des « solutions de communication » encore plus évoluées, permettant la voix, l'e-mail mobile, la navigation internet, la vidéo, ainsi que la possibilité d'accéder au réseau interne de l'entreprise (par ex : smartphones BlackBerry® de RIM, SPV d'Orange, N95 de Nokia, iPhone d'Apple dans sa version « 2 » entreprise …). La gamme de prix du service est identique à la précédente.

Pour l'accès de ces terminaux à la messagerie, il faut disposer :

- soit d'une messagerie ouverte sur l'internet (cas d'une PME par exemple). Ces solutions peuvent intégrer les comptes de messageries professionnelles ou personnelles des utilisateurs en utilisant POP3/IMAP et/ou le transfert d'emails ;

- soit d'un serveur sur le réseau de l'entreprise dédié à la solution et permettant d'accéder à la messagerie (Microsoft Exchange, IBM Lotus Domino, Novell GroupWise). Dans ce cas, l'entreprise doit investir dans la passerelle d'interconnexion (coûts d'investissement et de fonctionnement, à ramener au nombre de terminaux de la flotte).

Enfin, il existe deux modes de fonctionnement différents, à choisir compatible avec sa propre messagerie :

- le mode « Pull e-mail », le terminal doit se connecter régulièrement sur le serveur de messagerie afin de recevoir les e-mails. Cette solution « mail à la demande », en temps différé, est compatible avec les 3 catégories des terminaux ;

- le mode « Push e-mail » : cette solution « pousse » directement les mails ou toute autre type de donnée vers le terminal (à condition qu'il soit compatible avec l'option push-mail), et permet ainsi la réception des mails en temps réel (par exemple solution BlackBerry® de RIM, précurseur du marché, mais aussi Nokia ou Microsoft sur SPV). Un serveur de messagerie dédié sur le réseau de l'entreprise peut être nécessaire à cette fonction.

Ces terminaux fonctionnent aussi bien avec des offres au volume de données transférées que des forfaits, dont certains « illimités » (compter quelques dizaines d'euros en plus du forfait mensuel).

Dans les critères de choix de la solution il s'agira alors de veiller à ce que la solution déployée garantisse la confidentialité et l'intégrité des données sans coût supplémentaire pour l'entreprise, qu'elle s'intègre de façon transparente à son système d'information et supporte ses stratégies informatiques tout en permettant une administration simple et centralisée.

Fiche 4

Les aspects juridiques liés à l'utilisation de l'e-mail

Sommaire

Quelle est la valeur juridique des e-mails ?

Quelle est la valeur d'un e-mail au plan juridique ? En d'autres termes, un e-mail peut-il être produit en justice pour prouver en faveur de l'entreprise ?

À l'exception de certains actes, notamment les contrats passés avec des non-commerçants pour une chose d'une valeur supérieure à 1500 € (décret n°2004-836 du 20 août 2004), pour lesquels la loi exige un écrit, la preuve des faits et de la plupart des actes peut être faite par tous moyens. Ce qui veut dire qu'un e-mail (y inclus ses éventuelles pièces jointes) sera normalement recevable en justice à titre de commencement de preuve. Si la partie adverse dénie la valeur juridique de l'e-mail produit en justice, elle peut y parvenir au motif qu'il émane de la partie qui s'en prévaut.

S'agissant des e-mails reçus de la partie adverse ou de tiers, il faudra convaincre le juge qui appréciera librement le caractère probant de l'e-mail invoqué. Cependant, la partie adverse pourra difficilement se borner à rejeter ou renier l'e-mail concerné.
En effet, tout e-mail comporte un certain nombre d'informations cachées sur son origine et son cheminement sur le réseau Internet, situées dans une partie normalement cachée du message qu'on appelle « l'entête ».

```
Return-Path: <jean@dupont.fr>
Received: from mwinf1108.durand.fr (mwinf1108.durand.fr)
        by mwinb0703 (SMTP server) with LMTP; Fri, 18 Feb 2008
11:06:11 +0100
Received: from me-durand.net (localhost [ 127.0.0.1] )
        By mwinf1108.durand.fr (SMTP server) with ESMTP id
563751C0009E;
        Fri, 18 Feb 2008 11:06:11 +0100 (CET)
Received: from [ 127.0.0.1] (pc0001.dupont.fr [ 192.168.6.24] )
        By mwinf1108.dupont.fr (SMTP server) with ESMTP id
715011C000C2;
        Fri, 18 Feb 2008 11:06:09 +0100 (CET)
X-Sieve: Server Sieve 2.2
X-ME-UUID: 20080218173405436.6A7332400088@mwinf1108.dupont.fr
Message-ID: <4215BEC8.2090503@dupont.fr>
Date: Fri, 18 Feb 2008 11:09:12 +0100
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-Us;
rv:1.7.5) Gecko/20041217
X-Accept-language: en-us, en
MIME-Version: 1.0
To: paul@durand.fr
Subject: Structure des messages
Content-type: multipart/mixed ;
```

Exemple d'un en-tête d'e-mail

Or, ces informations techniques complexes seront difficilement modifiables, de même que le contenu de l'e-mail, sans que cela puisse être détecté par un expert. Cet entête demeure modifiable mais une telle action serait alors constitutive d'un faux comme pour une lettre sur papier, dont l'usage sera puni par le code pénal (art. 441-1 du code pénal). A cet égard, si la partie à laquelle on oppose un e-mail envoyé par elle conteste, non l'e-mail lui-même, mais son contenu, elle pourra utilement communiquer à l'expert l'archive de l'e-mail tel qu'envoyé.

Il faudra donc considérer qu'un mail reçu revêt une relative valeur probante, en tout cas la valeur d'un commencement de preuve par écrit. Il convient en conséquence que :

- les collaborateurs de l'entreprise soient attentifs à ce qu'ils écrivent ;
- ils demandent un accusé de lecture par le destinataire pour les e-mails importants qu'ils envoient ;
- l'entreprise se dote d'une politique de conservation des e-mails qu'elle échange notamment avec ses clients et fournisseurs (cf. infra) ;
- les e-mails soient conservés sous forme électronique et dans leur format d'origine (.msg/.pst/.ost pour Outlook ou .nsf pour Lotus Notes) afin d'en conserver l'entête.

La signature électronique des e-mails (voir fiche 8)

Afin de sécuriser totalement la valeur probante des e-mails, on peut envisager d'avoir recours à leur signature électronique.

Cette signature sera directement intégrée dans le client de messagerie (notamment Microsoft Exchange/Outlook ou Lotus Dominos/Notes).

L'entreprise aura le choix d'opter pour :

- Une signature électronique sécurisée dans la mesure où le code civil lui confère une présomption de fiabilité, c'est-à-dire que le signataire n'aura pas à démontrer que sa signature est fiable. En revanche, ce sera à la partie qui contestera la fiabilité de la signature électronique de démontrer que cette signature n'est pas conforme aux principes de l'article 1316-4 du code civil (elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache). Suivant le décret n°2001-272 du 30 mars 2001, la signature électronique sécurisée est basée :
  - sur l'utilisation d'un dispositif sécurisé de création de signature ayant fait l'objet d'une certification par un organisme tiers dans le respect d'exigences prévues par le décret n°2002-535 du 18 avril 2002, ainsi que
  - un certificat qualifié et délivré par un prestataire de certification répondant à différentes exigences ou étant qualifié.

  Il est toutefois aujourd'hui utile de noter que la signature électronique sécurisée n'est pas encore disponible (voir en ce sens le site de la DCSSI qui tient à jour une liste des dispositifs sécurisés de création de signature et des certificats qualifiés : www.ssi.gouv.fr).

- Une signature électronique « simple ». Ce type de signature semble suffisant par rapport à l'usage qui va être fait, dans la grande majorité des cas, de la messagerie, la signature électronique sécurisée étant surtout requise dans certaines situations : actes authentiques (notaires, huissiers) notamment. Il convient de noter que la différence essentielle entre la signature électronique et la signature électronique sécurisée se situe au niveau de la charge de la preuve. Elle variera selon que l'on bénéficie ou pas de la présomption de fiabilité. Mais la présomption de fiabilité est une présomption simple, qui peut donc être combattue par celui qui conteste les qualités du procédé de signature utilisé. Dans un cas, il appartient à l'utilisateur du procédé de signature de prouver cette fiabilité (signature électronique « simple »), dans l'autre, c'est celui qui la conteste qui devra prouver son absence de respect des exigences (signature électronique sécurisée).

  L'expéditeur d'un e-mail signé électroniquement devra s'assurer que son correspondant est équipé d'un dispositif de signature électronique soit identique soit interopérable avec le sien. Or, c'est malheureusement cet « effet de réseau » qui freine encore le développement de la signature des e-mails. Cet état de fait pourrait toutefois évoluer favorablement dans les mois ou au plus tard quelques années qui viennent.

L'archivage des e-mails (voir fiche 6)

L'entreprise aura intérêt à adopter une politique de conservation de ses e-mails.
Cette politique visera au respect d'exigences d'historisation / de traçabilité / de chemin de révision requises par la mise en œuvre de différentes réglementations financières (par ex. Sarbanes Oxley) ou industrielles (santé, agroalimentaire, aviation civile, etc.)

Elle visera à permettre à l'entreprise de se ménager la preuve de ses échanges avec les tiers notamment ses clients et fournisseurs.

Cet archivage devra intervenir dans des conditions assurant à l'entreprise que l'e-mail archivé ne verra pas sa valeur juridique initiale dégradée ou anéantie par sa période d'archivage. L'entreprise aura alors intérêt à recourir à un archivage électronique sécurisé.

Ce dernier visera à garantir l'intégrité des e-mails archivés, c'est-à-dire que ces derniers n'ont pas pu être modifiés durant leur archivage. Cette garantie d'intégrité sera assurée par le recours à une signature électronique [Pas une signature électronique sécurisée].

L'entreprise aura également grandement intérêt pour la sécurité juridique de son archivage à observer les principes posés par les guides et normes techniques applicables en la matière (Guide de l'archivage électronique sécurisé, Association Ialta France, 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, Norme française NF Z42-013 : recommandations 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, 2001, Norme internationale ISO 19005-1 sur le format PDF/A ("A" comme "archive"), approuvée de façon unanime en juin 2005, ISO 15489 et la méthodologie DIRKS (Design and Implementation of Recordkeeping Systems) d'implémentation en 8 étapes d'un système global d'archivage ; le 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 ; Modèle OAIS (système ouvert d'archivage d'informations), devenu la norme internationale ISO 14721 : description de l'organisation et du fonctionnement d'un centre d'archivage pour la pérennisation des données numériques).
Quand à la durée de conservation des e-mails, celle-ci procédera :

- de l'examen d'éventuelles réglementations applicables à l'entreprise eu égard à son activité et qui commande directement ou indirectement la conservation des messages ;
- de l'appréciation qu'aura l'entreprise de ce que nécessite la préservation de ses intérêts en cas de contentieux judiciaire.

L'entreprise devra à ces deux égards s'interroger sur les délais durant lesquels elle pourra avoir besoin d'apporter certaines preuves devant une administration ou un juridiction. Cette durée procédera des délais de prescription prévus par la loi pour chaque type d'obligation.

Il sera par exemple de 10 ans pour les contrats commerciaux[2].

Ce délai résultera également d'une mise en balance du coût de l'archivage sur une durée considérée avec les risques encourus par l'entreprise si elle ne disposait plus des messages.

L'entreprise devra également prévoir que l'archivage des e-mails de ses salariés constitue un traitement de données à caractère personnel et à ce titre, la loi Informatique et libertés[3] trouvera à s'appliquer (notamment les déclarations préalables). Une délibération de la CNIL n°2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique dans le secteur privé de données à caractère personnel (www.cnil.fr) fournit certaines réponses dans le cadre de l'archivage des e-mails.

Le contrôle de l'usage des e-mails

Il faut bien garder à l'esprit qu'un e-mail constitue au plan juridique une correspondance, au même titre qu'un courrier papier, et qui peut dans certains cas être privée. Il est en effet émis par une personne déterminée vers une ou plusieurs personnes bien déterminées. Les adresses génériques info@... ou

[2] Article L110-4 du code de commerce : « Les obligations nées à l'occasion de leur commerce entre commerçants ou entre commerçants et non-commerçants se prescrivent par dix ans si elles ne sont pas soumises à des prescriptions spéciales plus courtes (…) ».

[3] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés loi Informatique et libertés.

sav@... seront considérées comme adressées à la personne morale sauf s'il s'agit d'un pseudonyme d'une personne physique connue des personnes concernées.

Cette correspondance pourra avoir un objet professionnel ou personnel. En pratique, et sauf exception, les e-mails au sein de l'entreprise et/ou échangés entre l'entreprise et l'extérieur seront des « correspondances privées » dont la violation du secret est punie par le code pénal[4]. Elles seront selon les cas des « correspondances privées professionnelles » ou des « correspondances privées personnelles », au titre de la vie privée résiduelle.
Toutefois, il est évident que si les e-mails sont issus d'une adresse de messagerie professionnelle et qu'une instruction d'utilisation des moyens informatiques mis à disposition des salariés prévoit les conditions de surveillance de ce type de mail, le secret des correspondances privées ne devrait, sous réserve d'une jurisprudence contraire, trouver à s'appliquer.
Si ces e-mails constituent clairement des correspondances privées, le collaborateur n'a pas moins une obligation de loyauté vis-à-vis de son entreprise compte tenu du lien juridique crée par son contrat de travail avec l'entreprise. En exécution de cette obligation de loyauté, le collaborateur devra mettre à disposition de son entreprise les e-mails qu'il aura reçus dans le cadre de son activité professionnelle afin de permettre à l'entreprise de garder une mémoire notamment de ses relations avec les tiers.

L'entreprise devra par conséquent organiser cette mise à disposition par le collaborateur de ses e-mails dans le respect du secret des correspondances. Cette mise à disposition pourra par exemple s'opérer dans le cadre du classement des e-mails et de leur archivage. Ce sera également organiser les délégations d'accès précitée notamment afin d'éviter que des messages urgents demeurent ignorés de l'entreprise faute d'être consultés.

L'entreprise aura intérêt à organiser l'identification et l'isolement des messages personnels afin d'éviter toute ambiguïté.

L'entreprise devra également gérer la question des e-mails des collaborateurs la quittant. Il pourra être prudent d'acter avec le salarié partant, si nécessaire par une notification officielle, de ce qu'il lui appartient de réclamer avant son départ ses éventuels messages personnels et qu'il remet à l'entreprise ses autres messages professionnels.

Enfin, les salariés devront être informés que leurs messages professionnels seront archivés (cf. supra) pendant telle durée ainsi que des conditions dans lesquelles l'entreprise pourra y accéder.
Afin d'être opposables aux salariés, ces règles devront être consignées dans un document annexé au règlement intérieur de l'entreprise dans les conditions prévues par le code du travail (communiqué pour avis au comité d'entreprise et adressé à l'inspecteur du travail et enfin déposé au greffe du conseil des Prud'hommes).

Quelles mentions légales doit comporter un e-mail ?

De très nombreuses entreprises ou organisations ajoutent automatiquement à la fin de leurs e-mails différentes mentions à vocation légale notamment en termes de responsabilité. D'inspiration anglo-saxonne, elles sont parfois dénommées « disclaimer ».

Si ces mentions peuvent être juridiquement souhaitables au regard du droit de pays étrangers dans lesquels serait situé un correspondant de l'entreprise, elles n'ont pas de valeur en droit français qui ne reconnaît les exclusions ou limitations de responsabilité civile du fait de ses commettants (collaborateurs) que dans certains cas relativement rares. Ces mentions auront tout au plus une valeur informative ou pédagogique lorsqu'elles invitent celui qui a reçu un message par erreur à le signaler à l'expéditeur et à l'effacer.

Il doit être en revanche signalé que les articles R123-237 et R123-238 du code de commerce prévoient que toute personne immatriculée au registre du commerce et des sociétés indique sur ses documents commerciaux dont notamment ses factures et ses correspondances différentes informations dont notamment sa forme sociale si elle est une société commerciale, son numéro d'immatriculation au RCS et le lieu de celui-ci, le lieu de son siège social, etc.

Dans la mesure où l'entreprise utilise l'e-mail dans ses échanges avec les tiers dans le cadre de son activité, bien souvent en remplacement des courriers papiers traditionnels à son entête, il sera prudent qu'elle fasse figurer les informations prévues aux articles R123-237 et R123-238 précités en pied de page de ses e-mails.

(4) Art. 226-15 du code pénal.

Aspects juridiques de l'e-mailing

L'entreprise qui souhaite utiliser la voie de l'e-mail pour ses actions marketing doit avoir à l'esprit les limitations suivantes prévues par l'article 34-5 du code des postes et communications électroniques. Ce texte pose en principe l'interdiction de toute prospection directe au moyen d'un courrier électronique adressé à une personne physique « qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen ».

Le texte précise que la prospection directe par courrier électronique est autorisée à la double condition que :

- les coordonnées du destinataire aient été recueillies à l'occasion d'une vente ou d'une prestation de services, le destinataire sera donc un client,
- la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale.

