Obligations Légales et Tableau de Bord pour l'activité virale

Direction Informatique & Télécommunications
Division Pilotage Sécurité Qualité

Julien VEHENT – Mai/Août 2006
Master Management de la Sécurité des Systèmes Industriels
et des Systèmes d'Information – 1ére année

Je tiens à adresser mes sincères remerciements à Monique BUREAU
pour m'avoir accueilli dans son équipe.

Je tiens également à remercier Christophe MOREAU, Marcel POUPIN et
Jérôme BROSSARD pour leurs aides et conseils tout au long de ce stage

RÉSUMÉ

L'une des principales missions du Responsable de la Sécurité du Système d'Information (RSSI) est de s'assurer que le système d'information de son entreprise répond aux exigences légales posées par les lois « *Informatique et Libertés* » et « *Confiance dans l'Économie Numérique* ». Ces exigences sont nombreuses et il est rare qu'elles soient au coeur des préoccupations des chef de projets. L'un des rôles de Monique BUREAU, RSSI du groupe MAAF, et de son équipe est donc d'accompagner les projets afin qu'ils respectent les lois précédemment citées, mais également d'effectuer l'interface, de manière plus générale, entre la Commission Nationale Informatique et Libertés (CNIL) et le système d'information du groupe MAAF.
Je m'attache, dans la première partie de ce rapport, à décrire plus amplement ces problématiques et leurs résolutions en particulier au travers de la mise en place de la fonction de « *Correspondant Informatique et Libertés* » (CIL) au sein du Groupe MAAF.

En 1999, MAAF Assurances s'est engagé, au travers du projet d'entreprise « Challenger Attitude/Cap99 », à « *être la référence du marché en offrant le meilleur rapport qualité/prix* » d'ici 2010. Au travers de la certification ISO-9001, la Direction Informatique et Télécommunications (DIT) s'inscrit pleinement dans cette démarche et c'est via la mise en place d'un tableau de bord pour l'activité virale que j'y ai contribué. L'ensemble de ce projet, de l'intégration de la démarche qualité à la livraison d'une solution fonctionnelle compatible avec la norme ISO-27001 (*à peine sortie*), est détaillée dans la seconde partie de ce rapport.

ABSTRACT

One of the most important task of the Information Security Manager is to make sure that the Information System of its company fulfills the legal requirements posed by the laws « Informatique et Libertés » and « Confiance dans l'Économie Numérique ». Those requirements are numerous and seldom considered by projects managers. A Monique BUREAU mission, Information Security Manager of MAAF group, and of her team is to accompany projects to ensure they fulfills the laws. Moreover, She's doing the interface between MAAF group and the « Commission Nationale Informatique et Libertés », in charge of the law application.
In the first part of this report, I describe this problems and their solutions, in particular through the creation of the function « Correspondant Informatique et Libertés ».

Since 1999, MAAF Assurances is engaged to become the reference of the French market in providing the best quality/price ratio. Through ISO-9001 certification, the Telecom and Computer Direction seek to achieve this goal. I've brought my participation to this challenge by the deploiement of a dashboard for virus activity. This project, since quality certification requirements until the delivery of a complete solution (compatible with the new ISO-27001 standard), is presented in the second part of this report.

Sommaire

Introduction

Veiller à la sécurité d'un système d'information est une tâche aussi vaste que complexe. Les problématiques sont nombreuses et, dans un système d'information comme celui de MAAF Assurances, demandent la considération d'un nombre important de paramètres.
Maintenir la sécurité des informations du Groupe MAAF est une démarche qui commence dès les premières spécifications des projets, et s'arrête uniquement lorsque les applications mises en oeuvre sont en fin de vie et retirées du système. Dans ce rapport, je vais présenter le travail que j'ai effectué sur deux des champs de compétences de l'équipe Sécurité des Systèmes d'Informations au sein de la Direction Informatique et Télécommunication.

Le premier d'entre eux concerne le respect de la réglementation Informatique et Libertés. Les différents aspects de la loi de 1978 modifiée en 2004 seront présentés dans une première partie. Je m'attacherai particulièrement, dans un premier temps, à décrire une partie des obligations qui pèsent sur le système d'information de MAAF Assurances. Le processus de déclaration de ces traitements sera présenté dans un deuxième temps en prenant pour exemple le système MAAF Santé.
La participation à la mise en place de la fonction de Correspondant Informatique et Libertés, nouveauté introduite par la nouvelle loi Informatique et Libertés, au sein du groupe MAAF fait également partie des tâches qui m'ont été confiées au cours de ce stage et dont je parlerais en troisième point.
Enfin, le quatrième et dernier point de ce chapitre concerne la préparation d'une formation ayant pour objectif la sensibilisation des employés MAAF à la loi Informatique et Libertés.

La seconde tâche que j'ai traitée au cours de ces quatorze semaines de stage est la mise en place d'un tableau de bord pour l'activité virale au sein du réseau informatique du Groupe MAAF. La présentation complète du projet est décrite dans le second chapitre. J'y présente les problématiques, non seulement en termes de sécurité, mais également en terme de qualité, puisque la Direction Informatique et Télécommunication est certifiée ISO-9001 depuis l'année 2002.
Afin de mener à bien cette mission, j'ai réalisé un travail de synthèse concernant l'activité virale qui m'a permis de comprendre les objectifs des indicateurs existants. J'ai ensuite réalisé un travail technique d'étude du logiciel en place.
Au terme de cette étude, il a été décidé de créer un nouveau système, dont nous avons défini les spécifications et que j'ai ensuite développé. Ce logiciel apporte une solution complètement nouvelle, répondant plus précisément aux besoins de l'équipe Sécurité des Systèmes d'Information. Ce projet, nommé TBvirus, permet à l'équipe Sécurité de produire automatiquement des indicateurs de l'activité virale pour une période déterminée allant jusqu'à J -1. Il est présenté dans la dernière partie de ce rapport.

Le groupe MAAF

Un peu d'histoire...

La Mutualité trouve son origine dans les sociétés de secours mutuel qui se développent au 19ème siècle. Mais c'est en 1902, avec la naissance de la Fédération Nationale de la Mutualité Française (FNMF) qu'elle se structure véritablement. Après 1945 et la création de la Sécurité sociale, la Mutualité se réoriente vers l'action sociale et notamment vers les besoins de couverture complémentaire des régimes obligatoires (Mutuelles 45).

Le 30 mai 1950, la Mutuelle d'Assurance Automobile Artisanale de France (ou MAAAF) est créée avec l'appui de la Chambre de métiers des Deux Sèvres. Les artisans fondateurs décident, par économie, de s'assurer mutuellement. La MAAAF débute son activité le 3 décembre 1951 dans les locaux d'une ancienne charcuterie située 83, rue de la Gare, à Niort.

Grâce au relais des Chambres de métiers, le développement de la MAAAF est rapide. A la fin de l'année 1952, la MAAAF a enregistré 7 000 adhésions et compte déjà 17 salariés. En 1960, la MAAAF compte déjà 100.000 sociétaires. A la demande des artisans, elle propose depuis 1957 une assurance Incendie et depuis 1959 une garantie Responsabilité Civile familiale et professionnelle. Dès lors en 1961, la MAAAF perd le " A " d'Automobile pour devenir la MAAF : Mutuelle d'Assurance Artisanale de France.

Les années 60 et 70 sont marquées par une forte croissance. Dans les années 60, la création d'un réseau commun avec la MACIF permet à la MAAF de couvrir tout l'hexagone. En 1972, la MAAF inaugure son nouveau siège social à Chauray, près de Niort. En 1976, suite à la rupture avec la MACIF, la MAAF étend son offre au grand public pour nourrir le réseau développé sur tout le territoire. Cette ouverture au grand public est officialisée, à la fin des années 70, par l'élargissement de ses statuts. Lors de l'assemblée générale de 1980, la MAAF fête son millionième sociétaire.

Dans la seconde partie des années 80, la MAAF continue de diversifier ses activités. Si certaines diversifications sont un succès (assistance, assurance vie, protection juridique etc), d'autres l'amènent à vivre la plus grande crise de son histoire. Les causes de cette crise sont à la fois externes - la concurrence est de plus en plus vive - et internes - erreurs de gestion, échec de la diversification bancaire, luttes intestines. A l'heure de fêter ses 40 ans d'existence, la MAAF est au bord de la faillite.