Attention, l'entreprise devra dans tous les cas :

- offrir à son client la possibilité de s'opposer à l'utilisation de ses coordonnées, lors du recueil des données à caractère personnel le concernant et à chaque envoi d'un courrier électronique de prospection,
- indiquer des coordonnées auxquelles le destinataire pourra demander à être désinscrit.

Concrètement, ces informations prendront la forme d'une notice par exemple en fin du formulaire de collecte et de l'e-mail.

L'entreprise qui méconnaîtrait ces règles s'exposerait aux poursuites pénales applicables en matière d'atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24 du code pénal).

Fiche 5

L'intérêt de l'e-mail pour le marketing

Sommaire

Introduction

L'e-mail est désormais un outil incontournable de toute bonne stratégie de marketing, de vente et de communication. A condition toutefois de savoir en exploiter les nombreuses possibilités et d'en connaître les dangers.

L'e-mail marketing peut alors constituer une nouvelle source de profits très efficace et peu coûteuse. Il permettra même d'**identifier les meilleurs clients** et leurs modes de consommation, puis de **les inciter à l'achat (impulsif) en fonction de leur historique d'achat et de leurs préférences.**

Comment utiliser l'e-mail dans une stratégie marketing ?

L'e-mailing touche tous les domaines de la communication : événementiel, prospection, annonce, support, relance, etc.

D'un point de vue **marketing**, il servira essentiellement à :

- Communiquer sur de nouveaux produits
- Annoncer des événements
- Envoyer un bulletin d'information
- Faire connaître les différentes gammes de produits et services
- Etablir une relation client individualisée (CRM).

Au niveau des **ventes**, il permettra de :

- Faire connaître les promotions du moment
- Annoncer les déstockages
- Gérer la relation avec les distributeurs, clients et prospects
- Réaliser des propositions commerciales personnalisées et adaptées à chaque client, en fonction de son historique d'achat.

L'e-mail est complémentaire des formes de communication traditionnelles. Rapide et convivial, ce nouveau support publicitaire permet de véhiculer un message auprès de nombreux destinataires par courrier électronique. Il permet également de savoir si ces derniers ont ou non pris connaissance du message et s'ils ont visité les liens qui y étaient insérés.

Très économique, sans papier ni affranchissement, l'e-mailing se décline aujourd'hui à travers une grande variété d'offres et de solutions locales ou hébergées.

De quoi a-t-on besoin ?

Pour lancer une campagne e-mailing trois éléments sont nécessaires :

- une liste d'e-mails
- un logiciel pour le côté technique de la diffusion
- un message à envoyer.

Une fois ces trois éléments réunis, l'envoi en lui-même ne prendra que quelques minutes. Avec les nouvelles technologies, il sera même possible de suivre l'actualité de ses campagnes en temps réel (ouvertures, clics, etc.) et de conserver un historique des achats qui permettra ensuite d'individualiser les futures campagnes.

Le degré de succès dépendra surtout de la qualité des trois éléments de base. Cette fiche a pour objectif de fournir quelques recommandations en la matière et avant tout de faire prendre conscience de toutes les possibilités offertes par l'e-mail marketing.

Comment utiliser l'e-mail en marketing et vente ?

Quelques idées pour bien exploiter le canal de l'e-mailing dans le domaine du marketing ou de la vente, depuis le service le plus basique jusqu'aux scénarios plus complexes.

Quelques idées pour le marketing

Informer ses clients

On peut utiliser l'e-mailing pour communiquer sur ses offres de produits et de services. Cela permet d'informer aisément et à moindre coût l'ensemble de sa base de données consommateurs.

L'expression la plus simple de cette utilisation de l'e-mailing est la campagne d'information ou newsletter régulière (bihebdomadaire, mensuelle…).

Elle pourra par exemple :

- renseigner les clients sur l'actualité de l'entreprise
- renvoyer aux derniers articles parus sur le site Internet
- présenter les nouveaux produits

L'e-mailing pourra même devenir un support de contact et de suivi pour le service clientèle. Il servira alors à informer les clients sur les mises à jour de leurs contrats ou plus prosaïquement à leur envoyer des confirmations et alertes d'expédition de commande.

Soutenir un lancement de produit : de l'intérêt du multi-canal

Bien utilisé, l'Internet devient un outil de plus en plus efficace pour faire connaître un nouveau produit. Il vient en complément des autres canaux traditionnels, à un coût moindre.

Parallèlement à des campagnes presse, radio ou télévision, il est par exemple possible de concevoir un mini site Internet consacré au nouveau produit. On dévoilera l'identité de ce produit par le biais d'un e-mailing adressé aux clients et prospects avec un lien vers ce mini site.

Le marketing viral permet d'aller encore plus loin.

Organiser du marketing viral

Le marketing viral s'appuie sur la vieille méthode du bouche à oreille. Transposé sur Internet cela consiste tout simplement à augmenter la popularité d'un site ou d'un produit en amenant les internautes à en faire la publicité à votre place.

Cela implique la mise à disposition d'un mécanisme de parrainage permettant à une personne qui vient de découvrir votre produit d'envoyer un e-mail automatique et personnalisé à ses amis internautes.

Ce mécanisme devra être utilisable aussi bien sur le mini-site Internet du produit que dans les messages envoyés. Pour renforcer la propagation (ou buzz), on peut par exemple assortir le lancement du produit avec des jeux concours.

S'assurer une présence durable auprès de ses clients

Accompagner le lancement d'un nouveau produit ne suffit pas à garder une présence durable auprès de ses clients. Le plan marketing inclura donc régulièrement une série d'événements qui permettront de continuer à promouvoir la marque (brand marketing).

L'utilisation de l'e-mailing permettra là aussi de promouvoir ces événements. Inauguration d'un nouveau magasin, visite d'une personnalité pour des dédicaces ou le lancement d'une exposition…pour toutes ces occasions, un e-mail envoyé aux clients qui habitent sur la zone géographique concernée **(géomarketing)** se révèlera souvent payant.

Quelques idées pour la vente

Créer du trafic sur le site web

Lorsqu'on dispose d'un site Internet, l'un des princi-

paux objectifs sera d'en augmenter la fréquentation, surtout s'il s'agit d'un site marchand.

L'e-mailing, peut rapidement faire connaître le site, à travers notamment des liens sur les produits du catalogue, incitant les internautes à se rendre sur le site. Une utilisation régulière de l'e-mailing permettra ainsi d'entretenir, voire d'accroître, un bon niveau de fréquentation du site marchand, donc du niveau des ventes.

Autre bonne méthode pour créer du trafic : la vente flash. Limitée en durée, elle consiste à vendre un ou plusieurs produits assortis d'un rabais exceptionnel et peut assurer une hausse notable du trafic sur le site.

Générer du trafic sur le point de vente

Parallèlement, l'utilisation de l'e-mailing est devenue un outil incontournable du géomarketing. Envoyer un message aux clients habitant dans la zone géographique proche d'un de ses magasins est très efficace. Ce le sera plus encore si l'e-mail est assorti d'offres proposées au niveau local par ce magasin en particulier.

Il devient alors très simple d'émettre des messages promotionnels locaux : ouverture d'un nouveau magasin, soldes anniversaires ou annuelles, ventes flash, animations ciblées sur certains produits…

Gérer et animer un programme de fidélisation

Une fois la vente effectuée, pourquoi ne pas garder contact avec le nouveau client dans le cadre d'un programme de fidélisation ? Ce client, dont on a déjà gagné la confiance, sera bien plus enclin à acheter à nouveau, pour un investissement en marketing moindre que celui nécessaire à l'acquisition de nouveaux clients.

L'e-mailing peut servir d'outil de communication de base pour tout programme de fidélisation. L'envoi de messages réguliers permettra en effet de :

- Garder le contact avec le client,
- Lui faire connaître les derniers produits,
- Lui proposer des offres spécifiques,
- Gérer le suivi administratif,

De plus, une relation continue et suivie avec ses clients permet de bien mieux les connaître tant en ce qui concerne leurs préférences produits que leurs comportements d'achat. A condition bien sûr de conserver une trace de toutes les interactions avec eux. A partir de là il sera possible de pousser des **stratégies incitant à l'achat compulsif !**

Les possibilités offertes par l'e-mailing sont, on le voit, nombreuses et riches. Comment les mettre en œuvre ?

Bien constituer sa base de données

La première chose à faire est de constituer une base de données d'e-mails, soit par l'intermédiaire des clients, soit via le site web, soit en utilisant une base de données de location. Il faut ensuite veiller à la qualité de cette base.

Informations à recueillir

Les champs suivants sont communément considérés comme indispensables :

- L'adresse e-mail
- Les Noms et/ou Prénoms, qui permettront de rendre le message plus direct et personnel.
- Le Nom de l'entreprise,
- Le Sexe, critère de ciblage fondamental
- La Ville et/ou le Code Postal, qui ouvriront les portes du géomarketing
- Le N° de téléphone portable qui permettra de doubler les campagnes d'e-mailing de campagnes SMS ou MMS

De manière générale, il faut choisir les champs qui serviront le plan marketing et préférer ceux qui rendront le message plus direct et mieux adapté à la cible.

Qualité de la base de donnée

Une base « propre », c'est-à-dire de bonne qualité, sera très peu encline au filtrage « anti-spam ». On appelle spams tous les messages nos sollicités (voir ci-dessous et fiche N° 7).

Les messages envoyés sont acheminés vers les boîtes mails des destinataires. Généralement, un certain nombre d'adresses de la base de données ne sont plus valides pour des raisons diverses : abandon de l'adresse, fermeture du compte, boite pleine... Cela correspond à l'usure de la base, ce qui est normal.

Pour chacun des e-mails non parvenus à leur destinataire, un message d'erreur sera renvoyé sous la forme d'un e-mail au contenu technique. On appelle cela des « bounces » (e-mails rebond), ou des « mail undelivery », (e-mails non remis).

Si le pourcentage d'e-mails non remis est trop élevé,

les filtres anti-spam risquent de classer l'ensemble des e-mails de l'expéditeur en spam. Pire encore, la plupart des fournisseurs d'accès risquent même de bloquer l'envoi (cela s'observe principalement chez les opérateurs majeurs, Hotmail, Yahoo! Mail et AOL).

La durée de vie moyenne d'une adresse e-mail est de deux ans. Il est donc important de se méfier des bases trop anciennes. Il faut s'assurer de la mise à jour régulière des adresses de la base et de leur validité, et procéder au retrait de toutes celles tombées en obsolescence. La plupart des bons logiciels d'e-mailing permettent d'écarter ou de supprimer les e-mails invalides, ne pas hésiter à utiliser ces fonctionnalités.

Législation à respecter

En France, comme aux Etats-Unis et dans la plupart des pays Européens, la législation interdit l'envoi de spam.

Selon la loi, est considéré comme spam, tout e-mail à but lucratif, envoyé à une personne physique n'ayant pas exprimé son consentement préalable de le recevoir.

Si cette autorisation préalable est nécessaire pour l'envoi de messages dans un contexte BtoC, elle n'est toutefois pas obligatoire pour les messages BtoB.

Les fichiers prospects constitués sans consentement préalable ne peuvent être utilisés.

La CNIL (Commission Nationale de l'Informatique et des Libertés, http://www.cnil.fr) a souligné le 14 Octobre 1999 qu'une adresse électronique est une information nominative. Utilisée via un traitement automatisé, cette information devra donc être déclarée auprès de la CNIL.

D'autres réglementations concernent les messages envoyés, et les méthodes de consentement. Elles sont développées ci-dessous.

Une analyse complète des réglementations est disponible dans le document "Loi pour la confiance dans l'économie numérique" édité par le Forum des droits sur Internet (http://www.foruminternet.org/) On le trouvera à l'adresse suivante : http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0200175L

Concept de permission

Pour éviter tout ennui futur, tant avec les destinataires des e-mails qu'avec la législation, il suffit de prendre la règle de base suivante : toujours éviter d'ajouter dans la base de données un contact dont on sait pertinemment qu'il ne sera pas intéressé par l'e-mail qui va lui être adressé. Il faut préférer la qualité à la quantité et ne pas oublier que chaque individu mécontent recevant un e-mail non sollicité nuira à la notoriété et à la crédibilité de l'image de marque de l'émetteur.
Les lois anti-spam ont fait un premier pas dans la bonne direction mais cela reste insuffisant. La conception française du spam va plus loin que celle de la plupart des pays et permet d'exploiter un véritable e-mail marketing.

En France, est considéré comme spam tout e-mail envoyé à une personne qui n'a pas, directement et explicitement, donné la permission de la contacter sur le sujet abordé dans l'e-mail.

Avec le nombre croissant de « spammeurs » en circulation, le concept de permission est devenu, de loin, l'aspect le plus important de l'e-mail marketing. Il est capital d'être du bon côté de la loi. La permission peut s'obtenir de plusieurs façons :

- **Par l'intermédiaire du site web**
  L'internaute remplit un formulaire d'inscription à la newsletter ou coche une case correspondante sur un autre type de formulaire en ligne. Cette case ne doit jamais être cochée par défaut et il convient d'expliquer clairement que cocher cette case signifie accepter d'être contacté par e-mail.

- **Via des formulaires hors ligne**
  Une personne remplit un formulaire hors-ligne (sondage, concours…) et coche la case indiquant de façon explicite qu'elle accepte d'être contactée par mail.

- **Via une carte de visite**
  Une personne qui remet en direct sa carte de visite, pourra être contactée par e-mail, à condition de le lui avoir clairement indiqué au préalable. Si la carte de visite est déposée dans une urne pendant un salon, une pancarte doit signaler la possibilité de contacts par e-mail.

Après avoir obtenu la permission des abonnés, il est préférable de la confirmer par la méthode du double **opt-in** (double validation) avant de leur d'envoyer des e-mails.

Cette méthode, communément répandue, consiste à envoyer un e-mail avec **un lien de confirmation**, à toute personne qui s'abonne à une liste de diffusion. Ce n'est qu'après avoir cliqué sur ce lien que le nouvel abonné sera ajouté à la liste.

Autre avantage, le double opt-in permet de contrôler la qualité d'une adresse e-mail avant de l'ajouter à la base. Toute adresse erronée ou fausse ne recevra pas l'e-mail de confirmation et ne viendra ainsi pas nuire à la qualité de la base de données.

L'acquisition de nouveaux clients

Une vérité simple du marketing Internet : plus on donne à ses visiteurs, plus on reçoit en retour.

Ajouter un formulaire d'inscription à la newsletter dans un endroit visible de son site Internet est un moyen simple et efficace d'attirer de nouveaux abonnés. Le formulaire doit être lié au logiciel d'e-mailing qui s'occupera de collecter, puis de traiter les informations. On peut également ajouter des cases d'abonnement à cocher sur tous les autres formulaires existants, en respectant les règles énoncées plus haut.

Cette méthode d'inscription via formulaire est devenue un standard mais d'autres méthodes existent et la complètent efficacement.

Les internautes, du fait du nombre croissant d'e-mails publicitaires qu'ils reçoivent, se montrent de plus en plus réticents à donner leur adresse e-mail. D'où l'importance de les mettre suffisamment en confiance pour qu'ils acceptent de laisser leurs coordonnées.

Une bonne méthode : leur offrir un contenu à valeur ajoutée en échange de leur adresse e-mail. Cela peut prendre n'importe quelle forme : documentation, livres blancs, fichiers mp3, accès à un service, etc. Il suffit de commencer par créer une page web présentant et vantant les bienfaits du produit offert et d'indiquer que pour l'obtenir gratuitement il est nécessaire de laisser son adresse e-mail et éventuellement d'autres informations, comme les noms, prénoms, etc. Une fois ces informations collectées, l'accès au contenu promis est offert via une autre page web ou un répondeur automatique. Cette méthode, reconnue pour son efficacité, est désormais largement utilisée.

Bien rédiger et bien envoyer ses e-mails

Bien rédiger

Définir le bon sujet

Le sujet/objet de l'e-mail est la première chose que les destinataires liront. C'est donc un des éléments les plus importants et celui qui doit demander le plus de réflexion.

La qualité de l'accroche que constitue le sujet conditionnera largement l'ouverture de l'e-mail. Un sujet mal rédigé conduira souvent le destinataire à ignorer, archiver, supprimer ou classer en spam, l'e-mail concerné. Le sujet est également très important pour éviter les filtres anti-spam.

Quelques recommandations :

Intitulé du sujet.