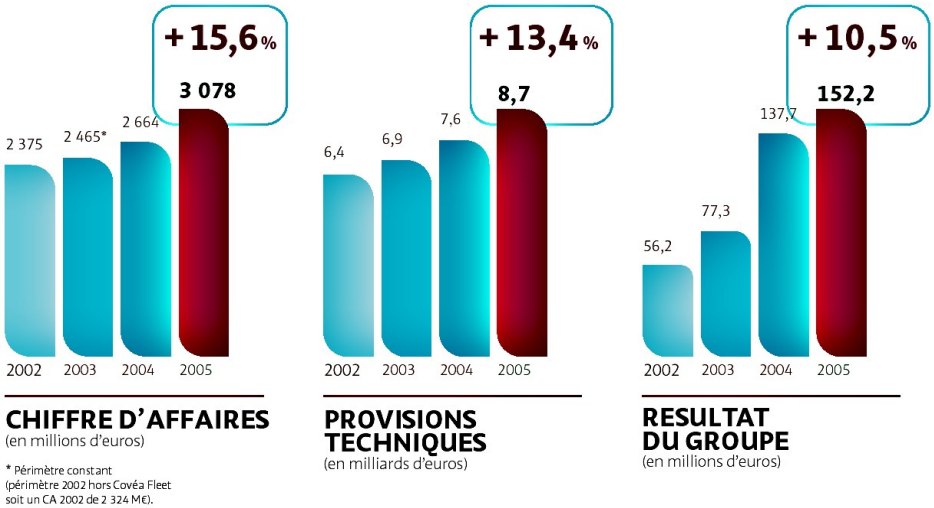
En 1990, l'arrivée de Jean-Claude Seys à la tête de la mutuelle marque la fin des errements par la mise en place d'un nouveau conseil d'administration, d'une nouvelle équipe de direction et d'une charte de progrès.

Le changement de siècle s'accompagne d'un renforcement de la concurrence. MAAF Assurances y répond par la création de produits et services et par la diversification de ses métiers et de ses canaux de distribution. Par ailleurs, la création de Covéa, avec MMA, et l'ouverture à l'Europe à travers l'alliance Eureko permettent d'explorer de nouvelles pistes en autorisant un partage d'expériences, de moyens et de coûts.

A ce jour, le groupe MAAF est composé des sociétés suivantes :

- MAAF Assurances
- MAAF Assurances S.A.
- Assurances Banque Populaire IARD
- NEXX Assurances
- NOVEA Assurances
- MAAF SANTE
- FORCE ET SANTE
- MAAF VIE
- et l'ensemble des Groupements d'Intérêt Economiques (GIE) dont les GIE EURODEM et EUROPEX en charge des moyens informatiques.

Il compte 3,5 millions de sociétaires et clients pour un chiffre d'affaires combiné d'environ 3,1 milliards d'euros. Ces résultats font de MAAF, au niveau national, le 5ème assureur automobile, le 8ème assureur Incendies, Accidents et Risques Divers (IARD) et la 1ére mutuelle des professionnels. MAAF c'est également plus de 6 600 salariés répartis entre le siège social de Chauray, les sociétés diverses et les 573 agences.

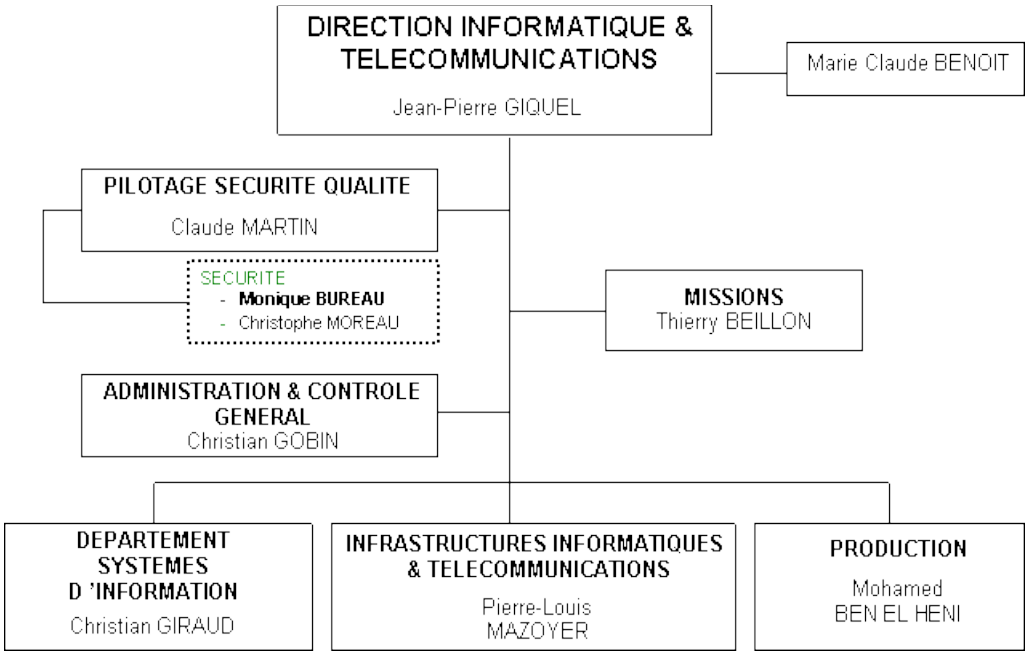


Chiffres 2005 pour le groupe MAAF

La Direction Informatique et Télécommunications (DIT)

La Direction Informatique et Télécommunications regroupe deux GIE (GIE EUROPEX et GIE EURODEM), est au service de la stratégie du Groupe mutuel MAAF Assurances. Elle doit assurer la maintenance et l'évolution du système d'information du réseau MAAF et être source de proposition s'appuyant sur les évolutions techniques. De plus, la DIT doit effectuer la convergence avec les MMA (Mutuelles du Mans Assurances) et GMF-Azur.
La DIT se compose de 364 salariés et d'environ 235 prestataires.

Organigramme de la DIT :



Les missions de la division PILOTAGE SECURITE QUALITE (11 salariés):

- Élaborer, suivre et faire le plan de développement en participation avec les métiers de la DIT et les MOA,
- Contrôler l'allocation des ressources aux différents projets,
- Veiller au respect des engagements de la DIT,
- Assister les Maîtrises d'Ouvrage (MOA) dans l'expression de leurs demandes,
- Assister les différentes entités de la DIT dans la prise en charge et la conduite des projets,
- Contribuer à une meilleure adéquation entre les besoins de l'entreprise et les réalisations de la DIT,
- Veiller à la Sécurité du Système d'Information.

Informatique et Libertés à MAAF Assurances

La loi « Informatique et Libertés » du 06 Janvier 1978 instaure des droits pour les personnes qui figurent dans des fichiers de données à caractère personnel, des obligations pour ceux qui les créent et une autorité de contrôle indépendante : la « Commission Nationale Informatique et Libertés ».

MAAF Assurances doit, dans un souci de respect de la législation, se conformer aux obligations suivantes :

- L'obligation de déclarer ou de demander une autorisation à la C.N.I.L. avant toute constitution de fichiers nominatifs ;
- L'obligation d'informations vis-à-vis des personnes sur lesquelles une information a été collectée ;
- Le droit d'accès, d'opposition et de rectification au profit des personnes sur lesquelles il est détenu des informations ;
- L'obligation de sécurité sur les informations détenues, qui s'étend à la fiabilité des logiciels et des matériels ;
- L'interdiction de gérer des données relatives à la race, la religion, l'apparence syndicale, les opinions politiques et philosophiques et les mœurs de personnes physiques ;
- Le contrôle et la durée de conservation des informations nominatives.

L'équipe Sécurité des Systèmes d'Information a la charge de ces missions (en coordination avec le département juridique). En tant que stagiaire dans ce service, j'ai effectué un certain nombre de tâches en rapport avec la loi Informatique et Libertés. De la veille réglementaire à la mise en place du Correspondant Informatique et Libertés en passant par les déclarations de traitements sensibles, les pages suivantes présentent une synthèse du travail que j'ai effectué.

I.1 La Commission Nationale Informatique et Libertés (CNIL)

Genèse

La révélation, dans les années 70, d'un projet du gouvernement d'identifier chaque citoyen par un numéro et d'interconnecter sur la base de cet identifiant tous les fichiers de l'administration créa une vive

émotion dans l'opinion publique.

Ce projet, connu sous le nom de SAFARI, qui montrait les dangers de certaines utilisations de l'informatique et qui faisait craindre un fichage général de la population, a conduit le gouvernement à instituer une commission afin qu'elle propose des mesures tendant à garantir que le développement de l'informatique se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques.
Cette “Commission Informatique et Libertés” proposa de créer une autorité indépendante. C’est ce que fit la loi du 6 janvier 1978.

La CNIL est chargée d’appliquer la loi du 6 janvier 1978, modifiée par la loi du 6 août 2004, relative à l’informatique, aux fichiers et aux libertés. La mission générale de la CNIL est de veiller à ce que l’informatique soit au service du citoyen et qu’elle ne porte atteinte ni à l’identité humaine, ni aux droits de l’homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Une autorité administrative indépendante

La CNIL élit son Président parmi ses membres ; elle ne reçoit d’instruction d’aucune autorité ; les ministres, autorités publiques, dirigeants d’entreprises, publiques ou privées, ne peuvent s’opposer à l’action de la CNIL pour quelque motif que ce soit et doivent prendre toutes mesures utiles afin de faciliter sa tâche.

- Le Président de la CNIL recrute librement ses collaborateurs.
- Le budget de la CNIL est imputé sur le budget de l’État.
- Les agents de la CNIL sont des agents contractuels de l’État.
- Les décisions de la CNIL peuvent faire l’objet de recours devant la juridiction administrative.

La CNIL en 2005

- ❑ 96 contrôles;
- ❑ 10 avertissements; concernant le secteur bancaire et du crédit
- ❑ 5 normes simplifiées;
- ❑ 36 mises en demeure;
- ❑ 80 677 nouveaux traitements de données nominatives enregistrés.

Les données à caractère personnel

Est considérée comme une donnée à caractère personnel toute information relative à une personne physique identifiée ou susceptible de l’être, directement ou indirectement par référence à un numéro d’identification (ex : n° de sécurité sociale) ou un ou plusieurs éléments qui lui sont propres (ex : initiales du nom et du prénom, avec recoupement d’informations de type : date de naissance, commune de résidence, éléments biométriques...).
La difficulté est qu'il faut considérer l’ensemble des moyens d’identification dont dispose le responsable du traitement ou tout autre personne, pour déterminer si une personne est identifiable. Il peut s’agir aussi d’informations qui ne sont pas associées au nom d’une personne mais qui permettent aisément de l’identifier. Par exemple « l*e titulaire du numéro de ligne 01 53 73 22 00 téléphone souvent au Sénégal »* ou encore « *le propriétaire du véhicule 3636AB75 est abonné à telle revue »*.

Le principe est, au final, très simple : il est interdit de traiter des informations concernant les moeurs et la vie privée de personnes **identifiables**.

I.2 2004 : modification de la loi « Informatique et Libertés » (I&L)

L'année 2004 est l'occasion pour la CNIL de refondre la loi I&L datant de 1978. Ce travail de modification et d'adaptation de la protection des données aux nouvelles technologies introduit un grand nombre de changements dans le fonctionnement de la CNIL et dans la façon dont MAAF Assurances prend en compte la loi I&L.

Sanctions

Cette refonte de la loi I&L offre de nouveaux pouvoirs à la commission et lui permet désormais de prononcer des sanctions allant de l'avertissement à l'injonction de cesser le traitement, en passant par les sanctions pécuniaires et de mise en demeure. La loi dote ainsi la CNIL d'une autorité qui lui manquait jusqu'alors et nomme cette autorité « formation restreinte », véritable *conseil des sages* ayant pour mission de prononcer les sanctions précédemment citées. La formation restreinte est composée de 6 membres sélectionnés parmi les 17 commissaires qui composent la CNIL.

Autorisation de la CNIL

Seconde modification majeure : les traitements soumis à autorisation de la commission. Ce champ est élargi pour inclure des traitements non prévus dans l'ancienne version de la loi. Cette évolution de la loi a des conséquences importantes pour MAAF Assurances. En effet, les traitements :

- Comportant des données sensibles (ex : données du système Complémentaire Santé);
- Susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat (ex : rapport sinistre/cotisation);
- Ayant pour objet l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes;
- Relatifs aux infractions, condamnations et mesures de sûreté;

sont désormais soumis à autorisation de la CNIL. MAAF Assurances s'est d'ailleurs vu refuser un projet par la CNIL car ce dernier permettait, même si ce n'était pas son objectif premier, d'une part de localiser en permanence un assuré et d'autre part de connaître les infractions que ce même assuré était susceptible de commettre.

Ce projet avait pour objectif d'offrir une nouvelle offre d'assurance automobile à de jeunes conducteurs, leur permettant notamment de réduire leur prime d'assurance automobile, s'ils respectaient un certain nombre d'engagements (respect des vitesses autorisées, des durées de conduites, etc...). Pour cela, ils devaient accepter l'installation sur leurs véhicules d'un boîtier télématique qui permettaient de les géo-localiser en permanence et de capter un certain nombre d'informations nécessaires au traitement.

La CNIL a jugé, je cite, que « *l'enregistrement de l'intégralité des déplacements effectués par les assurés ne répond pas à l'exigence de proportionnalité posée par la loi et portait une atteinte excessive à la liberté d'aller et venir anonymement* ». Elle a également basé sa décision sur l'interdiction pour des personnes privées de mettre en oeuvre un traitement concernant les infractions.

Le Correspondant Informatique et Libertés

Enfin, le dernier apport majeur de la loi de 2004 est la possibilité offerte aux entreprises de mettre en place la fonction de Correspondant Informatique et Libertés (CIL). Le CIL est avant tout un conseiller dont la fonction principale est d'assister le responsable d'un traitement afin que ce dernier soit en accord avec les termes de la loi. De fait, le CIL doit posséder des qualifications adaptées à la taille et l'activité de l'organisme dans lequel il exerce sa fonction. Toutefois, aucun agrément n'est prévu par la CNIL mais elle conseille que ces compétences et qualifications portent tant sur la législation I&L que sur l'informatique et les nouvelles technologies, sans oublier le domaine d'activité propre du responsable des traitements.

L'avantage pour un groupe comme MAAF de se doter d'un CIL est que cette fonction exonère l'entreprise des déclarations systématiques de nouveaux traitements auprès de la CNIL. Par contre, une liste précise de ces traitements doit être tenue à jour par le CIL et doit être tenue à disposition éventuelle de la CNIL ou de toute personne en faisant la demande.

Évidemment, le CIL n'exonère pas l'entreprise de ses responsabilité en termes de conformité à la réglementation et des formalités liées aux demandes d'autorisation.

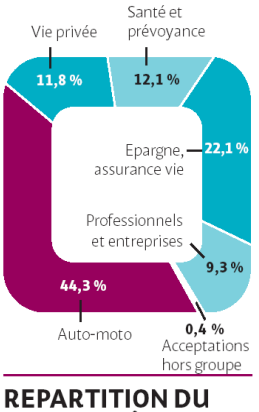
I.3 Le processus déclaratif

La déclaration à la CNIL d'un nouveau traitement de données à caractère personnel peut être un travail complexe qui demande du temps et un grand nombre d'informations. En effet, si pour un traitement simple comme un fichier clients ou un logiciel de gestion comptable, la CNIL prévoit des déclarations simplifiées par Internet, pour des systèmes plus importants il faut recourir à la déclaration normale quasiment systématiquement. Hors, les deux feuillets du formulaire de déclaration normale sont souvent la face cachée d'un iceberg bien plus important.

Les pages suivantes présentent le travail que j'ai effectué sur l'une de ces déclarations, en l'occurrence concernant le système Santé de MAAF Assurances.

MAAF Santé et questionnaire CNIL

Parmi les prestations proposées par le groupe MAAF, l'assurance complémentaire santé joue un rôle de premier plan. Ces prestations sont gérés par MAAF Santé et représente, pour l'année 2005, plus de 883 000 bénéficiaires, 303 millions d'euros de chiffre d'affaires (soit un peu plus de 12% du chiffre d'affaires du groupe) et plus de 7 millions d'euros de résultat.



Chiffres 2005 pour le groupe MAAF

Hors, l'article 8 de la loi I&L énonce clairement que :

*« **Il est interdit de collecter ou de traiter des données à caractère personnel** qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les*

opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou ***qui sont relatives à la santé*** *ou à la vie sexuelle de celles-ci. »*

Ainsi, mettre en place un système d'information permettant la gestion d'assurances complémentaire santé tout en restant dans le cadre posée par la loi est une tâche délicate. Le système actuel existe depuis de nombreuses années mais, lorsqu'en avril dernier, MAAF Santé a reçu un questionnaire envoyé par la CNIL afin de mener « *une action de contrôle de certains organismes du secteur de l'assurance santé* », cette problématique de conformité a alors pris toute son importance.

Ce questionnaire a été soumis par le groupe européen G29, qui est composé des différentes commissions européennes liées à la protection des données. Son objectif premier est de consulter un panel assez large de société proposant des assurances santé afin d'évaluer les méthodes et techniques de chacun et, a terme, de proposer une législation européenne en la matière. Ce document, traité par Monique BUREAU, Jérôme BROSSARD (stagiaire), le département juridique et un consultant externe, a nécessité la collecte d'informations auprès des équipes MOA et DIT puis a été retourné à la CNIL à la fin du mois de mai.

En parallèle de la réponse à ce questionnaire, il fallait donc s'assurer que les quatre déclarations relatives au système santé étaient à jour, en accord avec la nouvelle loi I&L et en accord avec les réponses renvoyées à la CNIL.

Le travail déclaratif

Notre tâche, à Jérôme et à moi-même, fût donc de reprendre les différents points de ces quatre déclarations qui concernent :

- la gestion des adhérents;
- Le calcul et paiements des prestations dues aux assurés;
- Le calcul et paiement des prestations dues aux professionnels de la santé par échange de fichiers;
- Les échanges de fichiers avec la Caisse Primaire d'Assurance Maladie pour rembourser les décomptes des assurés sociaux.