Eviter de manière générale les sujets amenant à penser trop clairement « Ceci est une pub ».
Choisir un sujet court, simple et sans supposition.
Recourir à la curiosité des lecteurs et ajouter une accroche personnalisée du type
« Julie, votre nouveau parfum ! », ou « Julien, que pensez vous de ce baladeur ? »

Effet d'urgence

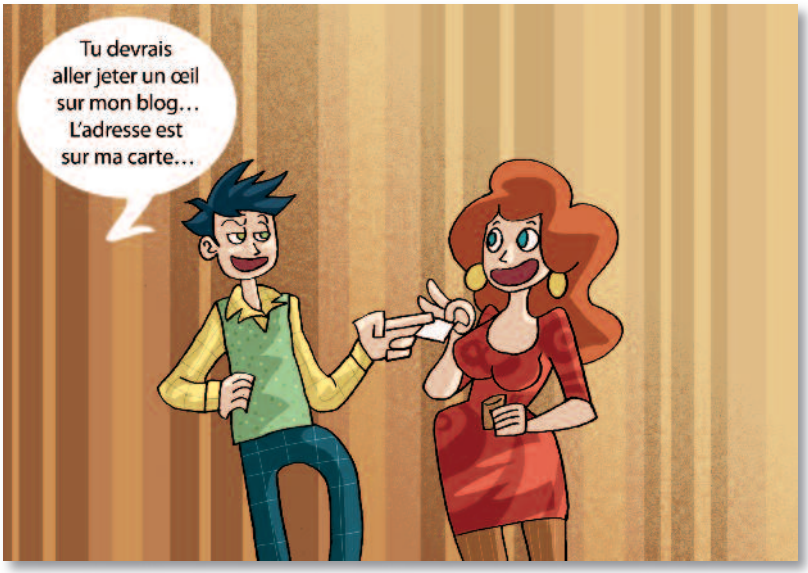
Ne pas hésiter à jouer l'effet d'urgence dans le choix du sujet pour inciter à la lecture immédiate de l'e-mail. Le risque est en effet grand de voir le lecteur se dire « Je lirai cet e-mail quand j'aurai le temps » et ensuite l'oublier.
Si cela est pertinent, fixer des échéances du type « Plus que 3 jours avant la fin des soldes » et prolonger l'action avec un second mail « 24 heures avant la fin des soldes ! »

Taille du sujet

Un dernier point concernant le sujet de l'e-mail : sa taille. Selon les logiciels de messagerie et autres webmails, le nombre de caractères affichés peut grandement varier. Un webmail comme celui de Wanadoo limite à 30 le nombre de caractères affichés, alors que Yahoo en affichera la totalité. Pour cette raison, il peut être pertinent de limiter la taille du sujet, ou du moins de placer les mots clés en premier. Par prudence, il est conseillé de se limiter à 25 ou 30 caractères et de vérifier le résultat sur différents clients de messagerie.

Soigner le champ expéditeur

Après le sujet, le champ « De » est l'autre élément décisif d'un e-mail. Ce champ informe les destina-



taires de la provenance du message et pourra lui éviter d'atterrir directement dans la corbeille. D'où l'importance d'une certaine cohérence entre sujet et champ expéditeur.

Des études montrent que le champ expéditeur est utilisé par plus de 60% des personnes sondées pour détecter les spams et choisir entre suppression ou lecture du message. Ce champ expéditeur est limité à 18 caractères seulement.

Deux solutions sont possibles : utiliser le champ expéditeur comme nom, marque ou slogan ou l'utiliser pour afficher l'e-mail de la société.

Si le logiciel de messagerie utilisé ne permet pas de définir de texte pour ce champ expéditeur, il faut alors choisir une adresse e-mail. Cette adresse devra être différente de celle utilisée pour gérer les e-mails non remis ou les réponses. Exemples : «offres@societeabc.com» ou «newsletter@societeabc.com» plutôt que «info@societeabc.com » ou «noreply@societeabc.com ». Cela aidera à inspirer confiance à la cible.

Choisir le bon contenu

Le contenu de l'e-mail doit achever le travail amorcé par le sujet et le champ expéditeur, à savoir intéresser suffisamment la cible pour qu'elle accepte d'entrer dans le jeu du plan marketing.

Au moment de rédiger le message il est important de garder à l'esprit ce pour quoi la personne s'est inscrite sur la liste de diffusion : que souhaite-elle recevoir ? Que peut-on lui apporter qui l'intéresserait ou lui serait bénéfique ?
Pour bien tirer profit d'une liste d'e-mails, il convient donc de bien la connaître. Sans aller jusqu'au « data-mining », il ne faut pas hésiter à analyser les messages précédents. Choisir celui qui a le mieux réussi, le reprendre, l'adapter et le réutiliser. Il est important de tirer profit de l'expérience accumulée.

Un bon message est un message court et qui va droit au but car les internautes sont de plus en plus impatients du fait du bombardement publicitaire

Image ou texte ?
Le pouvoir des images est bien connu et leur efficacité surpasse souvent celle des mots. Elles sont donc de plus en plus utilisées sur l'Internet mais souvent de manière peu judicieuse, sans réelle correspondance avec le texte.

Par ailleurs, il faut veiller à ne pas abuser des images. Le rapport entre quantité d'images et de texte peut en effet avoir un impact significatif sur la réception de l'e-mail.

La plupart des clients de messagerie les plus populaires bloquent par défaut les images contenues dans les e-mails. D'où l'importance de bien s'assurer que les contenus les plus importants : entêtes, titres, liens sont en texte et non en images. De plus, beaucoup de filtres anti-spam s'appuient sur le ratio images/texte pour repérer les spam.

Il est donc conseillé de mélanger images et textes de façon équilibrée. Découper une grosse image en plusieurs petites facilitera également le temps de chargement du message. Compresser les images au maximum diminuera également ce temps de chargement.

Personnaliser ses envois

L'internaute moyen reçoit des centaines d'e-mails

commerciaux chaque mois, et rares sont ceux qui proposent de la personnalisation. Pourtant, personnaliser un message c'est renforcer le lien avec les destinataires et leur inspirer plus de confiance.

Un moyen simple est de s'adresser directement à son interlocuteur par son nom ou son prénom, par exemple : « Bonjour Julie ». Il se peut toutefois que la base de données ne contienne pas les noms et prénoms, auquel cas il faut contourner le problème en interpelant le groupe auquel s'adresse le message : « Cher Voyageur », « Amateur de vin, bonjour », etc.

Les dernières versions des logiciels d'e-mailing permettent de découper le message en plusieurs parties. Celles-ci offriront des contenus entièrement personnalisés en fonction des éléments fournis par le profil décrit dans la base de données.

Ainsi, l'accroche texte + photos encourageant à prendre une carte de fidélité ne sera pas présente dans les messages adressés à ceux qui possèdent déjà cette carte. Elle sera remplacée par une offre personnalisée par rapport aux préférences d'achats et au niveau de fidélité.

De la même façon, les offres seront différentes selon que le destinataire est homme ou femme, marié ou célibataire, avec ou sans enfants, jeune ou senior …

Envoyer intelligemment

Contraintes législatives et désabonnement

Signaler son identité au destinataire et rappeler comment ont été obtenues ses coordonnées.
Il est important de rappeler à ses cibles comment on a obtenu leur adresse e-mail

Pour cela, ajouter au sommet de tous les e-mails une note qui explique clairement qui on est et comment a été obtenue l'adresse e-mail.

Les lois américaines vont jusqu'à imposer l'insertion de l'adresse postale dans tous les messages conçus à l'intention de clients américains. Si cela est possible, il est donc recommandé d'insérer son adresse postale en bas de ses e-mails. Cela rajoute du crédit aux envois et permet d'être en conformité avec les exigences juridiques d'un bon nombre de pays, notamment des Etats-Unis.

Le lien de désabonnement
Tout envoi d'e-mail doit également inclure un lien de désabonnement. Il faut prendre garde de ne pas cacher ce lien dans un tout petit texte dissimulé en bas de page. Un lien de désabonnement bien apparent inspirera confiance à tous les destinataires et montrera le sérieux de l'expéditeur et son souci de conserver la permission de ses cibles.

Comme le veut la loi « Informatique et liberté » du 6 Janvier 1978 « le titulaire du droit d'accès peut obtenir la communication des informations le concernant et exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite. »

La plupart des bons logiciels d'e-mailing permettent de créer des liens de désinscription dynamique et spécifiques à chaque e-mail envoyé.

Tester et apprendre

Les Tests de vérification

Bien tester un e-mail avant de l'envoyer est absolument crucial. La quasi-totalité des environnements de messagerie l'afficheront en effet différemment.

D'un point de vue pratique, ne pas hésiter à établir une petite liste d'adresses e-mail qui serviront de test avant l'envoi final. Cette liste inclura l'adresse de l'expéditeur ainsi qu'une sélection d'adresses fonctionnant avec différents clients de messagerie.

Cela permettra de vérifier ce que les destinataires vont recevoir et d'éviter tout problème.

Vérifiez le nombre et le taux d'ouvertures, de clics et de désabonnements

Il est important de mesurer et comparer les résultats de ses campagnes dans le temps. Pour cela, tester différents objets dans les e-mails et différentes offres promotionnelles entre chaque nouvelle campagne. Avec l'expérience on pourra ainsi déterminer ce qui marche et ce qui ne marche pas vis-à-vis de la cible.

Affiner la présentation de l'e-mail en fonction des résultats.

Le résultat de ces tests servira à améliorer le design des e-mails ou le contenu de la newsletter. Si un sujet particulier apparaît de loin comme le plus populaire en termes de nombre de clics, la newsletter devra systématiquement commencer par ce sujet.

Fiche 6

E-mails et archivage

Sommaire

L'archivage, au-delà du stockage et de la sauvegarde

Bien distinguer gestion de l'information, conservation, stockage, sauvegarde et … archivage ?

Le stockage à la base de tout

Le stockage est la première étape du traitement de l'information dont l'e-mail fait évidemment partie. On peut même dire qu'il conditionne l'existence de l'information : si les données qui constituent l'information produite par une personne ou un système ne sont pas enregistrées et stockées quelque part dans une mémoire informatique ou sur un support physique, l'information n'a plus d'existence matérielle ; elle est perdue ou se limite à une information orale ou mémorielle qui ne peut donc pas être archivée.

Les supports et systèmes de stockage offrent une gamme variée d'outils face à des besoins variés de gestion de l'information dans l'espace et dans le temps :

- technologies optiques, numériques,
- sécurité,
- capacité,
- résistance à l'obsolescence,
- temps d'accès aux données,
- modalités de migration.

Sauvegarde et archivage

Certains utilisateurs et quelques acteurs de la gestion de l'information ont encore tendance à confondre sauvegarde et archivage. Il s'agit pourtant de notions bien distinctes.

La finalité de la sauvegarde est uniquement de permettre une copie des données d'origine dite copie de sécurité afin d'éviter de les perdre en cas de dysfonctionnement du dispositif sur lequel elles sont enregistrées ; la durée de conservation est déconnectée de la valeur du contenu et relative à la périodicité de la sauvegarde (journalière, hebdomadaire, mensuelle, annuelle).

À l'inverse, l'archivage doit permettre une conservation qui peut être beaucoup plus longue, voire ad vitam aeternam. De plus, l'archivage permet une interrogation aisée et fine des objets conservés. Contrairement à la sauvegarde, les données archivées sont considérées comme figées, c'est-à-dire non modifiables.

D'autre part, l'archivage doit permettre de consulter les informations indépendamment de leur système d'origine (ce qui suppose d'extraire et de conserver les informations dans des formats pérennes et si possible ouverts tels que XML) et des droits d'accès initialement affectés aux documents.

Retenons donc que si la sauvegarde est conçue pour la restauration de données et systèmes perdus, l'archivage quant à lui est conçu pour conserver des documents de référence ou probants.

Il y a encore peu, le cycle de vie des données au sein de l'entreprise pouvait se résumer à :

- la création de la donnée,
- son utilisation courante et sa gestion au quotidien, modifications, accès...,
- l'archivage des données à des fins légales ou réglementaires,
- la destruction ou l'archivage patrimonial (histoire de l'entreprise).

Actuellement l'archivage, dans sa version électronique permet de remonter très en amont dans le cycle précédent et intervient ainsi dans une utilisation courante, au quotidien dès l'instant où les données sont figées, ce qui ne modifie en rien leur emploi régulier. Quel meilleur exemple pour illustrer cela que l'e-mail dont la principale caractéristique est justement celle d'être figé (non modifiable) dès sa création.

Gestion Electronique de Documents et Archivage

L'archivage électronique est également à distinguer des outils de gestion électronique de documents. Ces derniers visent en général à répondre aux besoins de partage et d'amélioration de la productivité des services. A contrario, contrairement aux systèmes d'archivage électronique, ces outils prennent rarement en compte la gestion de la valeur probante de ces documents en garantissant leur intégrité sur le long terme.

Correspondances dématérialisées et mémoire d'entreprise

L'archivage est-il une nécessité ?

Ainsi l'archivage électronique ne doit pas être vu comme la simple « dématérialisation de l'archivage papier ». L'une des principales différences provient du fait que les documents électroniques sont archivables dès lors qu'ils ne sont plus modifiables, ce qui n'enlève rien à leur accessibilité. On est loin des interrogations fastidieuses des archives dans les arrières caves poussiéreuses et il serait dès lors plus précis d'utiliser une autre terminologie comme archivage actif (proposé par le Gartner) ou encore « archivage dynamique » afin de bien marquer la différence.

La conséquence en est une prise de conscience très en amont de la notion d'archive sans attendre la quasi fin de vie des documents. La loi elle-même est très claire sur le sujet dans la mesure où l'un des critères de recevabilité d'un écrit électronique en est la garantie d'intégrité depuis son origine et non pas uniquement pendant sa période d'archivage au sens classique du terme.
Comme vu précédemment, l'e-mail constitue un parfait exemple de ce qui précède en matière d'archivage. En effet il possède cette caractéristique de ne plus être modifiable à partir du moment où il existe. Dès lors que l'on conserve des e-mails il s'agit en fait d'un archivage au sens actif du terme. Plutôt que de parler d'archivage des e-mails il serait donc plus juste de présenter cela comme une gestion optimisée et efficace de ces derniers.

Pour être tout à fait précis, il est parfaitement possible de « gérer » ses e-mails au quotidien et au bout d'un certain temps de les archiver au sens classique du terme. Cependant une telle approche a pour principal mérite de se priver de tous les avantages liés à l'archivage dynamique des e-mails et de leur gestion au quotidien.

Qui est concerné par l'archivage ?

De plus en plus d'informations transitent par les e-mails, ce qui ne va pas sans poser un certain nombre de problèmes auxquels tout chef d'entreprise se doit de trouver des réponses.

Sans vouloir aborder ici les aspects purement sécuritaires, traités par ailleurs, nous nous attacherons à plutôt définir la mise en place de moyens destinés à simplifier la gestion des e-mails au quotidien, tant du point de vue de l'utilisateur, que du directeur informatique et 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 e-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 ! Par rapport à ce qui précède, la sauvegarde des données ne doit plus s'appliquer aux données figées dans la mesure où elles sont éligibles à l'archivage. Il y a là un gain potentiel considérable à réaliser par simple élimination des doublons et autre duplication d'information totalement inutile à supprimer. L'autre vrai problème consiste à pouvoir si possible éliminer les e-mails qui n'ont aucun sens à être conservés mais toutefois avec la certitude de ne pas éliminer des e-mails potentiellement utiles.
Remarque : le décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques impose aux opérateurs de communication de conserver la trace des échanges électroniques et donc des e-mails. Bien que cette loi ne concerne a priori que les opérateurs, elle concerne en réalité de plus en plus d'entreprises ayant mis en place des réseaux ouverts et notamment Wi-fi.

Côté archiviste, l'e-mail constitue une source d'information de plus en plus critique, notamment sur le plan juridique et patrimonial mais elle constitue également une source d'information difficile à collecter et à traiter du fait d'une part des volumes d'informations véhiculées et d'autre part de la nature

très personnelle et non-structurée de cet outil. Il est essentiel pour les archivistes d'une part d'être en mesure de sélectionner puis de collecter facilement les messages méritant d'être conserver sur le long terme, et d'autre part de disposer d'informations structurées (« méta-données ») exploitables pour retrouver facilement l'information.

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 de traçabilité de l'ensemble des opérations au sein de l'entreprise.

Enfin toujours sous l'angle des contraintes il ne faut pas oublier de prendre en compte celles liées au droit à la conservation de données personnelles, d'où la problématique juridique directement liée aux exigences Informatique et Libertés pour le respect de la vie privée qui induit une durée limitée en rapport avec la finalité d'une conservation.

Par rapport aux aspects juridiques de l'e-mail voir la fiche 4.