Ne connaissant pas le métier de l'assurance santé, la première étape était de comprendre son fonctionnement (que je ne détaillerais pas ici pour des raisons de complexité) et plus particulièrement au niveau des données traitées et échangées entre les prestataires (CPAM via D'ARVA, ATOS, etc...) et en interne (vers l'informatique décisionnelle, par exemple).

Sur un système d'information aussi vaste, la première difficulté n'est pas forcément de comprendre une information mais plutôt de réussir à l'obtenir. Le nombre de personne administrant l'ensemble du système est important et plus personnes ne connaît tout le système. Trouver une information peut donc s'avérer tout aussi complexe que de la comprendre.
En possession de ces données, chaque traitement doit être répertorié et être accompagné de sa finalité, c'est à dire l'objectif recherché lors de sa mise en place.

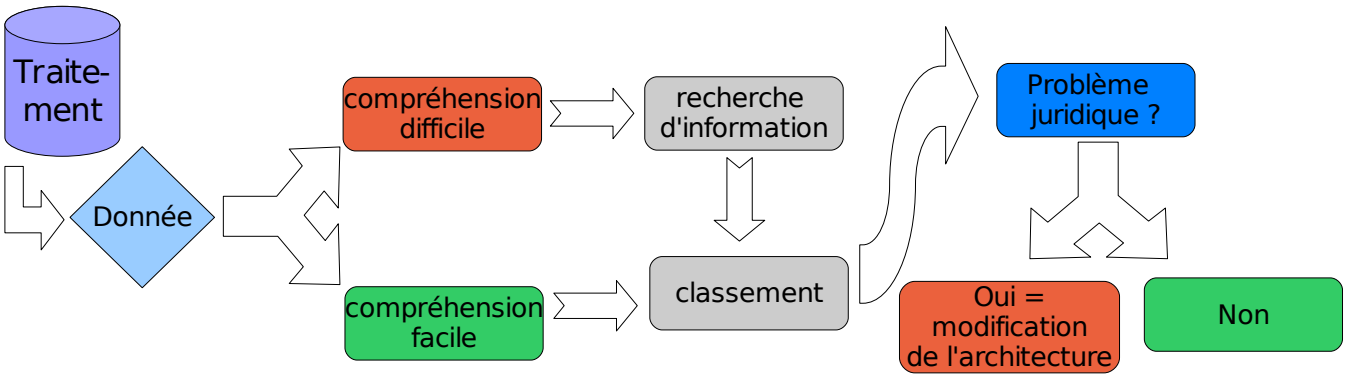
Une fois ce travail effectué, il faut catégoriser les différentes données selon, dans la mesure du possible, les critères de la CNIL. La commission fournie 16 catégories de données qui sont sensibles au regard de la loi I&L :

- A : Données d'identification (nom, prénoms sexe, initiales, n°s d'ordre, date et lieu de naissance…)
- B : NIR, N° de Sécurité Sociale ou consultation du RNIPP
- C : Situation familiale
- D : Situation militaire
- E : Formation – Diplômes – Distinctions
- F : Adresse, caractéristiques du logement
- G : Vie professionnelle
- H : Situation économique et financière
- I : Moyens de déplacement des personnes
- J : Utilisation des médias et moyens de communication
- K : Données à caractère personnel faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses ou les appartenances syndicales des personnes
- L : Données biométriques
- M : Santé, données génétiques, vie sexuelle
- N : Habitudes de vie et comportement
- O : Informations en rapport avec la police
- P : Informations relatives aux infractions, condamnations ou mesures de sûreté

Si une donnée ne rentre pas dans l'une des catégories précédentes, elle doit être classée dans une catégorie annexe dont la définition est laissée à la libre appréciation du déclarant.

Analyse des données

Sur un système aussi important, établir les déclarations des traitements représente un travail conséquent du fait de la quantité d'informations à analyser. Le travail d'analyse suit généralement le schéma suivant :



Dans le cas du système santé, nous nous sommes aperçus que la présence de certaines données dans un traitement particulier pourrait constituer un problème aux yeux de la CNIL. Ce cas de figure nécessite donc une modification de l'architecture, c'est à dire redéfinir avec les concepteurs et administrateurs du système

une nouvelle méthode ne faisant pas appel à cette information et s'assurer que cette dernière sera supprimée du système existant et des sauvegardes.

Avec une quarantaine de traitements de données à caractère personnel, le travail de maintien des déclarations normales effectuées par l'équipe Sécurité est plus que conséquent. Fort heureusement, la modification de la loi I&L apporte une solution très intéressante : le Correspondant Informatique et Libertés.

I.4 Le correspondant Informatique et Libertés

« Introduit en 2004 à l'occasion de la refonte de la loi Informatique et Libertés du 6 janvier 1978, le correspondant à la protection des données est désormais un personnage incontournable dans le paysage de la protection des données à caractère personnel. Sa désignation est facultative et permet un allègement considérable des formalités de déclaration ; elle constitue surtout un moyen efficace de veiller à la bonne application, dans l'organisme, de la loi Informatique et Libertés et donc à assurer le respect du droit fondamental à la protection des données personnelles.

Tous les responsables de traitements et de fichiers peuvent recourir à cette formule, qu'ils soient publics ou privés, qu'ils aient le statut d'associations, de collectivités locales ou de grandes administrations de l'État, qu'il s'agisse de PME-PMI ou d'entreprises multinationales. »

extrait du « Guide du Correspondant Informatique et Libertés », CNIL 2005

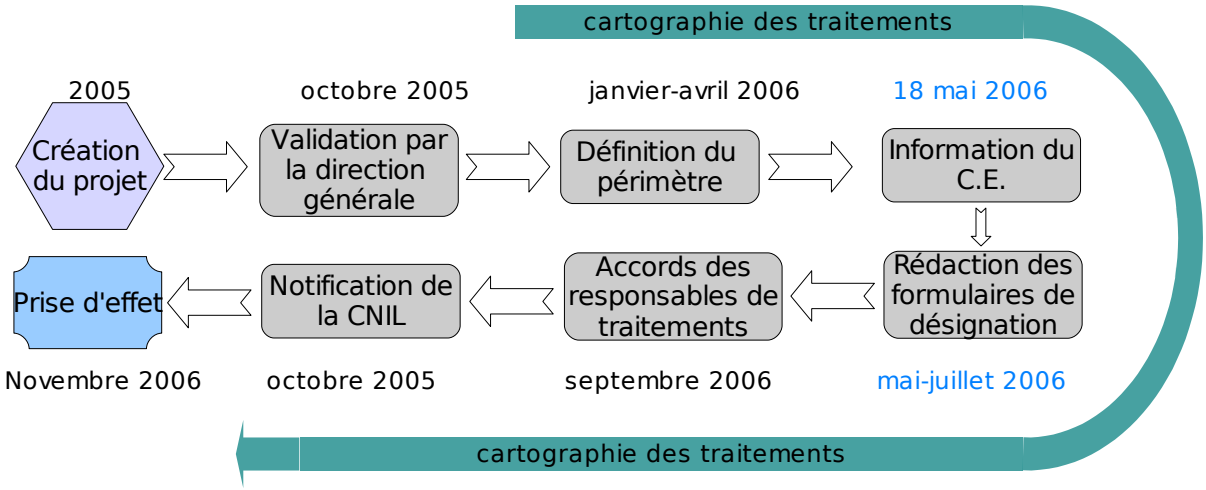
Le groupe MAAF, dans un souci d'amélioration de la gestion interne des contraintes I&L, à décidé de mettre en place la fonction CIL au moment de la parution du décret de mise en application de la loi, en octobre 2005. C'est Monique BUREAU, RSSI du groupe, qui assurera cette fonction. Les intérêts pour un groupe comme MAAF de désigner un CIL sont multiples :

a) **Réactivité** : la mise en place de la fonction CIL exonère l'entreprise de l'envoi à la CNIL des déclarations normales et simplifiées. Cette période de temps, entre l'établissement de la déclaration et la réception de la réponse de la CNIL, disparaît avec la mise en place du CIL et permet donc de réduire le temps de réalisation d'un projet (un traitement ne peut démarrer que lorsque le récépissé de prise en compte de la déclaration est renvoyé par la CNIL). Toutefois, le CIL doit tenir à jour la liste des traitements. A Maaf Assurances, la cartographie des traitements est en cours de réalisation par Jérôme BROSSARD et sera tenue à jour par Monique BUREAU.

b) **Transparence** : veiller à la bonne application de la loi. C'est évident si l'on pense aux sanctions que peut désormais prononcer la CNIL, mais également afin de préserver l'image de marque. En effet, pour une entreprise qui gère, comme nous venons de le voir avec le domaine Santé, des données souvent délicates, les conséquences commerciales d'une sanction de la CNIL seraient désastreuses. A l'inverse, la mise en place de la fonction CIL souligne l'implication de l'entreprise concernant la protection des données personnelles.

c) **Conseil** : le CIL dispose d'un lien privilégié avec la CNIL, ce qui lui permet d'être parfaitement informé des tenants et aboutissants de la loi I&L. De fait, il assure un rôle de conseil et de recommandation sur les projets.

L'une de mes missions de stage a été d'accompagner la mise en place de la fonction CIL. Cette désignation est programmée en plusieurs étapes :



Phases de la désignation du CIL (en bleu : phases auxquelles j'ai contribué)

Suite à la validation du projet par Jean-Jacques VOUHE, l'administrateur de la Direction Générale des Ressources (dont fait partie la DIT), l'une des premières tâches a été de définir un périmètre des sociétés pour lesquelles Monique BUREAU assurera la fonction de CIL. A ce jour, le périmètre comprend 21 sociétés dont la majorité est situé sur le site de Chauray, le siège social du groupe.

Lors de mon arrivée, l'étape suivante de la désignation du CIL était l'information des membres du Comité d'Entreprise (CE). J'ai été sollicité afin de réaliser la présentation de la fonction CIL, présentation qui a été effectuée par Jean-Pierre GIQUEL, directeur de la DIT. La réalisation de cette tâche a impliqué un travail de veille documentaire et législative conséquent, tant sur les missions de la CNIL et la loi I&L que sur la fonction CIL et son application à MAAF Assurances.

L'étape suivante, une fois la validation du CE effectuée était donc la rédaction des formulaires de désignation pour chacune des sociétés (voir annexe A). L'essentiel du travail effectué concerne la recherche des informations légales de ces sociétés et la définition des caractéristiques du correspondant pour chacune d'elles.

Le projet de désignation du CIL devrait trouver son terme avant la fin de l'année 2006 et va permettre une amélioration importante des méthodes de travail liées à l'informatique et aux libertés. Ce que je vais maintenant présenter est donc la suite logique de ce travail, à savoir la sensibilisation des employés au respect de la loi I&L, prérogative du CIL.

I.5 Formation CNIL : la sensibilisation des employés MAAF

La raison principale de la présence inopportune d'une donnée à caractère personnel dans un traitement sensible est, dans 90% des cas, que les concepteurs du système n'avait pas connaissance des limitations posées par la loi Informatique et Libertés.

Il est, en effet, peu probable qu'un traitement corrélant abusivement des données à caractère personnel (par exemple, à des fins de marketing) soit mis en place sans que personne ne se pose à un moment donné la question : « *Mais, au fait, a t-on le droit de faire ça ?* ». La sensibilisation des employés MAAF (et plus particulièrement ceux travaillant sur les différents projets) aux tenants et aboutissants de la loi I&L a pour objectif d'amener le plus grand nombre de personnes à se poser ce genre de questions.

Cette formation est réalisée sous la forme d'une présentation d'environ une heure faite par l'équipe Sécurité à un groupe restreint de personnes. Mon travail, sur ce projet, était de reprendre le support existant afin d'en effectuer une ré-écriture, nécessaire du fait de la modification de la loi, et une remise en forme du fait de l'évolution de la charte graphique MAAF. La présentation s'articule autour des axes suivants :

1. **Contexte législatif** : dans un premier temps, l'objectif est de présenter à l'interlocuteur les notions indispensables à la compréhension de la loi I&L. Cela comprend le contexte de la loi, ce qu'est une donnée à caractère personnel, les obligations (déclaration, information, sécurité), les dispositions (droit d'accès, interdictions, durée de conservation), etc... La fonction CIL y est également présentée et l'accent est mis sur le fait que l'entreprise n'est pas pour autant exonérée de ses responsabilités. Enfin, un rapide tour d'horizon de la Loi pour la Confiance dans l'Économie Numérique (LCEN) est effectué.
2. **Qu'est-ce que la CNIL** : son nom est généralement connu de tous, mais c'est tout. Les quelques *slides* de cette seconde partie ont pour objectif de présenter ses missions et ses domaines d'activité. L'objectif est d'amener l'auditeur à prendre toute la mesure du rôle de la CNIL, et surtout de ses pouvoirs.
3. **Stratégie de déclaration** : que doit-on déclarer ? Quand une demande d'autorisation est-elle nécessaire ? Comment intégrer la loi Informatique et Libertés dans les projets ? Cette troisième section présente une procédure de mise en conformité à prendre en compte dès les premières phases d'un projet.

4. **Collecte et échange d'informations** : la dernière partie de la formation présente les bonnes pratiques à mettre en oeuvre dès qu'une collecte d'information est requise, ce qui inclut les questionnaires, sondages, formulaires, etc... Le principe d'analyse systématique par le CIL et le département juridique est également présenté.

Le support réalisé a un objectif double. Dans un premier temps, il permet évidemment de former le personnel, mais son second intérêt est de servir de support documentaire pour la prise en compte des considérations CNIL dans les projets. A ce titre, les informations qu'il contient se doivent d'être précises, synthétiques et pédagogiques.

I.6 Informatique et Libertés à MAAF Assurances

Étant issu de domaines plus techniques et ne possédant que quelques connaissances scolaires sur le domaine de l'Informatique et Libertés, j'ai abordé ce sujet de stage avec une certaine timidité. Toutefois, l'étendue des problématiques que cette loi pose à MAAF Assurances a rendu ce sujet des plus intéressants. J'y ai découvert énormément d'aspects différents, tant sur les systèmes d'informations et la façon dont ils sont constitués (en particulier concernant les mouvements et interconnexions d'informations) que sur les problématiques juridiques auxquelles, bien trop souvent, nous ne faisons pas attention.

La CNIL impose aux responsables de traitements de prendre du recul par rapport à leurs utilisations des outils informatiques, outils qui peuvent se révéler extrêmement puissants pour corréler des informations qui ne devraient pas l'être (ex : outils d'informatique décisionnelle mis à disposition des équipes Marketing).

Dans la suite de ce rapport, je vais parler de corrélations d'informations qui, cette fois, rentrent parfaitement dans les critères de la CNIL et sont même au coeur des considérations des Directions des Systèmes d'Information : les indicateurs et, plus précisément le tableau de bord pour l'activité virale.

Indicateurs de l'activité virale

Le volume d'informations ne cesse d'augmenter et les systèmes informatiques participent à cette accélération avec les bénéfices de la dématérialisation. Les entreprises sont aujourd'hui connectées en interne mais aussi dans le monde entier. De ce fait, le système d'information est accessible de l'extérieur et qui dit accessibilité dit aussi vulnérabilité vis à vis d'attaques potentielles. Des risques tels que les vols d'informations, l'usurpation d'identité, l'intrusion, la corruption et destruction de données ou encore la mise hors service des systèmes de ressources informatiques sont donc bien présents aujourd'hui. De fait, il n'est pas étonnant de voir que la sécurité informatique est un des 5 risques majeurs recensés par l'entreprise (étude Protiviti/TNS Sofres).

II.1 Démarche qualité et indicateurs sécurité

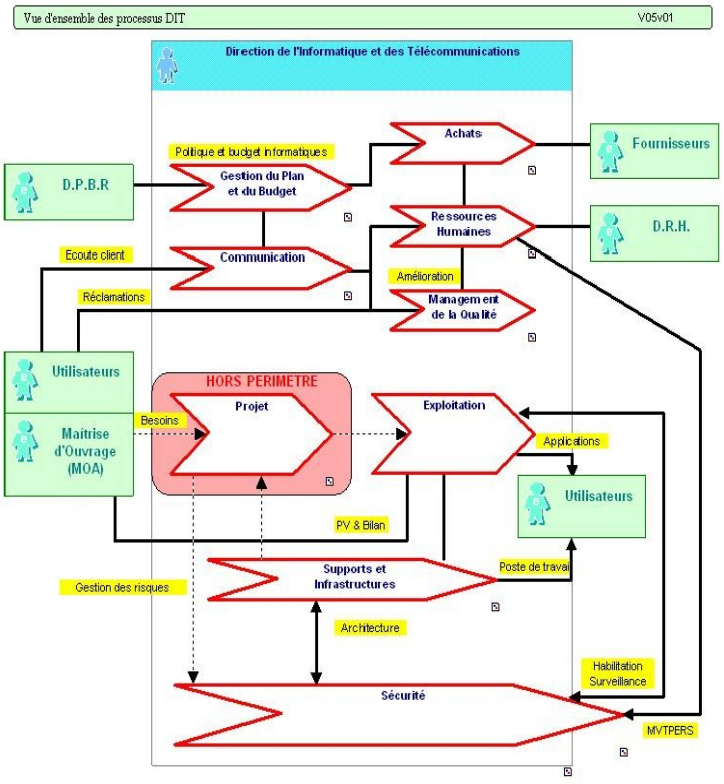
L'engagement de la Direction Informatique et Télécommunications en matière de qualité date de 2002, avec la certification ISO-9001, dont le renouvellement a eu lieu pendant mon stage au mois de Juin. La DIT est pionnière au sein du groupe MAAF dans ce domaine, c'est en effet la seule entité du groupe à être certifiée ISO à l'heure actuelle.