Nécessité de s'appuyer sur une politique d'archivage

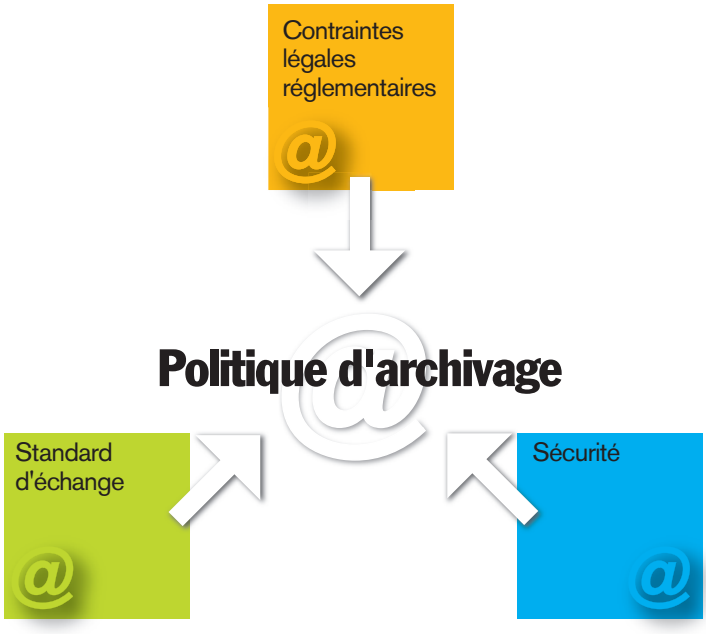
Les règles de fonctionnement définies dans la politique d'archivage des e-mails devront entre autre préciser d'une part les modalités de prise en compte des messages « privés » que l'entreprise n'est pas habilitée à archiver, et d'autre part les conditions d'accès aux messages une fois archivés (délais et conditions de restitution, droits d'accès aux archives…)
Les modalités opérationnelles devront quant à elle prévoir de gérer le dédoublonnement des messages et des pièces jointes associés aux messages reçus par plusieurs utilisateurs de façon notamment à limiter l'espace de stockage dédié à leur archivage.

Le lien avec la sécurité dans l'entreprise

Pourquoi construire une politique d'archivage
L'archivage des e-mails doit être vu comme un projet à part entière dans l'entreprise et abordé dans ce sens avec la définition d'objectifs précis, d'identification des contraintes, du retour sur investissement attendu, d'un accompagnement éventuel auprès des utilisateurs,…

En matière de retour sur investissement la mise en place d'un système d'archivage actif des e-mails doit permettre entre autres d'économiser énormément d'espace disque du simple fait de sortir des procédures traditionnelles de sauvegarde l'ensemble des e-mails comme indiqué précédemment. La où un e-mail et son contenu sont malheureusement aujourd'hui répliqués des dizaines de fois sans aucune utilité, un bon système d'archivage doit permettre la quasi unicité de l'information tout en la laissant accessible à un ensemble de personnes.

Afin d'aider la direction de l'entreprise à gérer ce type de projet il est fortement recommandé de s'appuyer sur une politique d'archivage (PA) qui permet avant tout de bien définir les acteurs en présences, leurs rôles et leurs responsabilités, de lister les contraintes qui pèsent sur l'entreprise (légales, réglementaires, internes), de fixer les objectifs poursuivis en particulier les durées de conservation, de décrire les fonctions attendues par le système d'archivage électronique, de préciser l'environnement de sécurité nécessaire. La politique d'archivage se présente ainsi au centre de différents éléments qui eux-mêmes évoluent dans le temps, d'où la nécessité d'actualiser cette politique régulièrement



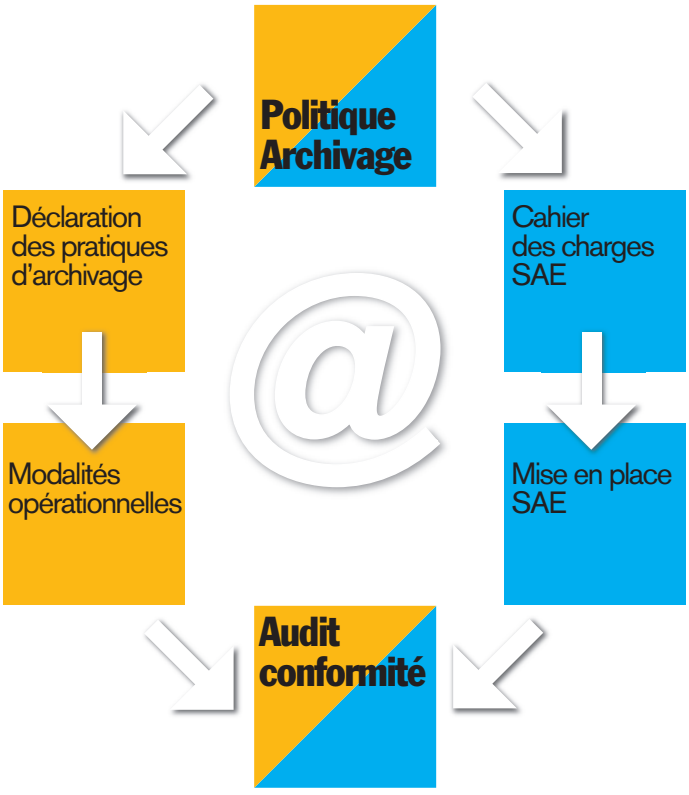
Disposant d'une politique d'archivage adaptée aux e-mails il est alors possible d'en déduire un cahier des charges précis destiné à pouvoir choisir parmi telle ou telle offre du marché.

Remarque : Il est important de noter qu'une telle politique d'archivage, quoique décrite par rapport aux e-mails doit permettre également de traiter l'ensemble des données de l'entreprise, évitant par la même une gestion de l'archivage de type silo, interdisant toute mutualisation de moyens.

Enfin après avoir effectué la mise en place du système retenu il est indispensable de procéder à un audit destiné à vérifier la conformité de ce qui est installé par rapport aux objectifs et exigences définis dans la politique d'archivage.

De la politique d'archivage au système d'archivage électronique

Le schéma ci-après précise sur la partie droite la logique pratique de mise en place d'un système d'archivage électronique adapté tel que défini dans la politique d'archivage tandis que la partie gauche indique les documents indispensables à la bonne réalisation d'un tel système.
Pour plus de précisions sur le sujet voir le site : http://www.ssi.gouv.fr/fr/confiance/archivage.html



Les solutions d'archivage d'e-mails

Bien identifier son niveau de risque pour choisir
Les différents modes d'archivage opérationnel

En simplifiant le propos, il existe à ce jour trois grandes philosophies d'archivage des e-mails.

1. Par l'utilisateur qui est responsabilisé

La première solution consiste à décrire pour chaque utilisateur l'ensemble des procédures retenu par l'entreprise et à adopter sur son poste de travail : organisation des répertoires, création de fichiers .PST, etc…Certes la plus économique mais seulement en apparence, il s'agit d'une solution dangereuse car sans la mise en place de contrôles réguliers et coûteux, le chef d'entreprise n'aura absolument aucune maîtrise de la conservation ou non des données vitales échangées par e-mail.

2. Espace d'archivage sécurisé

Afin de pallier ce dernier inconvénient majeur, une deuxième solution consiste pour l'utilisateur à déplacer ses e-mails, à la demande et/ou en fonction d'une politique prédéfinie, vers un espace mutualisé de stockage disposant de toutes les fonctionnalités de recherche et de migration nécessaire. Sur son poste de travail l'utilisateur garde ainsi la trace et la visibilité sur l'ensemble de ses e-mails mais ne subsiste en réalité qu'un lien pour ceux qui ont été déplacés.

Il existe une variante de cette méthode.
Cette solution peut également être mise en œuvre en deux temps. Dans un premier temps, l'utilisateur transfère tout ou partie des messages qu'il émet ou reçoit dans une application métier, un système de GED (Gestion Electrique de Documents) ou un espace de travail collaboratif en associant aux messages des informations complémentaires (client concerné, type de message …). L'archivage électronique est alors réalisé à partir de ces applications et peut ainsi être mieux structuré que s'il est réalisé directement à partir des boites aux lettres. De nombreuses solutions de GED ou de travail collaboratif offre aujourd'hui cette possibilité de versement en standard.

3. Archivage déporté totalement automatisé

Enfin une troisième et dernière orientation consiste à opérer une copie systématique de tous les e-mails entrant et sortant vers l'espace d'archivage (ce qui nécessite d'avoir son propre serveur de messagerie). L'utilisateur peut alors se permettre de suppri-

mer l'ensemble des e-mails de son poste de travail dès qu'il les a traités dans la mesure où il accède à l'ensemble de sa base e-mail au travers du système d'archivage, généralement disponible via un simple navigateur web.

Attention. Cette solution consistant à automatiser totalement l'archivage rend problématique l'exclusion des e-mails « privés ».

Mise en place de la solution : en interne versus en mode externalisé

En fonction de la solution retenue, certaines peuvent être mises en place en interne dans l'entreprise ou être totalement externalisées en mode ASP chez un tiers archiveur. Là encore tout dépendra du type d'architecture dont l'entreprise dispose (voir fiche 8). En effet les solutions admissibles dépendent étroitement du fait que l'entreprise possède ou non son propre serveur d'e-mails (cf. troisième solution). Enfin certaines sociétés proposent un ensemble complet logiciel et matériel tandis que d'autres offrent uniquement la partie logicielle tout en préconisant un certain type de matériel.

L'ensemble des grands acteurs informatiques (IBM, HP, EMC, HDS, CA, SUN, …) proposent ainsi des solutions d'archivage d'e-mails tandis que d'autres présentent des solutions spécifiques comme AXSOne, SYMANTEC (plus connu pour ses antivirus) ou encore ZANTAZ, actuel leader en matière d'archivage d'e-mail.

Comment choisir l'outil ?

La première chose est de vérifier l'ensemble des caractéristiques fonctionnelles suivantes :

- sécurisation de l'ensemble des e-mails d'un point de vue de l'accessibilité (confidentialité), de l'intégrité, de la traçabilité, éventuellement de la non répudiation (impossibilité de remettre en cause l'envoi ou la réception d'un e-mail) ;
- rationalisation possible des espaces de stockage en fonction de la fréquence et de la criticité des e-mails. Il s'agit en fait de prévoir au besoin un système de migration adapté ;
- catégorisation possible des e-mails afin de permettre la rationalisation évoquée ci-dessus ;
- conservation des e-mails de façon sécurisée et surtout intègre avec vérification de l'intégrité de façon régulière ;
- indexation de l'ensemble des e-mails et des pièces jointes de telle sorte à pouvoir les retrouver facilement ;
- pérennisation des e-mails afin d'assurer une conservation à moyen voire long terme ;
- partage des e-mails au travers de la définition des droits accordés aux utilisateurs ;
- destruction des e-mails à expiration du délai de conservation.

Si la grande majorité des solutions proposées aujourd'hui offre cet ensemble de caractéristiques, la façon d'y répondre n'est pas toujours identique. Ainsi telle solution privilégiera plutôt l'utilisateur et l'ergonomie, telle autre offrira plus de facilités en matière d'administration centralisée, une troisième optimisera les espaces de stockage, etc…

Veiller à la performance

Le choix devra donc se faire en fonction de vos propres objectifs fonctionnels et de vos propres contraintes d'environnement informatique et de coût. Il faudra également veiller à l'importance en matière de performance des systèmes informatique. En effet, archiver est une chose, mais retrouver en est une autre sachant toutefois qu'il s'agit de la base même de l'archivage. Il est clair que retrouver un e-mail parmi plusieurs milliers n'est pas la même chose que parmi plusieurs centaines de milliers voire de millions. Si le volume global des e-mails à conserver est en général tout à fait acceptable, le nombre d'items est quant à lui en général considérable et la taille des index peut même dépasser la taille de l'e-mail d'origine !

Enfin, avant de se décider pour une solution, bien veiller également à la notion d'évolutivité, de réversibilité (très important dans le cas d'un tiers archivage) et d'interopérabilité afin de ne pas devoir remettre en cause le système retenu dans quelques années ce qui aurait pour principale conséquence de coûter extrêmement cher à l'entreprise.

Pour en savoir plus :

- Livre blanc « L'archivage électronique à l'usage du dirigeant » téléchargeable sur :
  - Cigref : http://cigref.typepad.fr/cigref_publications/fedisa/index.html
  - FedISA : http://www.fedisa.eu/index.php?pc=articles
- Dunod, collection Management des Systèmes d'Information : « Dématérialisation et archivage électronique. (Mise en œuvre de l'ILM)

Partie 3

Fiche 7

Que faire, face aux comportements déviants ?

Sommaire

Introduction

L'accroissement du volume d'e-mail est un fait avéré. Toutes les messageries électroniques se remplissent avec des e-mails que l'on peut faire entrer dans 2 ou 3 grandes catégories :

- les e-mails non sollicités, et dont la réception peut être associée à une perturbation de l'activité normale ou à une pollution ;
- les e-mails non sollicités, mais dont la réception peut légitimement se justifier ;
- les e-mails qui correspondent à une activité que l'on pourrait qualifier de "normale".

La facilité d'utilisation et de diffusion des e-mails peut aussi devenir un fléau lorsqu'ils sont utilisés mal à propos.
Nombreuses sont les entreprises dont les salariés voient leur messagerie professionnelle se remplir et être polluée par des e-mails qui ne correspondent en rien à leurs attentes ou à leur activité professionnelle. Et il en est de même avec les messageries personnelles.
L'e-mail est ainsi victime de sa facilité d'utilisation, de son faible coût et finalement, de son succès.

Cette fiche fait le point sur ces différents types d'e-mails :

- le SPAM, qui est constitué d'e-mails non sollicités ;
- le PHISHING, méthode notamment basée sur des e-mails et qui vise à leurrer les destinataires afin de leur soustraire certaines de leurs informations confidentielles ;
- le HOAX, ou canular, version moderne des chaînes fondées sur la crédulité humaine ;
- les VIRUS, véhiculés par les e-mails comme des pièces jointes malveillantes ;
- avec l'une des conséquences possibles, les BOTNET, qui sont des réseaux de machines compromises pouvant être contrôlées à distance.

L'objectif de cette fiche est, pour chacun de ces

types, de le décrire succinctement, d'en montrer un exemple, et d'émettre quelques préconisations pour l'utilisateur et pour le décideur afin de faire changer les comportements.

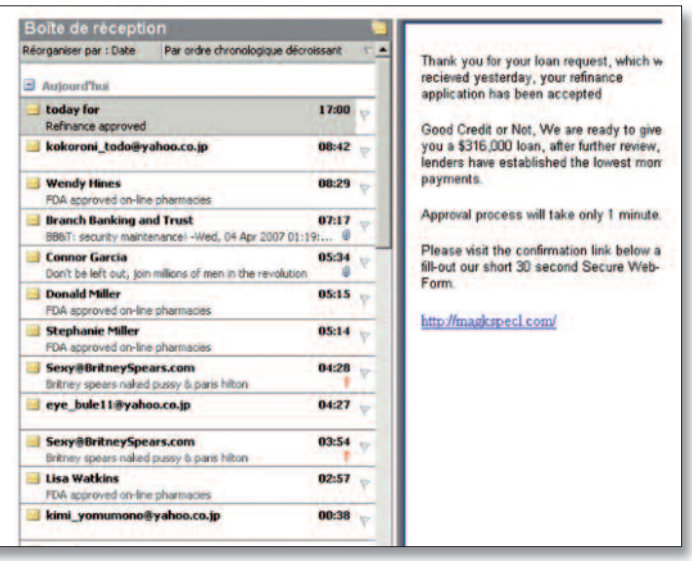
Le SPAM

Le SPAM est un e-mail non sollicité, envoyé massivement et souvent de manière répétitive, à vocation le plus souvent commerciale, à des destinataires dont l'adresse électronique a été collectée sans leur consentement explicite. Il est appelé également pourriel au Canada ou pollupostage en France. Le terme SPAM a été repris suite à un célèbre sketch des Monthy Python dans les années 70 et à sa lancinante réplique "spam, spam, spam, …".

Les chiffres varient selon les sources, mais pour la plupart elles estiment que le pourcentage de SPAM qui transite sur l'Internet serait supérieur à 75% du total des e-mails.
Les contenus de ces SPAM vantent souvent les mérites de soi-disant produits naturels ou miraculeux aux vertus rajeunissantes, aux effets miraculeux, ou capables de renforcer les performances physiques, le tout, bien entendu à des prix bien plus faibles qu'ailleurs. Parfois, il s'agit de produits pharmaceutiques d'autres natures, de montres prétendument de luxe ou de logiciels bureautiques dont on est censé pouvoir faire l'acquisition avec d'incroyables réductions.

Un exemple d'e-mail de SPAM :

Cette boîte aux lettres est envahie de SPAM



Recommandations

Pour l'utilisateur :

1) Vivre avec les SPAM

De plus en plus souvent, il est proposé dans le texte de l'e-mail, de suivre un lien ou de se connecter sur un site pour demander à être retiré de la liste de diffusion.
La première recommandation est de ne pas le faire ! En effet, cela risque surtout de produire l'effet inverse : demander à être retiré d'une liste de diffusion démontre l'utilisation réelle de l'adresse e-mail, ce qui incitera encore plus à l'inonder de nouveaux SPAM ! Donc, si vous ne connaissez pas l'expéditeur d'un e-mail, supprimez le message sans lire son contenu.

2) Disposer d'un anti-virus à jour

L'une des fonctions de l'anti-virus est de détecter les tentatives d'utilisation illicite d'un logiciel de messagerie. Si le poste de travail se trouve être infecté par un code malveillant, ce dernier peut être à l'écoute d'un ordre provenant d'Internet, et extraire des bases locales de destinataires ou d'expéditeurs pour collecter de nouvelles adresses d'e-mail, ou utiliser de façon furtive le logiciel de messagerie pour diffuser à son tour de nouveaux SPAM. Un anti-virus avec une signature anti-virale à jour permettra dans la plupart des cas, de détecter et d'éradiquer ce type de code malveillant.