L'engagement de la Direction définit cinq axes principaux d'améliorations, dont un concernant directement l'équipe Sécurité des Systèmes d'Information, a savoir : « *Assurer la cohérence et la pérennité des solutions techniques en terme de développement, d'exploitation et de sécurité des systèmes d'information.* »

L'importance de la sécurité dans la démarche qualité est d'autant plus significative que l'année 2006 est l'occasion de l'intégration d'un processus Sécurité au sein de la démarche Qualité.

Ce processus est piloté par 3 indicateurs regroupés sous l'intitulé « Efficacité des Anti-virus ». Leurs objectifs sont de:

- Mesurer les spams et les messages reçus de l'extérieur;



Vue d'ensemble des processus Qualité de la DIT

- Mesurer le nombre d'appels hot-line enregistrés pour des problèmes de spam ou de virus;
- Mesurer le nombre de postes/serveurs contaminés.

En parallèle des travaux de la DIT en matière de Sécurité, la parution en octobre 2005 de la norme ISO-27001 annonce un intérêt important des entreprises pour le domaine de la Sécurité des Systèmes d'Informations. Les indicateurs étant au coeur de la norme (et seront prochainement normalisés dans un document externe : ISO-27004), les réflexions et publications touchant ce domaine sont nombreuses et ont été une source importante d'informations pour la formalisation des indicateurs MAAF.

Le Système de Management de la Sécurité de l'Information (SMSI) définit par ISO-27001 s'appuie grandement sur ces indicateurs. Ces derniers sont spécifiques à chaque organisme et ne servent pas à contrôler le niveau de sécurité de l'entreprise mais plutôt à contrôler l'efficacité des mesures de sécurité mises en oeuvre.

Enfin, le groupe de travail « Sécurité » du CIGREF, Club Informatique des GRandes Entreprises Françaises, dont MAAF Assurances est membre, a récemment démarré un projet « Indicateurs Sécurité ».

L'objectif de ce projet est de formaliser un certain nombre d'indicateurs fournis par les entreprises membres puis de les centraliser afin de créer un tableau de bord sécurité à grande échelle.

Parmi ces indicateurs, on retrouve le nombre d'attaques reçues par voie virale, un pourcentage du type des attaques et un pourcentage de diffusion des définitions de virus (mises à jour des logiciels anti-virus fournies par les éditeurs) sur les machines du réseau.

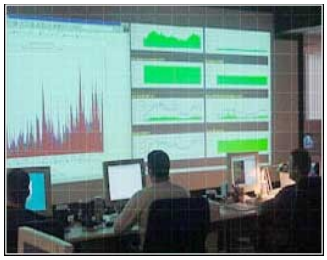
Ces différents projets montrent un intérêt croissant pour les indicateurs sécurité. Reprendre une démarche de formalisation des indicateurs de l'activité virale inclut donc forcément de conformer ces indicateurs non seulement aux besoins actuels mais également à ceux prévisibles. La définition du périmètre des indicateurs prend en compte ces considérations.

Le Gantt complet du projet est disponible en annexe B.

II.2 Périmètre des indicateurs

La définition du périmètre des indicateurs se découpe en trois parties :

1. Que veut-on mesurer ?
2. Pourquoi veut-on le mesurer ?
3. Peut-on le mesurer ?



Comme précisé précédemment, ce que nous souhaitons mesurer c'est l'efficacité des systèmes Anti-Viraux. Dans les faits, cela concerne deux architectures :

- L'architecture de messagerie : elle est composée de serveurs filtrants (premier niveau de protection effectué par le logiciel WebWasher) et de serveurs de messagerie (deuxième niveau de protection effectué par le logiciel Antigen);
- Les postes de travail et serveurs : ils sont protégés par le système Symantec Norton Antivirus.

Ces systèmes représentent les principaux points d'entrées/sorties d'informations entre le réseau MAAF et l'extérieur et le réseau MAAF et lui-même. De fait, la majeure partie des menaces est stoppée au niveau de la messagerie et en local sur les postes et serveurs. Mettre en place des indicateurs pour mesurer l'efficacité des Anti-Virus c'est donc, en fin de compte, maîtriser la première ligne de défense du système d'information de MAAF Assurances.

Il est possible, relativement simplement, de récupérer les traces des anti-virus de la messagerie car le nombre de serveurs impliqués dans ce travail est restreint. Pour les postes de travail et serveurs, c'est déjà plus complexe. Le réseau MAAF est doté de plus de 900 serveurs et plus de 6000 postes de travail, ainsi remonter les informations de l'ensemble de ces entités est complexe. De plus, il est probable que, sur un nombre aussi important de machines, des incohérences apparaissent (dysfonctionnement, etc...).

II.3 Étude de l'existant

Lorsque j'ai commencé ce projet, la publication des indicateurs anti-virus était déjà rodée au 15 de chaque mois mais ceci impliquait un important travail manuel de récupération, corrélation et exploitation. Afin de mieux expliquer ces problématiques, je vais revenir quelque peu en arrière pour présenter la situation au mois de mai 2006.

Dans un premier temps, les traces ne sont pas centralisées:

- Le système de filtrage de la messagerie est géré par l'équipe *télécom* et cette dernière met à disposition, chaque jour, les traces du jour précédent via une ressource réseau partagée.
- Le système de serveurs mail, basé sur le produit Lotus Notes, fournit un grand nombre de traces accessibles via la base de données du serveur. Il faut donc passer par un logiciel client Lotus Notes pour récupérer, via le langage de requêtes SQL, les traces de ces serveurs.
- Les traces des entités de l'architecture Symantec Norton sont stockées sur un serveur accessible via un script. Ce script crée un fichier contenant les dernières traces du réseau.

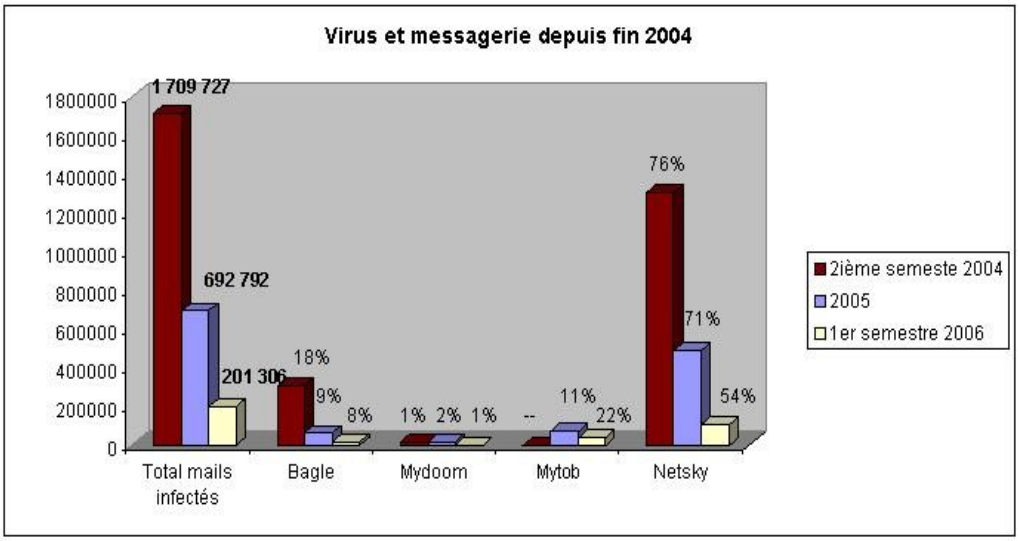
Christophe MOREAU, ingénieur sécurité, s'occupe des deux premiers systèmes. Pour chaque système ont été développés des scripts permettant la production des résultats qui sont ensuite ajoutés manuellement dans un tableau de bord annuel. Les informations récupérées sont journalières et concernent la quantité de mails entrants et sortants, la quantité de mails bloqués par le système de filtrage WebWasher, la quantité de mails bloqués par le système anti-virus Antigen et, enfin, le nombre de mails infectés par virus.

Monique BUREAU réalise l'exploitation des traces du système Norton manuellement par le biais de fichiers Excel. Les informations récupérées après exploitation sont le nombre de fichiers infectés et le nombre de postes différents infectés.

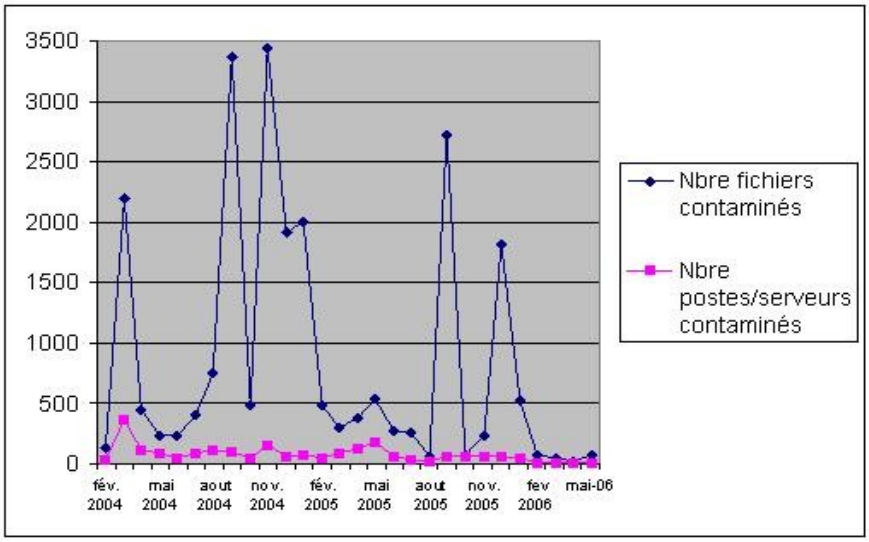
Ces informations permettent de produire deux documents. Le premier est mensuel est consiste en une diapositive (Powerpoint) de l'activité virale pour le mois précédent, le second est bi-annuel, c'est le tableau de bord de synthèse de l'activité virale.

J'ai réalisé ce tableau de bord pour le 1er semestre 2006 (janvier à juin). L'objectif de ce document est de présenter l'état d'avancement des projets internes (mise en oeuvre du système antispam, déploiement de l'architecture WSUS pour les mises à jour Microsoft, etc...), de présenter les indicateurs concernant le réseau MAAF et également d'effectuer un suivi de l'activité virale à un plus haut niveau, en corrélant des informations venant de divers éditeurs de solutions de protection, cabinet de conseil, etc...

Les graphiques ci-dessous sont issus de ce tableau de bord :



Évolution du nombre de mails infectés et de la présence des virus depuis le deuxième semestre 2004 à MAAF Assurances.



Évolution de la quantité mensuelle de fichiers infectés et de postes contaminés depuis 2004 à MAAF Assurances.

Ce document est diffusé à l'équipe de direction et aux équipes techniques. Il est également tenu à disposition des auditeurs Qualité. Sa réalisation m'a permis de comprendre la destination des indicateurs et donc de faire le tri parmi un certain nombre de données dont la connaissance n'est pas forcément utile.

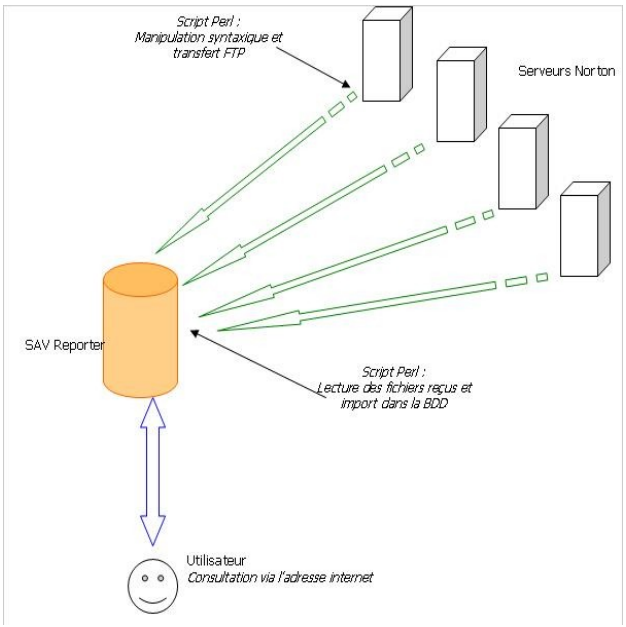
Ce mode de production du tableau de bord possède des défauts importants. Outre la lourde charge de travail manuel induisant forcément des erreurs, aucun contrôle de cohérence n'est effectué. Hors, nous verrons dans la suite de ce rapport que cela s'avère nécessaire.

II.4 Test et analyse du produit « *Symantec SAV Reporter* »

La seconde tâche qui m'a été attribuée, lorsque j'ai commencé ce projet, était l'étude du logiciel SAV Reporter. Ce produit, distribué gratuitement par Symantec, est un tableau de bord pour contrôler l'activité des entités membres d'une architecture Norton. Son périmètre de travail n'inclut pas la messagerie.

SAV Reporter est un outil divisé en plusieurs composants : un moteur client, un moteur serveur, une interface web et une base de données.

- Le moteur client est installé sur chaque serveur Norton du réseau MAAF et s'occupe d'envoyer périodiquement les traces de son serveur vers le serveur central.
- Le moteur serveur lit ces traces et les formate pour les injecter dans la base de données.
- L'interface web permet l'ensemble des opérations de consultations.



Architecture SAV Reporter

Le protocole de test comprend une évaluation de l'interface et des possibilités qu'elle offre, une évaluation de la cohérence des informations récoltées, une évaluation de la sécurité du logiciel et enfin l'étude de faisabilité de l'intégration d'autres sources d'informations (en particulier la messagerie).

Interface

SAV Reporter est, comme beaucoup de produits de manipulation de traces, accessible via une interface web basée sur les technologies HTML et PHP. L'accès est géré par plusieurs niveaux d'accréditation allant du simple accès de consultation à celui d'administration du système.

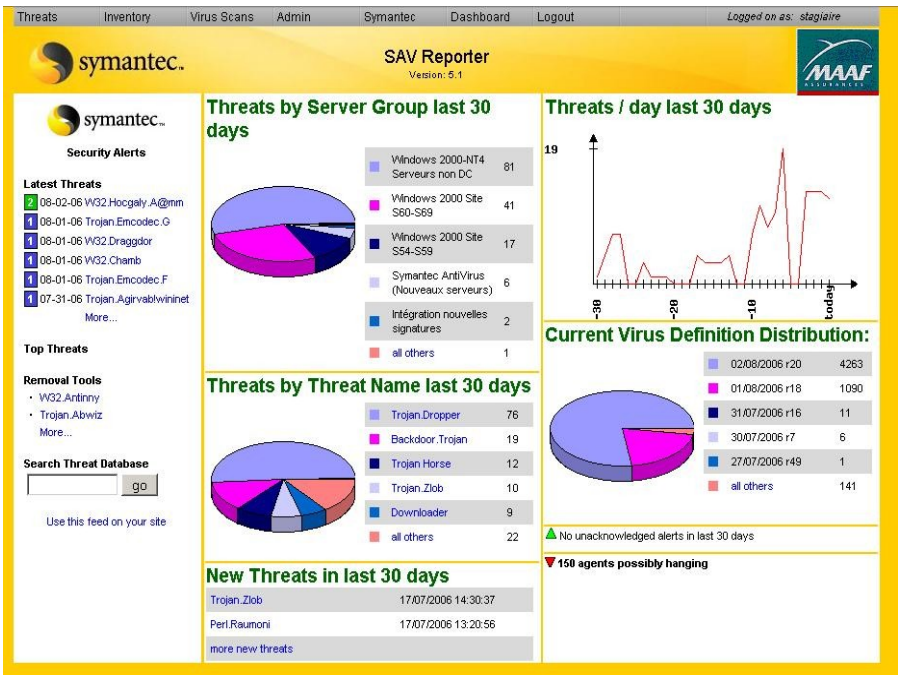
La première chose qui vient à l'esprit en abordant ce logiciel est qu'il est agréable à utiliser. Il permet de

récupérer très rapidement des informations intéressantes comme le nombre de postes infectés, le classement de ces postes par zones (une zone étant un serveur de rattachement de type Active Directory), le listing des derniers virus apparus et leurs niveaux de menaces, etc..

Il est possible de générer des rapports pour une période donnée, l'application se charge alors de la production des graphiques au format image et produits des résultats pour de nombreux paramètres.

Toutefois, on découvre ici une première limitation dans l'impossibilité de paramétrer ces rapports. Les informations produites sont très techniques et ne renseignent pas vraiment l'utilisateur sur le niveau d'efficacité des produits Norton.

De plus, le rapport est consultable dans une page internet et il n'est pas proposé à l'utilisateur d'exporter ce rapport vers un format modifiable (Excel ou Word) ou simplement portable (PDF).



Interface du logiciel SAV Reporter

Enfin, la dernière limitation majeure identifiée de l'interface concerne la consultation des infections. Cette consultation est bien faite et propose un grand nombre de critères de tri mais ne propose aucune option de classement ou de regroupement. De plus, l'export n'est possible que vers un fichier au format CSV, format dans lequel les données sont séparées par des points virgules, sans aucune mise en page. Il est donc indispensable d'effectuer un nouveau traitement de ce fichier dans un logiciel externe pour le rendre lisible.

Cohérence

Le logiciel a été mis en place à la fin du mois de mars. Lors de mes tests, il a donc été possible de comparer les résultats de celui-ci avec ceux issus de l'ancienne méthode (décrite en page 21). Hors cette comparaison a révélée un nombre sensiblement supérieur d'infections remontées par SAV Reporter (de l'ordre de 30%).