Pour le décideur

3) Utiliser des filtres anti-SPAM

Aussi bien sur les passerelles, sur les relais et les serveurs de messagerie il est possible d'installer des logiciels qui vont détecter puis filtrer ces SPAM, mais une telle possibilité est aussi offerte pour les postes de travail. Ainsi, la plupart des logiciels clients de messagerie permettent aux utilisateurs de définir des filtres basés sur des mots clés ou sur des noms ou domaines émetteurs. D'autres solutions spécifiques sont vendues pour jouer le rôle de filtre de détection et de suppression de SPAM. Outre les performances et les caractéristiques techniques de ces produits, la granularité et la finesse de la détection et du filtrage sont des critères de choix importants avec le mécanisme de mise à jour des filtres.
Attention cependant aux messages identifiés comme SPAM alors qu'ils n'en sont pas (ce que l'on appelle des "faux positifs"). Il est aussi recommandé d'au moins en parcourir la liste avant de les effacer. Enfin, certains filtres anti-spam ajoutent devant le titre du message le marqueur "**SPAM**" et le délivre ainsi, laissant au destinataire le soin de choisir le mode de traitement à faire pour l'e-mail litigieux.

4) Suivre l'évolution de la législation

Devant l'ampleur du phénomène du SPAM, une directive européenne publiée en juillet 2002 oblige l'émetteur d'un e-mail à solliciter la permission de son interlocuteur avant de lui présenter son produit. Les Etats-Unis, tout en autorisant a priori l'émission d'un message publicitaire, obligent l'émetteur à avertir le récepteur de son droit de demander à être retiré de sa liste de distribution.

Les législations diffèrent donc d'un pays à l'autre, il est intéressant d'en suivre les évolutions. Dans le cas d'une entreprise internationale, il convient aussi de respecter les différentes législations locales.

Le PHISHING

Le phishing, aussi appelé "hameçonnage" au Canada et "filoutage" en France, est une tentative de récupération de données confidentielles basée sur la tromperie et le leurre, afin de les utiliser à des fins frauduleuses.

Le mot "phishing" vient de la contraction des mots "phreakers", un "ancien" mot qui désigne des fraudeurs des réseaux téléphoniques qui y accèdent et l'utilisent sans payer, et "fishing", l'action de pêcher, qui dans ce contexte se transforme en une pêche aux naïfs !

Son principe est simple et repose sur trois mécanismes :

- Un e-mail est reçu semblant provenir d'une autorité dont la réputation est grande et dont l'identité ne peut pas être mise en doute : une banque, avec utilisation du logo, des polices de caractères, des couleurs, et du style, un site de vente en ligne, un site de partage et d'échange... Tout alors semble conforme et rassurant. Il est généralement demandé au destinataire de l'e-mail de ressaisir les informations permettant de l'identifier de façon formelle. Le prétexte n'est pas toujours crédible (une banque ayant perdu les coordonnées de ses clients par exemple !). Un lien est généralement proposé et permet à l'utilisateur de se connecter sur le soi-disant site.

- Une fois connecté sur le site, il est donc demandé de donner les réponses aux quelques questions dont, les codes d'accès en ligne, le numéro de carte bleue avec bien entendu son code secret, le ou les mots de passe, ….

- Une fois les éléments d'identification recueillis, il ne reste plus au phisher qu'à tirer profit concrètement de son butin.

La messagerie électronique n'est donc qu'un véhicule pour des attaques de type phishing, mais sa combinaison avec une usurpation d'identité d'un prétendu émetteur rend le tout crédible… à première vue.

Le taux de phishing est en constante augmentation. Même si les banques anglo-saxonnes et nord-américaines ont été les premières à faire les frais de ces tentatives d'extorsion de fonds, plusieurs sociétés françaises ont aussi été affectées.

Les auteurs de phishing jouent aussi parfois sur les noms de domaines, ou même parfois sur les similitudes entre les caractères.

Prenons par exemple une organisation française dont le nom serait CNPF (sic), le nom de domaine complet « cnpf.fr » et le site Web « www.cnpf.fr ». Il y aurait ainsi au moins deux types d'attaques de phishing dont elle pourrait être victime :

- des personnes malveillantes pourraient vouloir faire croire que cette organisation dispose d'une interface « en ligne » pour les membres et déposer le nom de domaine « cnpf-enligne.fr » ou « cnpf-online.fr ». Il leur suffirait alors d'envoyer des e-mails en prétendant qu'un nouveau site dédié vient de s'ouvrir, de demander aux destinataires de s'y connecter, et de remplir les questionnaires en ligne, pour un motif fallacieux.

- Si de tels noms de domaines sont déjà déposés, ils pourraient envoyer des e-mails demandant aux destinataires de se connecter, en cliquant sur un lien directement fournit dans le corps de l'e-mail. Ils pourraient ainsi écrire « www. cnpf-enligne.fr » (le « l minuscule » est remplacé par un « I majuscule », ou WWW.CNPF-0NLINE.FR (le « O majuscule » est remplacé par « zéro ».

Dans la réalité, on trouve de nombreux autres exemples de « jeux » sur les caractères, et pas seulement contre des institutions financières ou bancaires.

À la date de rédaction de cet ouvrage, les premiers noms de domaines avec des caractères accentués font leur apparition (« IDN » ou « Internationalised Domain Names » pour noms de domaines internationalisés). L'accentuation de certaines lettres de la langue française alliée à l'imagination débordante des personnes malveillantes incite donc à la méfiance.

Exemple d'un faux message bancaire :

Recommandations

Pour l'utilisateur

1) Connaître les habitudes "Internet" de ses partenaires financiers (banque, assurances, …)

Il n'arrive quasiment jamais qu'une banque communique directement avec ses clients par e-mail pour leur demander d'aller se connecter sur un site pour mettre à jour ses coordonnées. Et il est encore bien plus rare que cette même banque, qui a délivré une carte de crédit par exemple, demande à ses clients de lui communiquer des informations secrètes qu'elle n'est pas censée avoir !

2) Ne jamais cliquer sur un hyperlien Web contenu dans un e-mail

Un hyperlien trouvé dans un e-mail est une facilité donnée à l'utilisateur pour aller sur une page Web sans avoir à en saisir l'adresse sur son navigateur, surtout si cette adresse est longue et compliquée.
En cas de doute sur la légitimité d'un e-mail ou sur le site cible proposé, il est préférable de ne rien faire, et de contacter sa banque par téléphone pour vérification !
De façon générale, pour aller sur des sites connus, autant les conserver dans sa liste de liens privilégiés au sein du navigateur Internet.

3) Se méfier quand on donne des renseignements confidentiels

Dans la mesure où il s'avère nécessaire de fournir des informations confidentielles, il est recommandé de vérifier que le site en question offre au moins un mode de raccordement sécurisé en HTTPS (avec un pictogramme de cadenas sur lequel on peut cliquer pour connaître quelle autorité a signé le certificat authentifiant le site),

Pour le décideur

4) Eduquer les utilisateurs

Les attaques en phishing reposant essentiellement sur la crédulité et le manque de recul des utilisateurs, un effort d'éducation sur la connaissance de la cybercriminalité et la manière de la contrer est la première des défenses.

De plus, les solutions de filtrage des accès Web proposent souvent une catégorie "Phishing" composée de sites reconnus comme étant des sites servant au phishing. Il faut bien sûr interdire l'accès aux pages Web de cette catégorie.

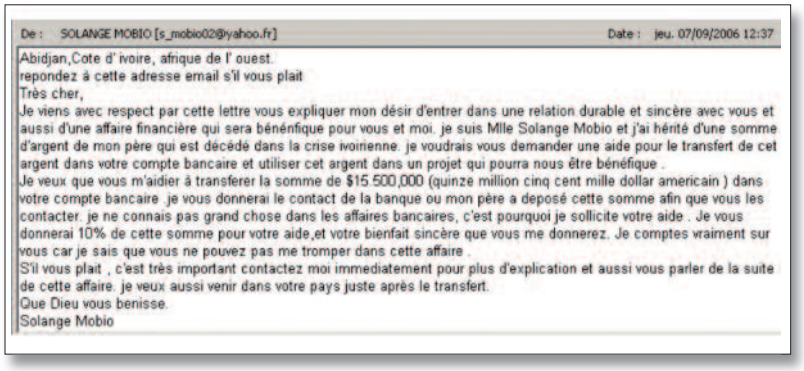
Les HOAX, ou contenus malveillants

Certains e-mails véhiculent des contenus qui jouent sur la naïveté, l'ignorance ou la peur du destinataire pour l'inciter à se situer dans un contexte de crise ou pour lui extorquer de l'argent. A titre d'exemple on peut citer, le "hoax" et la fraude nigériane.
Ces e-mails malveillants, appelés HOAX ou canulars, cherchent soit à saturer Internet (principe des chaînes), soit à porter directement préjudice (incitation de l'e-mail à supprimer un fichier système indispensable en faisant croire que c'est un virus).

Le HOAX, déclinaison moderne des lettres chaînées, est un phénomène né pratiquement avec la messagerie électronique. Il en tourne plusieurs milliers en permanence sur l'Internet, et ils parviennent à leurs destinataires au hasard des listes de distribution.

La fraude nigériane, censée donner une commission sur des transferts de fonds … suspects, cherche à obtenir des renseignements sur le compte bancaire de sa victime. Elle est l'œuvre de mafias, très organisées et expertes dans l'art d'agir sur les comptes en banque !

Exemple de « fraude nigériane » :



De : SOLANGE MOBIO [s_mobio02@yahoo.fr] Date : jeu. 07/09/2006 12:37

Abidjan,Cote d' ivoire, afrique de l' ouest.
repondez à cette adresse email s'il vous plait
Très cher,
Je viens avec respect par cette lettre vous expliquer mon désir d'entrer dans une relation durable et sincère avec vous et aussi d'une affaire financière qui sera bénénfique pour vous et moi. je suis Mlle Solange Mobio et j'ai hérité d'une somme d'argent de mon père qui est décédé dans la crise ivoirienne. je voudrais vous demander une aide pour le transfert de cet argent dans votre compte bancaire et utiliser cet argent dans un projet qui pourra nous être bénéfique .
Je veux que vous m'aidier à transferer la somme de $15.500,000 (quinze million cinq cent mille dollar americain) dans votre compte bancaire .je vous donnerai le contact de la banque ou mon père a deposé cette somme afin que vous les contacter. je ne connais pas grand chose dans les affaires bancaires, c'est pourquoi je sollicite votre aide . Je vous donnerai 10% de cette somme pour votre aide,et votre bienfait sincère que vous me donnerez. Je comptes vraiment sur vous car je sais que vous ne pouvez pas me tromper dans cette affaire .
S'il vous plait , c'est très important contactez moi immediatement pour plus d'explication et aussi vous parler de la suite de cette affaire. je veux aussi venir dans votre pays juste après le transfert.
Que Dieu vous benisse.
Solange Mobio

Recommandations

Pour l'utilisateur :

1) Vivre avec les contenus malveillants

Le meilleur conseil est surtout de ne pas devenir complice d'un HOAX en le transmettant à d'autres destinataires. Il ne faut évidemment pas répondre aux sollicitations des hoax et de la fraude nigériane. Avec un peu d'habitude, il devient facile de détecter l'arnaque et de ne pas tomber dans le piège.

2) Signaler hoax et fraude nigériane auxquels vous êtes confrontés

Il existe des sites Internet sur lesquels on peut signaler ce type d'e-mails malveillants, par exemple www.hoaxbuster.com pour les HOAX, ou même quelques sites étatiques.

Pour le décideur

3) Sensibiliser les salariés

La messagerie électronique est un outil mis à disposition du salarié uniquement à des fins professionnelles. Un message provenant d'une source inconnue, dont la teneur sort de l'ordinaire, n'a pas à être traité. Le chef d'entreprise est par ailleurs responsable des actions de ses employés durant leurs heures de travail, avec les outils qu'il leur a fournis, conformément à la politique de sécurité que l'entreprise doit avoir publiée.

Interdiction de participer à la transmission d'un HOAX durant les heures de travail, éducation aux dangers du piège d'une fraude nigériane sont des éléments pouvant être portés dans la charte de sécurité de l'entreprise.

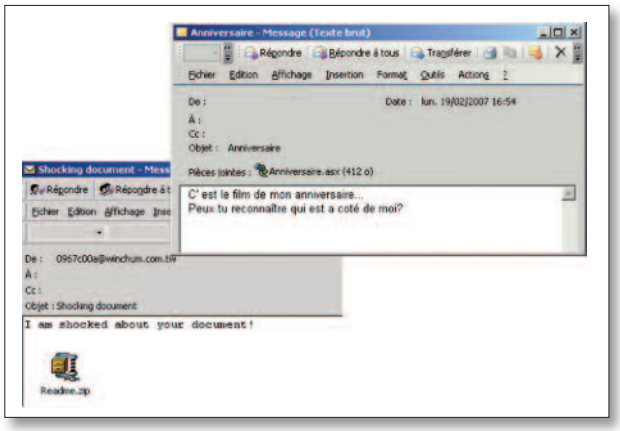
Les VIRUS véhiculés par les pièces jointes malveillantes

Un e-mail accompagné d'un ou de plusieurs fichiers attachés présente une probabilité non négligeable que ces fichiers soient infectés. Cela est particulièrement le cas avec des fichiers exécutables '.exe', de fichiers de liaison '.pif', Mais cela est parfois aussi vrai avec des fichiers bureautiques en ".doc", ".xls", ou même en ".zip".

Un virus est un code qui s'installe sur un poste de travail, après ouverture d'un fichier joint contaminé, et exécute sa « charge utile », pour détruire certaines catégories de fichiers du disque ou espionner l'utilisation de l'ordinateur à des fins de recueil d'informations secrètes.

On compte 60.000 souches de virus référencées et il s'en crée chaque mois entre 300 et 500. Jadis un anti-virus les identifiait assez facilement par leur signature spécifique et les éradiquait. Aujourd'hui les virus mutent, changent de signature, changent d'emplacement disque et se jouent des antivirus et parfois même les empêchent de fonctionner. Un poste de travail connecté à l'Internet sans protection est visité, voire contaminé, dans l'heure par l'extérieur.

Exemple d'e-mails véhiculant sans doute un virus



Recommandations

Pour l'utilisateur

1) Protéger le poste de travail par un antivirus à jour

La meilleure contre-mesure à opposer à un virus est de disposer sur son poste de travail d'un bon logiciel anti-virus tournant en tâche de fond avec sa base de signature fréquemment mise à jour. Cette mise à jour ne peut être réalisée que dans la mesure où un contrat a été souscrit auprès de l'éditeur du logiciel anti-virus ! Il s'agit donc d'une action qui doit être

menée en amont, puis renouvelée régulièrement.
En amont, une infrastructure de réception des e-mails peut être constituée avec d'autres logiciels anti-virus couplés aux serveurs de messageries comme mentionné ci-après.

2) Prendre garde aux pièces jointes attachées aux e-mails
Si on ne connaît pas l'émetteur ou la provenance d'un e-mail, il est particulièrement déconseillé d'exécuter un fichier qui lui est attaché, compte tenu du très fort risque de contamination. De même, avant d'envoyer un fichier en attachement à un e-mail, contrôlez le par votre anti-virus. Il est ainsi recommandé de privilégier un envoi de fichiers dans un format "passif", par exemple au format Acrobat PDF, plutôt que dans un format potentiellement "actif" car pouvant contenir des codes actifs, comme par exemple avec les logiciels de la suite bureautique Office (Word, Excel …) pouvant contenir des macro qui s'exécutent lors de l'ouverture du fichier.

Pour le décideur
3) Protéger l'entreprise
Un antivirus mutualisé sur le serveur de messagerie de l'entreprise est capital pour le contrôle systématique des messages entrants et sortants. De plus, il ne sera efficace que si sa base de signature est le plus à jour possible.

Il semble indispensable de mettre en place une solution de filtrage et d'éradication des codes malicieux dès l'entrée sur le réseau de l'entreprise, mais il l'est tout autant en sortie du réseau de l'entreprise, car la contamination des clients, partenaires et prospects rend le chef d'entreprise civilement responsable des dommages commis à l'extérieur par les e-mails de ses employés.

Le concept de BOTNET et de prise de contrôle à distance des machines…

Le BOTNET est un réseau de machines infectées par un type de virus particulier (le BOT) permettant d'en prendre le contrôle à distance, à l'insu de son propriétaire. Bien que semblant fonctionner normalement, le poste de travail est prêt à exécuter les ordres envoyés par un serveur maître, situé quelque part sur l'Internet, le plus souvent dans un pays étranger à législation généralement différente, voire inexistante. Ce serveur de commande, en général aux mains de mafias, en monnaye l'utilisation, par le biais de location ou d'un « service clé en main » par exemple pour bloquer un site marchand en réalisant une attaque massive en déni de service.

À ce jour, les plus grands réseaux de BOTNET répertoriés par les éditeurs de logiciels anti-virus comptent plusieurs centaines de milliers de postes compromis et potentiellement actifs

Cette contamination peut avoir deux sources potentielles :
- le téléchargement de fichiers (exécutables, utilitaires, jeux, musique, films,…) à partir de sites ou de réseaux peu fiables : sites de téléchargements « gratuits », réseaux de Peer-To-Peer ;
- exécution d'une pièce jointe attachée à un e-mail.

Recommandations

Pour l'utilisateur :
1) Vérifier fréquemment la configuration de votre machine
Les anti-virus ont une certaine efficacité pour détecter et éradiquer ces BOTS, petits logiciels qui infectent les PC. Il existe également des utilitaires (payants ou en mode freeware) qui analysent en détail la configuration de la machine et proposent de la nettoyer. Ne pas hésiter à y avoir recours souvent, en prenant garde, lors de la phase de nettoyage.

2) Écouter les plaintes contre des agissements dont vous n'êtes pas au courant
Si vous êtes l'objet de plaintes (pour envoi de SPAM vers une messagerie dont vous n'avez jamais entendu parler, pour une attaque en déni de service,…), ces accusations sont peut-être réellement fondées du fait de la contamination de votre machine. Procédez à une vérification, et à son éventuel nettoyage.

Pour le décideur :
3) Dans le cadre de l'entreprise, portez plainte si vos machines sont compromises
En France, une agression sur un système d'information constitue un délit, et est puni par la loi. Si vous pensez que votre réseau et ses postes de travail ont été agressés ou contaminés, vous pouvez notamment porter plainte auprès des autorités et organismes compétents tels que la BEFTI à Paris, et l'OCLCTIC. Le possesseur du serveur maître pourra alors être inquiété par la justice, surtout s'il réside dans un pays où la loi est répressive concernant les agressions sur les systèmes d'information.

Fiche 8

Utilisation de l'e-mail sécurisé : chiffrement, signature

Sommaire

À propos de la signature électronique

Données de base

Sans entrer dans le détail de la cryptographie, le principe de signature électronique nécessite la délivrance d'une bi-clé constituée d'une clé publique et d'une clé privée. Cette dernière doit absolument rester secrète et à la seule connaissance de son détenteur (sauf pour le chiffrement). 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 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.

Valeur juridique d'un e-mail signé : voir supra fiche 4

Signature et chiffrement d'un e-mail

Un exemple concret d'utilisation : l'e-mail sécurisé

- **Les pages qui suivent présentent un exemple d'utilisation du certificat dans le cadre de la signature et du chiffrement des e-mails**

- **Le scénario que nous avons déroulé est très simple:**
  - Un émetteur prépare un message, le signe et le chiffre, et l'envoie à un destinataire.
  - Le destinataire, à son tour, reçoit le message, l'ouvre, valide la signature de l'émetteur et déchiffre le message.

- **Ce scénario est basé sur une infrastructure de messagerie traditionnelle.**
  - Les utilisateurs sont munis de certificats sur leur poste de travail. Ces certificats sont publiés dans l'annuaire de messagerie.

Ce que garantissent la signature et le chiffrement d'e-mail

- **La signature d'un e-mail à l'aide d'un certificat électronique :**
  - Permet d'authentifier l'émetteur du message ;
  - Permet de se prémunir contre l'éventualité d'une répudiation du message et de ses pièces jointes par son émetteur ;
  - Garantit que le message et ses pièces jointes n'ont pas été altérés entre le moment où il a été émis et le moment où il est ouvert par son destinataire.

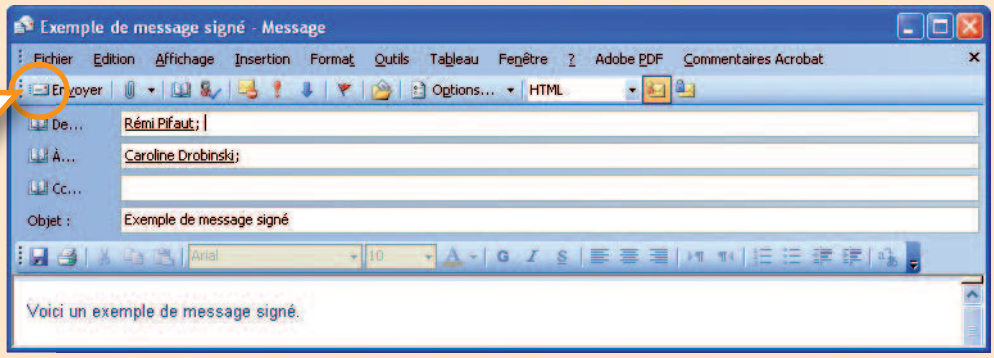
- **Le chiffrement d'un message permet de garantir la confidentialité totale des informations échangées (message et pièces jointes).**

Démonstration : envoi d'un e-mail signé

- **Pour illustrer la signature d'e-mails, le scénario suivant est présenté :**
  - Un émetteur prépare un message, le signe et l'envoie à un destinataire ;
  - Le destinataire reçoit le message, l'ouvre et vérifie la signature de l'émetteur.

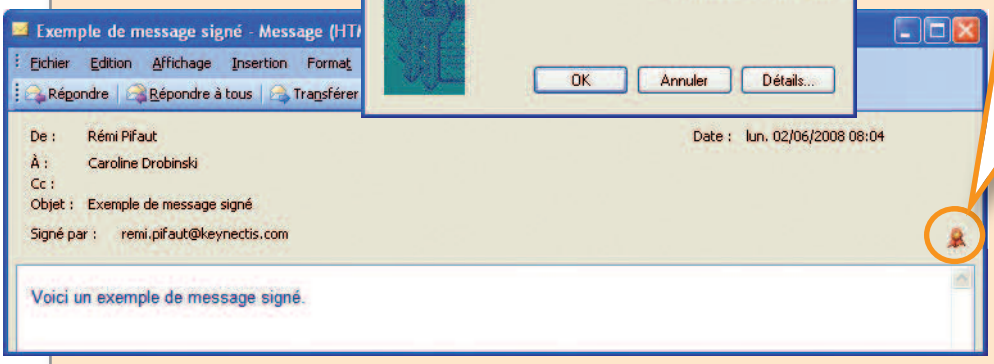
- **Ce scénario est basé sur une infrastructure de messagerie traditionnelle**
  - L'émetteur est muni d'un certificat électronique sur son poste de travail. (voir page ci-contre)

L'émetteur écrit son e-mail puis clique sur l'icône de signature d'e-mail de son logiciel de messagerie ;
Lors de l'envoi du message, le logiciel de messagerie va demander à activer la clé privée présente sur le poste de l'émetteur.
Dans le cas où la clé privée est sécurisée par utilisation d'un mot de passe, une nouvelle fenêtre apparaît.

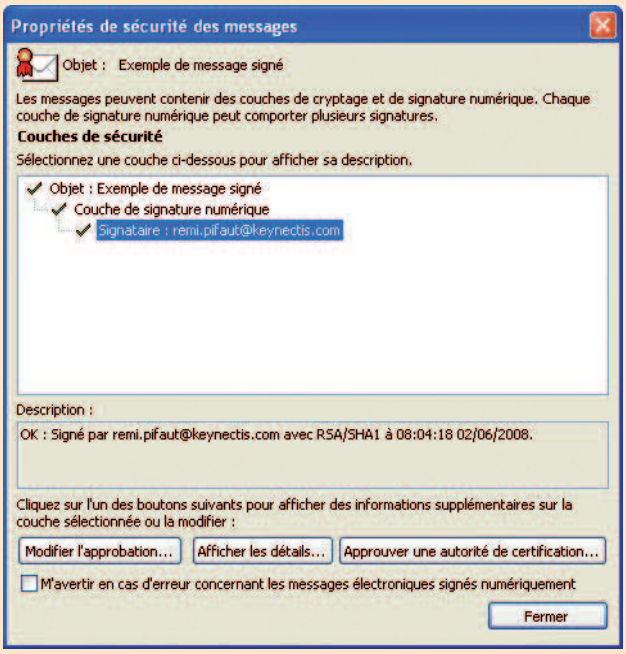


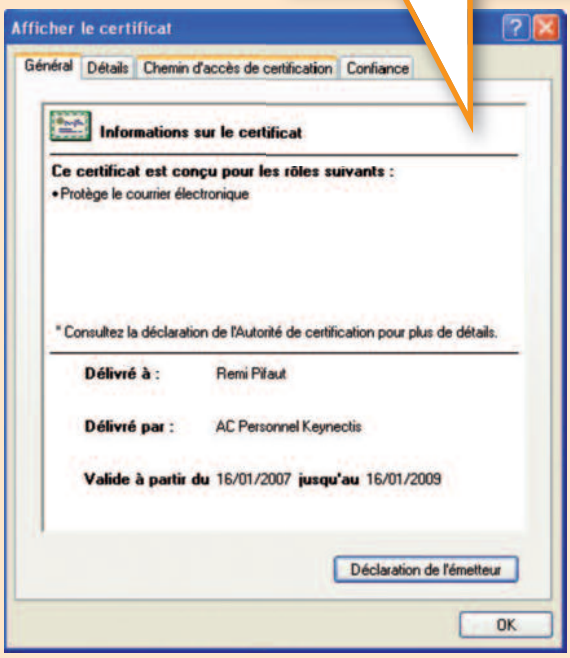
Sur correspondance du mot de passe entré, le message est alors signé de manière transparente par le logiciel de messagerie de l'émetteur.

Lors de la réception de l'e-mail, le destinataire est averti que l'e-mail a été signé. Ceci se traduit par l'apparition d'un certificat présent dans l'e-mail.



En cliquant sur l'icône représentant un certificat, le destinataire peut voir le détail du certificat qui a signé l'e-mail et vérifier aussi la signature de l'e-mail.





Démonstration : envoi d'un e-mail chiffré

- **Pour illustrer le chiffrement d'e-mails, le scénario suivant est présenté**
  - Un émetteur prépare un message et l'envoie en le chiffrant à un destinataire
  - Le destinataire reçoit le message, le déchiffre et l'ouvre

- **Ce scénario est basé sur une infrastructure de messagerie traditionnelle**
  - L'émetteur est muni d'un certificat électronique sur son poste de travail Il est important de préciser que ce certificat électronique ne peut en général pas être le même que celui utilisé pour signer. La contrainte essentielle de tout processus de chiffrement consistant à gérer les clés dans le temps, il est clair que ces dernières devront être détenues au minimum par deux personnes distinctes, contrairement à la clé privée utilisée dans le cadre de la signature électronique qui doit absolument rester secrète et à la seule connaissance de son détenteur.

(Voir page ci-contre)

Exemples d'applications d'un e-mail signé

La messagerie se différencie de la navigation web par la persistance des messages transmis. Cette persistance permet en particulier d'aller plus loin dans les fonctions de sécurité et de confiance que la messagerie peut véhiculer.

À titre d'exemple :

- l'authentification interactive est remplacée par une signature électronique authentifiant l'envoyeur et scellant en intégrité le message et ses pièces jointes ;

- le cryptage (chiffrement) de connexion est remplacé par le chiffrement persistant des messages, permettant ainsi de les conserver sous cette forme confidentielle protégée sur la durée. Bien entendu, cette potentialité s'accompagne de nécessaires précautions dans la gestion des clés : si l'utilisateur perd ses clés, il peut être gênant qu'il ne puisse déchiffrer ses anciens e-mails, des systèmes de back up de clés (aussi appelés séquestre et recouvrement de clés) peuvent alors être mis en place.

Ces propriétés ouvrent des possibilités nouvelles à l'utilisation de l'e-mail, non plus seulement comme facilitateur de communication mais comme véritable vecteur de dématérialisation d'échanges sensibles ou engageants. On a pu ainsi observer l'apparition de nouveaux services comme :

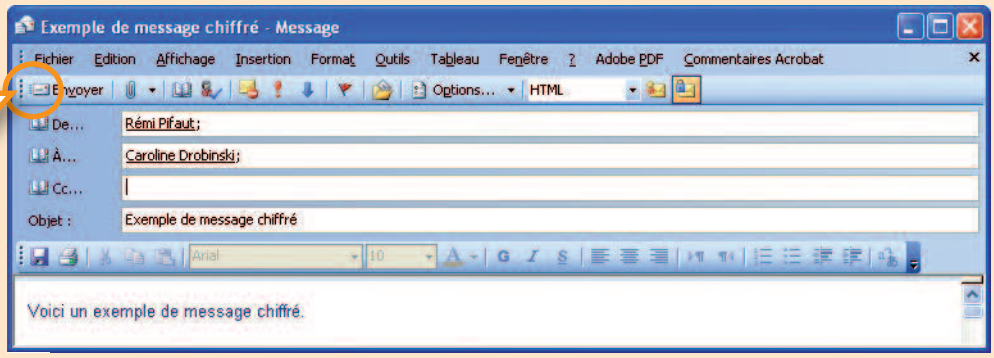
- la soumission électronique d'offres aux marchés publics, protégée en authenticité et en confidentialité ;
- l'échange d'actes administratifs authentiques (par exemple les délibérations communales soumises au contrôle de légalité du préfet) ;
- l'échange d'informations sensibles inter sites dans les entreprises (Pharmacie, Automobile, Aéronautique, Défense) ;
- la transposition en électronique du courrier recommandé avec accusé de réception, aujourd'hui proposé par La Poste et d'autres, et utilisé notamment par les professions du droit (avocats, notaires, greffiers, ...).

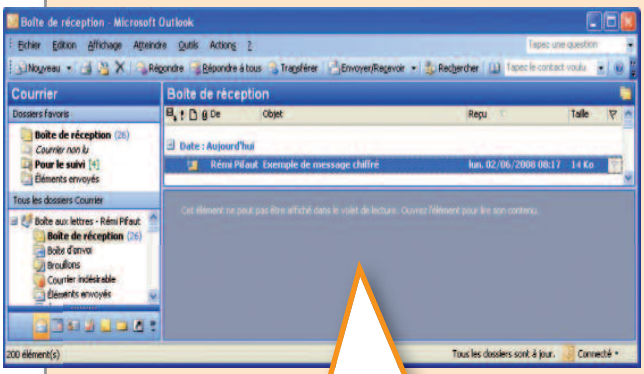
Utilisation de l'e-mail sécurisé : chiffrement, signature

L'émetteur écrit son e-mail puis clique sur l'icône de chiffrement d'e-mail de son logiciel de messagerie.

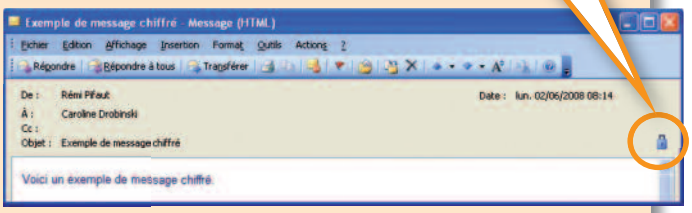
Lors de l'envoi du message, le logiciel de messagerie va demander à utiliser la clé publique contenue dans le certificat du destinataire afin de chiffrer l'e-mail.

L'e-mail est alors chiffré de manière transparente par le logiciel de messagerie de l'émetteur.





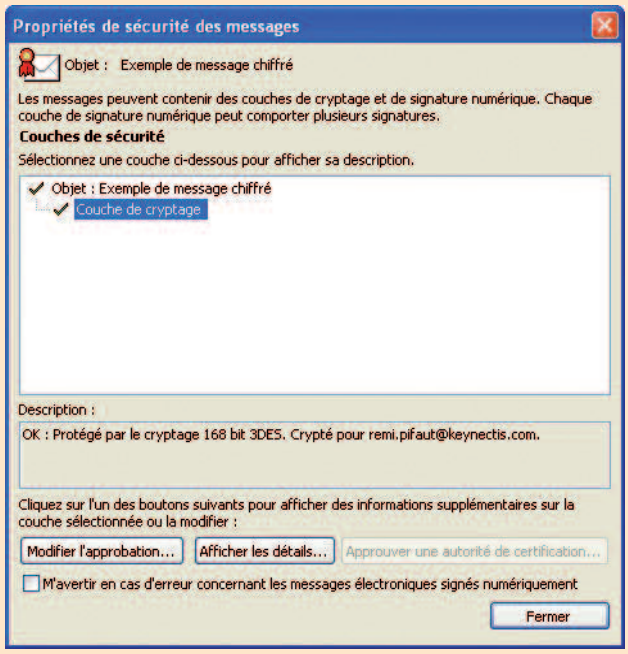
Une icône de chiffrement indique simplement que le message a été reçu chiffré.



Lors de la réception de l'e-mail, le destinataire reçoit un e-mail chiffré. Ceci se traduit notamment par le fait que le mail n'est pas lisible en l'état dans la zone de prévisualisation d'Outlook. Pour pouvoir lire l'e-mail, il faut l'ouvrir.

Pour lire le mail, le destinataire doit activer sa clé privée (utilisée pour déchiffrer l'e-mail) pour que le message puisse s'afficher en clair.

En cliquant sur l'icône représentant un cadenas, le destinataire peut avoir des détails sur le chiffrement de l'e-mail et sur le certificat utilisé pour le chiffrement.



Fiche 9

Architecture de l'e-mail, choix interne ou externe et services aux utilisateurs

Sommaire

Les 5 composantes techniques de l'e-mail

Faut-il investir dans un serveur de messagerie interne ou bien confier cela à un prestataire externe, société de services dans l'hébergement ou opérateur Télécom professionnel, souvent appelé FAI (Fournisseur d'Accès à Internet) ou ISP (Internet Service Provider). Ces sociétés fournissent souvent accès à Internet, dépôt de nom domaine, services de messagerie…

Dans le cadre d'un usage privé, ce type de services externes est bien connu (pensons aux messageries individuelles déclarées sur Hotmail, sur Yahoo,…).

Le choix d'une messagerie professionnelle en entreprise est-elle aussi simple ?

Une rapide étude de l'architecture et des services nécessaires permettra d'affiner la réponse.
(Voir figure page ci-contre).

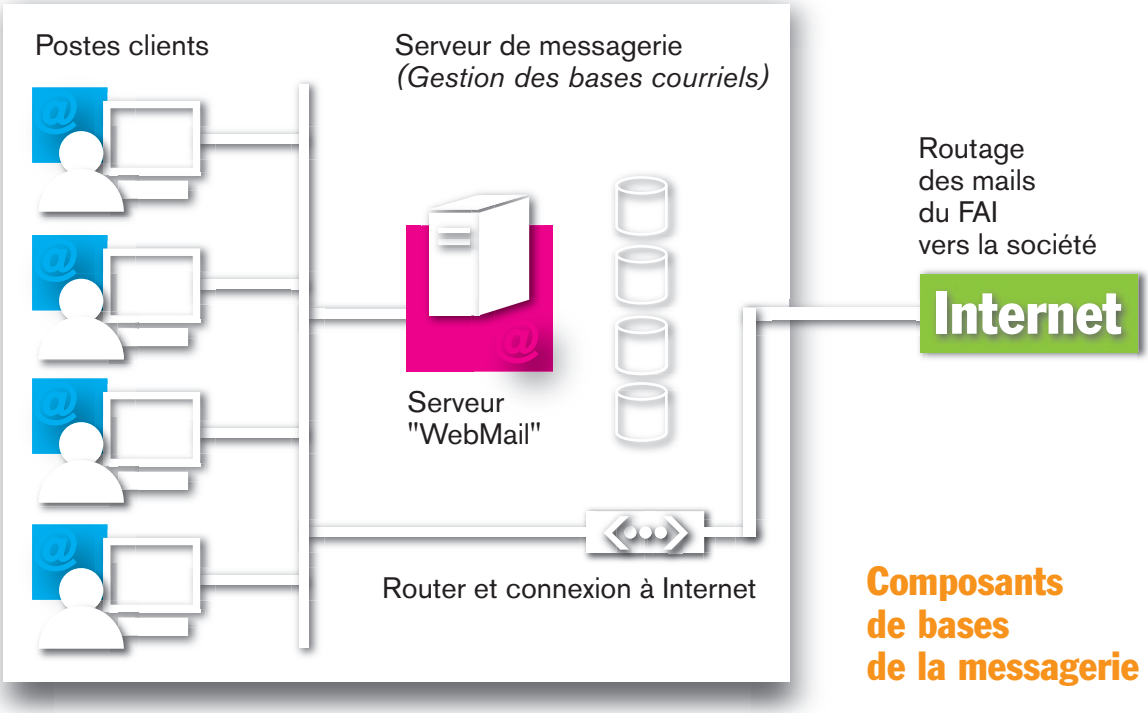
Le service de messagerie interne dans une entreprise se compose de 3 principaux éléments :

- D'un serveur de messagerie permettant de stocker toutes les bases e-mails des utilisateurs et de gérer le « routage » des e-mails vers les destinataires internes ou externes. D'autres fonctions sont aussi proposées par ces serveurs (agenda, actions, …).

- D'un accès « client lourd », c'est-à-dire d'un logiciel sur le PC de chaque utilisateur pour lire, répondre, gérer et classer ses e-mails. Les plus connus de ces logiciels sont bien sûr Microsoft Outlook et Lotus Notes, mais il existe aussi d'autres clients comme Eudora, Pine Mandrake, …

- La capacité de pouvoir recevoir et émettre des e-mails vers l'extérieur de l'entreprise nécessite que le nom de domaine de l'entreprise (@société.fr ou @société.com ou encore @société.eu) soit routé par un opérateur (FAI, ou opérateurs télécoms professionnels), c'est-à-dire dirigé depuis internet vers une porte d'accès de l'entreprise et vice-versa. Cette fonction implique la mise en place

Réseau de l'entreprise



Composants de bases de la messagerie

d'un accès internet, et donc d'un routeur (contrôlant les flux IP) au sein de l'entreprise.

Il faut aussi noter l'apparition du « WebMail ». Le WebMail est rendu possible par l'activation d'un serveur Web au niveau du serveur de messagerie. Ainsi les e-mails sont accessibles depuis un simple navigateur Web (internet Explorer par exemple) à la place d'une application à installer sur le PC (« client lourd » comme Microsoft Outlook, Lotus Notes,…).

En interne dans l'entreprise, le WebMail permet à chacun de se connecter sur n'importe quel poste de travail. Cela peut être utile pour des salariés qui se déplacent dans différents sites de l'entreprise. Chaque PC d'un collègue ou en accès libre leur permet de lire leurs e-mails.
Avec les nouvelles fonctionnalités (Web 2.0, Ajax,…), le « WebMail » propose une ergonomie et des fonctions aussi puissantes que le client lourd.

En externe, avec des éléments de sécurité, cela permet aux salariés itinérants de consulter leurs e-mails à partir de tout PC relié à internet par exemple.

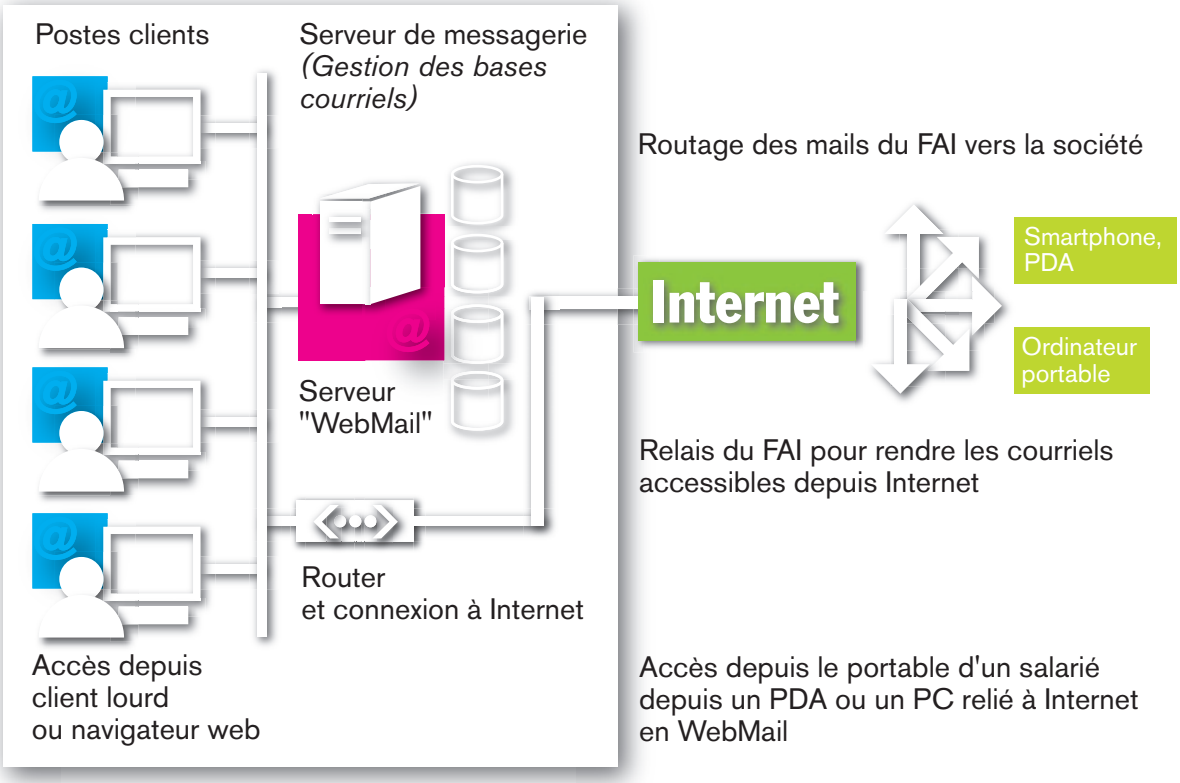
Le bon fonctionnement de ces composants induit deux autres éléments :

- Les coûts d'acquisition des logiciels, des machines (serveur, routeur, etc…) et les coûts de maintenance sur licences et machines (entre 10 à 20 % du prix d'achat en général).
- Les coûts induits par les hommes, absolument nécessaires, à la maintenance et exploitation des composants techniques.

L'entreprise peut aussi se poser les questions suivantes en fonction de ses besoins :

- Comment pouvoir récupérer mes e-mails professionnels facilement depuis mon domicile, en déplacement à l'hôtel, en France ou à l'étranger ?
- Comment profiter des nouvelles fonctions d'e-mails sur les PDA, les Blackberry ou les smartphones et autres terminaux mobiles.

Réseau de l'entreprise



Accès aux E-mails depuis un PC Portable ou PDA à l'extérieur de l'entreprise ou via WebMail

La réponse à ces deux questions nécessite la mise en place d'infrastructures complémentaires dont le coût et la complexité (ainsi que l'enjeu sécuritaire) peuvent varier suivant que la messagerie est interne ou externe (voir figure ci-dessus).

Il peut s'agir :

- d'un serveur de duplication chez un opérateur pour rendre les connexions accessibles depuis internet (PDA, Blackberry) ;
- de la mise en place de réseau VPN depuis l'extérieur avec le réseau de l'entreprise pour générer un flux de connexion pour les PC Portables en déplacement ;
- de l'externalisation complète des serveurs de messagerie (chaque client interne se connecte donc à un serveur à l'extérieur de l'entreprise).

La messagerie hébergée ou externe

En fonction de la taille de l'entreprise, des fonctions utilisées (agenda, annuaire, etc...) et des services souhaités par l'entreprise (accès en déplacement), l'arbitrage entre une messagerie interne ou externe est nuancée.

La location d'un service de messagerie au sein d'un opérateur de type FAI permet de s'affranchir de différentes contraintes et effets sur la trésorerie :

- Achats des serveurs et licences de messagerie pour la solution choisie.
- Gestion des coûts de maintenance et mise à jour régulière des composants applicatifs.
- Surveillance des composants réseau nécessaires au routage et à la sécurité.
- Mise en place d'une cellule informatique en

charge de la maintenance, de l'exploitation, mais aussi du support et soutien aux utilisateurs.

Ces services sont alors transformés en **loyers mensuels** et assurés par l'opérateur choisi, en fonction des différentes options du contrat.

L'intérêt est que la compétence technique (souvent pointue et à ne pas négliger pour la sécurité) n'a pas besoin d'être possédée par l'entreprise, elle est assurée par les experts du prestataire.

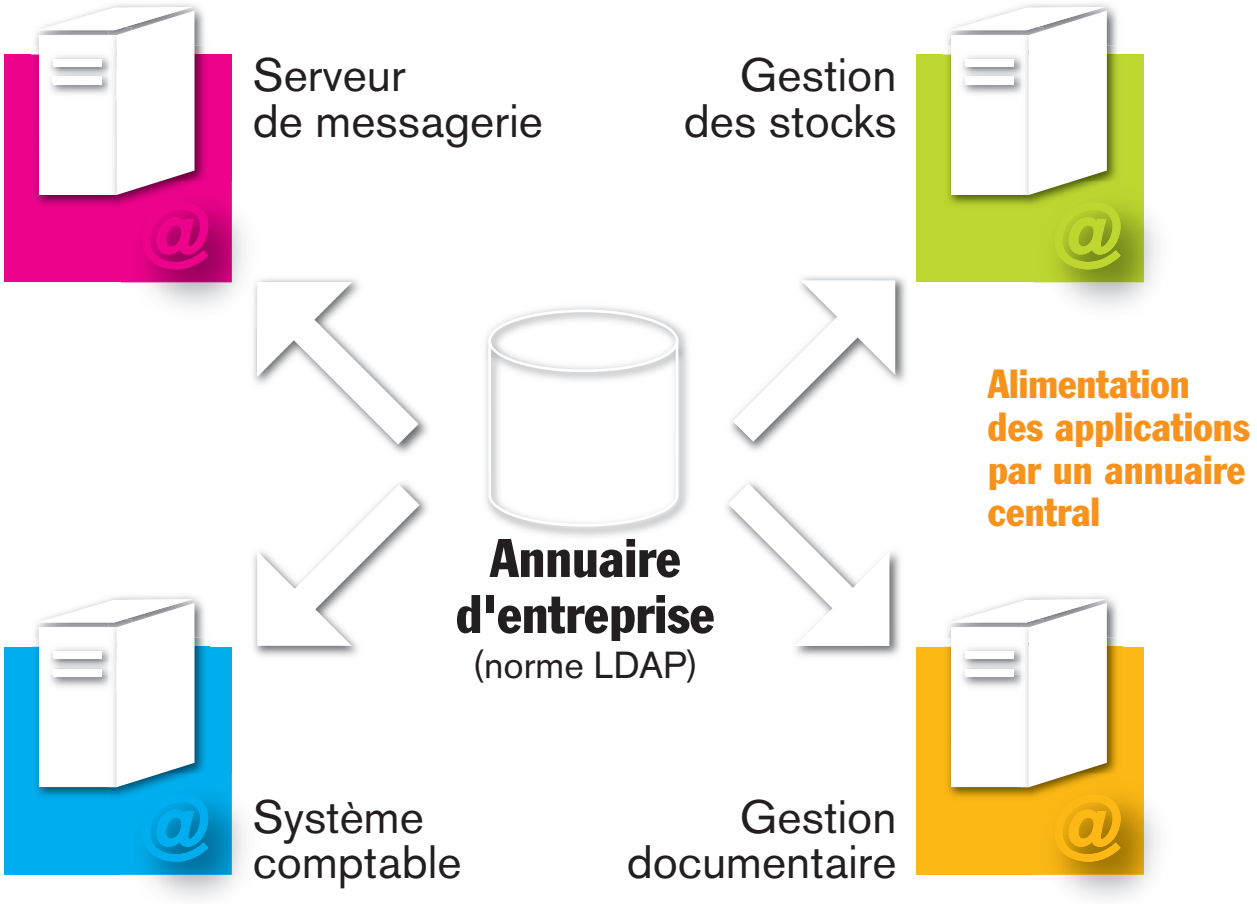
D'autre part, ce type de prestation est très évolutif. Il permet de compléter les services en fonctions des besoins de l'entreprise.

Dans le cadre d'une petite entreprise (20 à 100 personnes), ne disposant pas d'une équipe informatique pointue dans ces domaines, le choix d'une messagerie externe peut être un bon choix en terme de qualité de service pour les utilisateurs. **N'oublions jamais qu'il n'y a rien de pire pour les utilisateurs qu'une interruption ou une mauvaise confiance dans la messagerie.**

Par contre, une entreprise qui utilise le service de messagerie de manière très intégrée avec d'autres applications de l'entreprise (application de GED, Workflow, fonctions avancées des serveurs de messagerie) et qui dispose d'une équipe technique compétente en sécurité, flux réseau et messagerie, pourra investir dans son propre serveur de messagerie interne. Elle mettra également petit à petit en place des services avancées comme l'accès pour les grands voyageurs depuis leur hôtel,…

Le Rôle de l'annuaire

Un serveur de messagerie est une application comme les autres. Elle nécessite donc de déclarer chaque utilisateur dans un « carnet d'adresse » des utilisateurs et de lui affecter une adresse e-mail. Il est parfois également possible, lorsque le serveur de messagerie propose des accès « WebMail » (interface e-mail depuis internet explorer) d'affecter un login et un mot de passe (voir figure ci-dessous). Cet annuaire de messagerie est souvent compatible LDAP, c'est-à-dire qu'il puise les utilisateurs de



messagerie dans un annuaire d'entreprise plus global, ou bien il représente lui-même un annuaire centralisé, permettant d'alimenter les accès à d'autres applications.

En effet, lorsque l'on veut connaître l'ensemble des salariés de l'entreprise, il est parfois opportun de compter le nombre d'adresses d'e-mails de façon exhaustive. L'annuaire de messagerie représente donc parfois un bon annuaire global pour alimenter l'ensemble des applications.

La mise en place d'un annuaire et d'applications respectant la norme LDAP permet alors à chaque application de puiser les identités utilisatrices, et donc de gérer l'authentification, à partir d'un seul annuaire d'entreprise.

Cela évite de déclarer plusieurs fois, et dans plusieurs applications, des mêmes utilisateurs et diminue les problèmes d'erreurs et de cohérence, mais aussi de gestion des mots de passe, …

La mise en place d'un annuaire LDAP pour centraliser les « login/mot de passe » vers différentes applications peut tout à fait être compatible avec un service de messagerie externalisé. Il faudra alors envoyer une extraction régulièrement vers le FAI en charge de la messagerie pour que les annuaires correspondent bien.

En revanche, plus le système d'information global de l'entreprise s'appuie sur des éléments de Workflows, de collaboration, d'e-mails structurés, plus il sera nécessaire de rapatrier la messagerie en interne, pour une meilleure intégration et interfaces entre les différentes applications.

Les attentes vis-à-vis du service informatique

Mettre en place des services évolués pour les utilisateurs provoque forcément une attente forte de qualité de services.

En effet, lorsqu'il est possible de se connecter tard le soir depuis son hôtel, après un dîner client, pour envoyer un rapport, le commercial aura tendance à compter sur cette fonction.

Lorsqu'un technicien avant-vente parti en déplacement précipitamment, pense qu'il pourra toujours se connecter depuis l'hôtel en arrivant pour envoyer un e-mail important impactant la présentation commerciale du lendemain, il aura tendance à compter sur cette capacité d'accès.

Proposer des services évolués de messagerie (ou d'une autre application) aux utilisateurs de votre entreprise, c'est implicitement accepter qu'ils s'organisent autour de ces services et donc qu'ils s'attendent à ce que cela marche tout le temps.

Rien de pire que de découvrir qu'un service de messagerie est défectueux lorsque l'on en a besoin en urgence.

Ce constat a des répercutions profondes sur la mise en place des services de messagerie : il faut absolument définir leur cadre d'utilisation et mettre en place les organisations techniques pour respecter ce cadre.

Cela passe par :

- La mise en place d'un service de maintenance, exploitation et supervision des services de messagerie (serveur de messagerie, système d'accès aux e-mails à distance, accès internet…réseau,…) durant les heures de services annoncés. Cela peut se faire en astreinte à distance, ou bien sur site, par du personnel de l'entreprise ou bien par externalisation de la supervision.

- La mise en place d'un service de formation, et parfois de support Hot-Line pour les utilisateurs critiques, afin qu'ils ne restent pas bloquer par une mauvaise utilisation.

Ces aspects organisationnels peuvent influencer le choix d'un service de messagerie interne ou externe (l'entreprise a-t-elle les moyens et la nécessité d'organiser ces fonctions en internes, ou bien est-ce plus adapté de profiter d'un effet de mutualisation chez un prestataire ?).

Il ne faut pas prendre en compte la seule simulation financière, mais aussi la capacité de l'entreprise à maintenir un niveau de services, une disponibilité élevée des services de messagerie. Si la société n'en est pas capable, quelques milliers d'euros gagnés dans l'analyse financière lors du choix ne compenseront jamais la perte de productivité, la perte de confiance dans le système à des moments critiques.

Il est important d'évaluer avec votre responsable informatique un scénario financier entre messagerie interne et externe, mais aussi d'évaluer la capacité de l'entreprise à fournir des services de qualité. Et cela ne repose pas sur un seul homme. Le rôle de votre responsable informatique n'est pas de savoir ou ne pas savoir administrer, mais surtout de bien anticiper les besoins de vos utilisateurs et proposer la meilleure organisation pour que ces services soient fiables.

Le marché de l'e-mail

Le marché de l'e-mail : solution éditeur ou solution « libre ». Quelques grandes solutions de base pour pouvoir discuter avec son prestataire :

- serveur d'e-mail : exchange, domino, sendmail, qmail ;
- client de messagerie : outlook, outlook express, evolution, lotus;
- le web mail : squiremail.

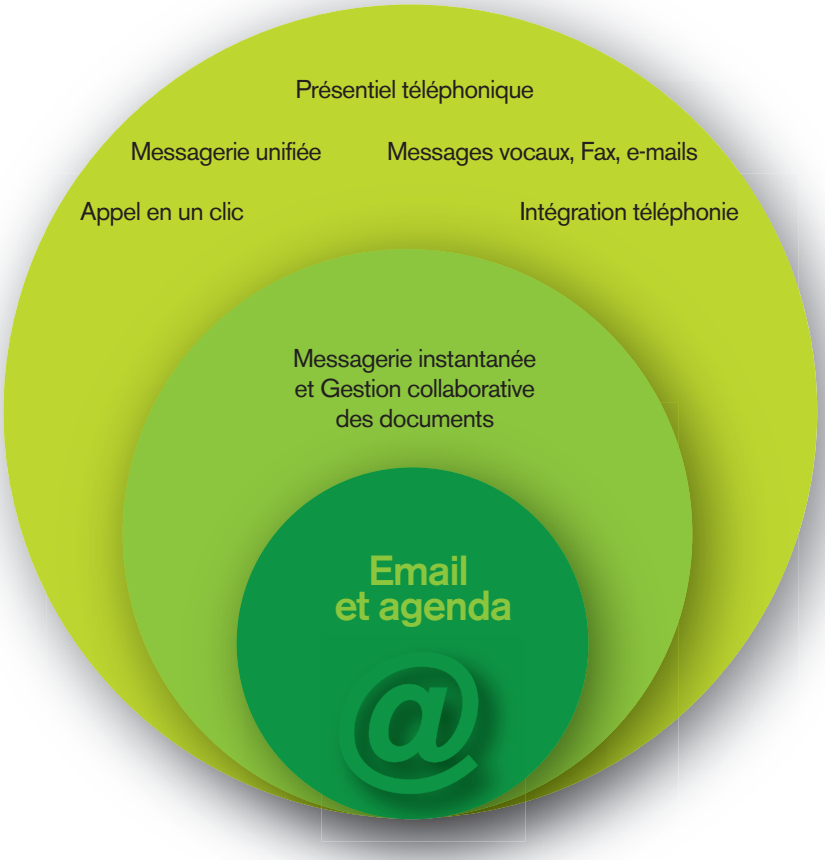
Le marché de l'e-mail est un marché qui a atteint sa maturité. Il est à ce jour fortement dominé par deux acteurs, IBM Lotus et Microsoft qui s'octroient près de 90% du revenu Mondial des logiciels d'e-mail. Cependant de nouveaux acteurs comme Google, Open Xchange, Scalix ou Zimbra, apparaissent. Ils sont issus de l'Open Source ou proposent un modèle hébergé.

Une évolution importante concerne le client de messagerie :

- le client léger accessible à travers le browser évolue progressivement vers le Web 2.0, proposant ainsi une interface plus riche et plus intuitive pour les utilisateurs ;
- le client lourd installé physiquement sur le poste de l'utilisateur évolue progressivement vers les Applications Internet Riches permettant ainsi une plus forte intégration avec d'autres composants du poste de travail

Cependant l'e-mail apparaît de plus en plus comme un élément d'un ensemble plus global visant à faciliter la communication et la collaboration en entreprise. N'utiliser qu'un système d'e-mail, c'est souvent ne pas se donner les moyens de mettre en œuvre les «bonnes pratiques» (voir figure ci-dessous).

De l'e-mail à un système complet de communication et de collaboration



Fiche 10

Les smileys

Sommaire

Qu'est-ce qu'un smiley ?

Un smiley est un code utilisé entre correspondants, représentant un petit visage créé à l'aide de caractères de ponctuation exprimant l'humeur de l'émetteur d'un message.

Exemples : :-) (content)

Les smileys sont là pour représenter son humeur du moment quand, lorsqu'on est devant l'ordinateur on ne voit pas la personne avec laquelle on parle, et on souhaite lui faire participer de ses humeurs. Exemple, la blague était drôle, je me marre, ou je suis déprimé(e), etc.

Les smileys sont donc une suite de caractères qui sont censés représenter ou illustrer l'humeur du moment. Comme la discussion sur Internet ne permet pas forcément d'envoyer des images, on envoie ce petit être qui, regardé de travers représente une figure.
Comment voir le smileys ? Vous tournez votre écran de 90° dans le sens des aiguilles d'une montre pour observer le symbole dans le bon sens, ou vous inclinez votre tête de 90° vers la gauche pour pouvoir l'observer.

Comment réaliser un smiley ?

Il faut tout faire en mode ASCII, c'est à dire que les caractères de votre clavier doivent représenter quelque chose.
On représente ces petits personnages à l'aide des caractères machine à écrire, souvent la police "Courrier New".
Ensuite c'est à vous de laisser votre imagination travailler pour rendre votre smiley communicatif, un smiley a une base, celle-ci : :-) et on la change comme on le souhaite.

Quelques exemples de smileys de base

Voici les smileys de base, les plus courants, universellement connus sur le Net :

:-)
Content
Le smiley de base, le souriant, utilisé pour indiquer un passage sarcastique ou humoristique, puisqu'on n'entend pas les inflexions de la voix sur le réseau. Si vous ne comprenez pas, penchez la tête sur le côté gauche...

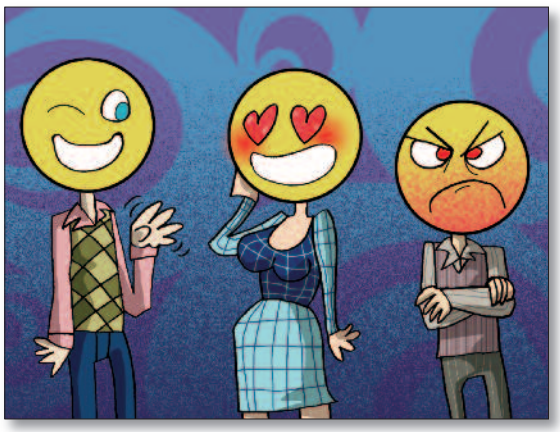
;-)
Le clin d'oeil, pour les remarques au second degré

:-(
Un smiley renfrogné. Pas content

:-I
Smiley indifférent.

:-O
Etonnement (bouché bée)

lol
Fort étonnement ou désespérance (on lève les bras au ciel)



Glossaire

Les principaux termes

Anti-virus
Logiciel destiné à rechercher et d'éliminer les virus informatiques et autres programmes conçus pour endommager ou entraver le fonctionnement normal d'un système.

Authentification
Processus visant à vérifier la correspondance entre un identifiant et une personne associée (exemples : le mot de passe, carte à puce avec code PIN,…)

Botnet
Réseau virtuel de postes de travail infectés et de ce fait devenus contrôlables à distance par un pirate.

Chiffrement
Mécanisme de sécurité permettant d'assurer la confidentialité des données.

Clé
Élément de codage sur lequel repose un secret, permettant de chiffrer et de déchiffrer un message. Il existe des clés secrètes et des clés publiques.

Courrier électronique
Mel, courriel, mail, e-mail (article 1.4 de la LCEN)

Déni de service
Attaque ayant pour but de bloquer le fonctionnement de machines ou de services, par saturation d'une ressource.

Faille de sécurité
Défaut dans un programme, pouvant de ce fait être exploité par un virus pour infecter un ordinateur.

Internet
Réseau mondial permettant l'interconnexion des ordinateurs, quels que soient le type de machine, leur système d'exploitation et le support de transport physique utilisé.

Intrusion
Pénétration non autorisée d'un système ou d'un réseau, ayant pour but la compromission de l'intégrité, la confidentialité ou la disponibilité d'une ressource.

LAN
Réseau local interconnectant des équipements informatiques (ordinateurs, serveurs, terminaux ...) dans un domaine géographique privé et limité.

Log
[ou historique d'évènements]
Fichier texte tenu à jour par un serveur, dans lequel il note les paramètres liés à chaque connexion.

PDA (Personal Data Assistant)
Assistant numérique de poche (contacts, calendrier). Pour traiter les e-mails, celui-ci doit être communicant avec un réseau (téléphonie cellulaire, Wifi, …).

Phishing
Technique d'escroquerie consistant en l'envoi de messages apparemment authentiques, issu d'une institution financière ou d'un site commercial connu [par usurpation d'interface].

Pirate (Cracker/Hacker) :
Terme générique désignant celui qui « craque » ou attente à l'intégrité d'un système informatique.

Proxy
Technique logicielle utilisée sur Internet pour partitionner une communication entre un client et un serveur.

SLA
(Service level agreements / engagements de niveaux de services)
Engagements de la part du fournisseur sur la qualité du service fourni, en particulier sur le niveau d'indemnisation éventuelle du client.

Signature électronique
Technique permettant d'assurer l'authentification du signataire et éventuellement celle d'un document signé par lui.

Smiley
ou « émoticon » (en français, on préférera parfois dire « émoticône »), aussi appelés « smiley », « smilies » au pluriel. Code utilisé entre correspondants, représentant un petit visage créé à l'aide de caractères de ponctuation exprimant l'humeur de l'émetteur d'un message.
Les règles pour la rédaction (la création) de smilies sont très libres, et il existe beaucoup de « petits bonshommes qui rigolent » tout à fait personnels... le principe de base étant de chercher à représenter un visage avec une poignée de caractères courants :-) (content)

Spam
Message non sollicité, envoyé massivement et souvent de manière répétée, à vocation le plus souvent commerciale.

Tiers de certification
Organisme chargé de gérer et de délivrer les clés publiques avec la garantie qu'elles appartiennent bien à leurs possesseurs reconnus.

Tiers de confiance
Organisme chargé de maintenir et de gérer, dans le respect des droits des utilisateurs, les clés de chiffrement ou d'authentification. Les tiers de confiance peuvent être des tiers de certification ou des tiers de séquestre.

Virus
Programme non sollicité qui se répand à travers les ordinateurs pour affecter leur fonctionnement, voire les endommager.

Vulnérabilité
faiblesse d'une ressource d'information qui peut être exploitée par une ou plusieurs menaces.

Zombie
Nom communément donné à une machine infectée, contrôlable à distance, et de fait pouvant faire partie d'un Botnet.

Quelques sites utiles

Sites gouvernementaux

- **http://www.ssi.gouv.fr/fr/dcssi/** la Direction Centrale de la Sécurité des Systèmes d'Information, site thématique institutionnel du Secrétariat Général de la Défense Nationale (SGDN).
- **http://www.service-public.gouv.fr** le portail de l'administration française
- **http://www.legifrance.gouv.fr** l'essentiel du droit français
- **http://www.telecom.gouv.fr** le site de la direction ministérielle chargée des télécommunications
- **http://www.interieur.gouv.fr/sections/contact/police/questions-cybercriminalite** l'Office central de lutte contre la cybercriminalité liée aux technologies de l'information et de la communication

Organismes publics ou privés

- **http://www.cnil.fr** la Commission nationale de l'informatique et des libertés
- **http://www.clusif.asso.fr** le club de la sécurité des systèmes d'information français
- **http://www.ossir.org** l'Observatoire de la sécurité des systèmes d'information et des réseaux
- **http://www.afnor.fr** l'Association Française pour la Normalisation
- **http://www.cigref.fr** le Club informatique des Grandes Entreprises Françaises
- **http://www.adit.fr** l'Association pour la Diffusion de l'Informatique Technique
- **http://www.medef.fr** le site du MEDEF où se trouvera ce guide.
- **http://www.foruminternet.org/** espace d'information et de débat sur le droit de l'internet et des réseaux
- **http://www.forumatena.org** un lieu d'échanges entre l'enseignement supérieur et l'industrie dans le domaine des technologies de l'information et des télécommunications.

Remerciements

Ce guide a été rédigé par le groupe de travail « Méthodologie des TIC » du MEDEF, présidé par Daniel Thébault, président d'Aliacom, président du MEDEF Midi-Pyrénées et membre du Conseil Exécutif du MEDEF.
Le rapporteur du groupe de travail est Catherine Gabay, directrice Innovation – Recherche - Nouvelles Technologies du MEDEF.
Ce groupe de travail fait partie du Comité Economie Electronique du MEDEF, présidé par Philippe Lemoine, président de LASER. Ce Comité fait lui-même partie de la Commission Recherche -– Innovation – Nouvelles Technologies du MEDEF, présidée par Charles Beigbeder, président de POWEO.
Le MEDEF tient à remercier grandement les participants pour leur contribution sans laquelle la rédaction de ce guide n'aurait été possible.

AGOSTI Pascal	Caprioli et Associés
BARBEY Vincent	Ocentis
BARBRY Eric	Alain Bensoussan Avocats
BRUCKMANN Francis	France Télécom - Orange
CALEFF Olivier	Devoteam Consulting
COLIN Pascal	Keynectis
CORNIOU Jean-Pierre	EDS
DANAN Alain	Symantec
GABAY Catherine	MEDEF
GUILLAUME Nicolas	Microsoft
HAYEM Laurent	IBM
JEANDEL Patricia	MEDEF Nord Franche Comté
LE HEGARAT Yann	Consultant indépendant SELF+
LE PORT Anne	Nextiraone
LE ROY Thierry	Connect To Me
LOUVET Benoit	Lamy et Associés
MESSAGER François	Nextiraone
NOEL Marc	Parkerwilliborg
PAILLARD Julie	RIM
PELIKS Gérard	EADS
QUEMARD Jean-Pierre	EADS
RIETSCH Jean-Marc	FEDISA
ROUMEFORT (de) Amélie	
SANSON Thierry	Nextiraone
SENACQ Stéphane	Microsoft
THEBAULT Daniel	Medef Midi-Pyrénées