En utilisant l'interface, il a été possible d'identifier un certain nombre de doublons, c'est-à-dire de lignes scrupuleusement identiques à l'exception de leur identifiant (créés lors de l'ajout du champ dans la base de données). Toutefois, pour tenter de déterminer la source de ces doublons, j'ai récupéré les documentations et scripts composants le logiciel et me suis plongé dedans pendant deux journées complètes.

Je n'ai, hélas, pas pu déterminer la source de ces incohérences, cet exercice m'a toutefois aidé à comprendre un certain nombre de particularités qui m'ont été utiles pour la suite de l'analyse.

Sécurité

Le niveau de sécurité du logiciel n'apparaît pas suffisant. Le système est constitué d'une base de données contenant quantité d'informations qui, sans être sensibles, détaille avec précision l'architecture du réseau informatique de MAAF Assurances.

Hors, la consultation d'une partie de ces informations ne nécessite pas d'authentification. De plus, les champs de consultations se sont révélés fortement réactifs à un type d'attaque connu (injection SQL) permettant de découvrir la structure de la base de données.

Fort heureusement, l'accès au logiciel est limité à l'Intranet MAAF mais les recommandations au terme de cette analyse sont de réduire au maximum l'accès à l'application au personnel le nécessitant.

Intégration de données externes

L'un des objectifs était d'évaluer la faisabilité de l'intégration des traces issues des logiciels WebWasher et Antigen, faisant alors de SAV Reporter un tableau de bord complet pour l'activité virale au sein du réseau MAAF.

Potentiellement, l'utilisation du langage Perl dans les scripts de SAV Reporter autorise les modifications à tous les niveaux. Mais, en fait, ce produit n'a pas été conçu pour cela. Les scripts sont donc imposants (1500 lignes pour les plus gros) et très peu commentés (en Anglais et même parfois en Allemand).

De plus, la documentation ne précise pas le fonctionnement global de l'application. Il faudrait donc refaire le travail d'algorithmique à partir de l'existant avant d'y intégrer les modifications... en supposant que cela soit possible.

Bilan

SAV Reporter n'apparaît pas comme une solution convenable pour répondre aux besoins de tableau de bord sécurité. Si l'important travail de ré-écriture et de maintenance qu'imposerait son utilisation n'était pas assez dissuasif, il faut ajouter à cela le fait que ce produit ne dispose d'aucun support contractuel.

Toutefois, SAV Reporter présente deux avantages :

- Il réalise tout le travail de centralisation des traces Norton
- Il fournit un certain nombre d'informations très intéressantes et cohérentes comme la diffusion des définitions de virus ou encore la liste des derniers virus apparus et leurs niveau de menace.

En conséquence, il est décidé de préparer un projet indépendant s'appuyant sur l'existant et donc, entre autre, SAV Reporter. C'est ce projet, qui représente l'essentiel de mon travail au sein de l'équipe sécurité, que je vais maintenant présenter.

II.5 Le projet « *TBvirus* »

A ce stade du projet, il est apparu que la solution la plus efficace pour résoudre notre problématique initiale était le réalisation d'un outil de gestion des tableaux de bord de l'activité virale. En concertation avec l'équipe Sécurité, nous avons établi les besoins suivants :

1. Centraliser la localisation des traces fournies par les différents systèmes en un point unique du réseau géré par l'équipe Sécurité;
2. Formaliser les indicateurs de l'efficacité des Anti-Virus;
3. Automatiser l'exploitation du tableau de bord.

A ces besoins il faut ajouter la nécessité de produire un outil simple, évolutif et utilisant des technologies connues.

II.5.1 Spécifications fonctionnelles

En coordination avec Monique BUREAU et Christophe MOREAU, nous avons établi les spécifications fonctionnelles suivantes :

- Réutilisation des traces existantes avec une charge de travail minimale pour les équipes techniques;
- Récupération et centralisation des traces;
- Exploitation des traces informatiques au jour précédent (J -1);
- Possibilité d'exploitation sur une période donnée, saisie par l'utilisateur;
- Visualisation synthétique des résultats;
- Corrélations d'informations entre les différents systèmes (totaux par virus, top 5 des virus, ...);
- Correction des erreurs de cohérence Norton;
- Export des données exploitées au format Excel;
- Traitement et mise à jour automatique d'un tableau de bord (au format Excel) incluant une synthèse mensuelle et annuelle.

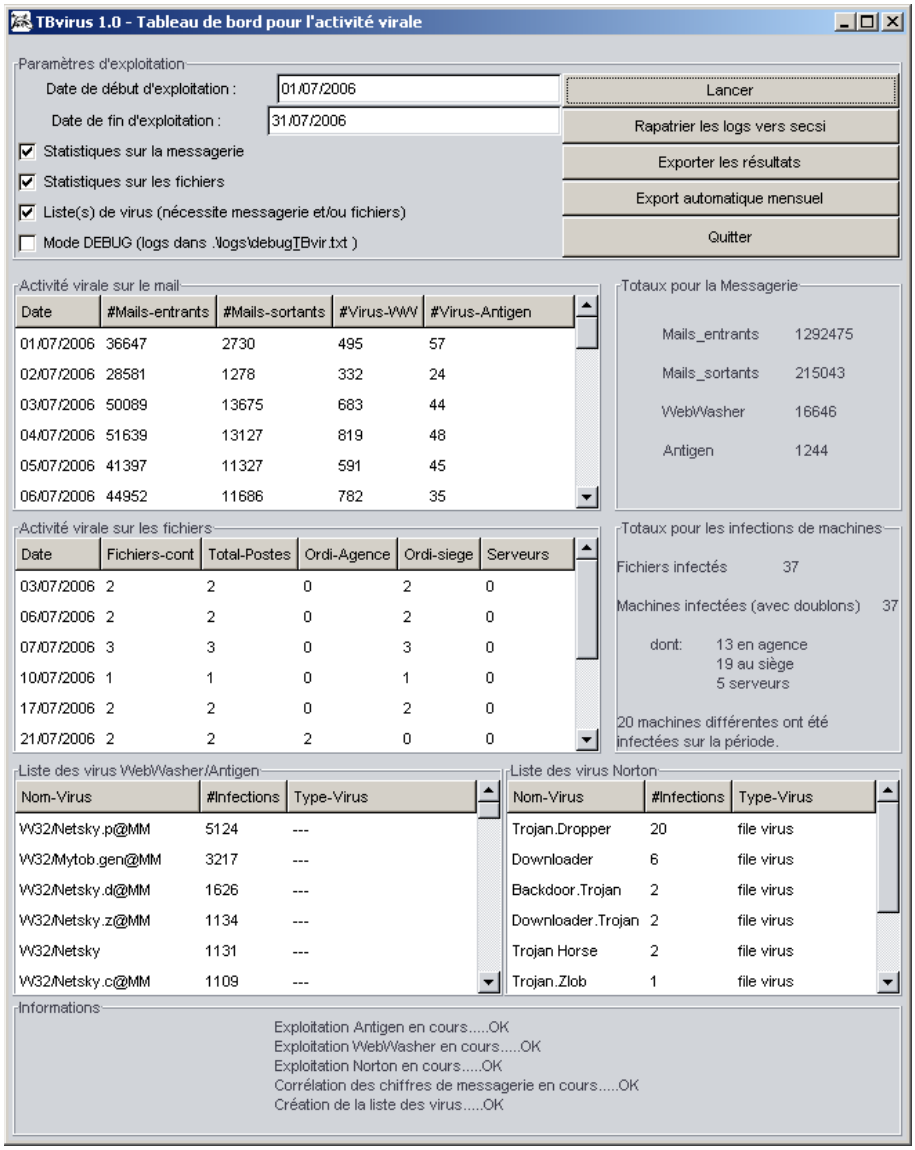
Dans un souci d'évolutivité, il a été décidé de conserver le format temporaire actuellement utilisé pour l'exploitation des traces informatiques. Ceci concerne les fichiers temporaires utilisés à mis chemin de l'exploitation des traces. Ainsi, si un composant de l'architecture MAAF venait à évoluer, les modifications à apporter sur le programme TBvirus ne concerneraient que le script permettant de produire ce fichier temporaire. Le reste de l'application ne nécessitera alors pas de modification.

II.5.2 Ergonomie

Un des souhaits exprimés lors des discussions autour du projet TBvirus était que l'application soit simple d'utilisation et que la majorité des actions effectuées soient transparentes à

l'utilisateur. Ainsi, en utilisation normale, les fonctionnalités sont réduites au nombre de quatre. Libre ensuite à l'utilisateur de modifier, améliorer ou remodeler les résultats qu'il récupère via le logiciel Excel.

L'application se présente comme suit :



La partie haute de l'application permet à l'utilisateur de paramétrer la période à exploiter et les données sources qui désire. Les cinq boutons en haut à droite permettent de lancer différentes actions :

- **Lancer** : appel les fonctions d'exploitation choisies pour la période saisie puis affiche les résultats dans la fenêtre principale.
- **Rapatrier les logs** : L'équipe Sécurité dispose d'une ressource réseau dont elle a le contrôle. Cette fonction permet de contacter les différents serveurs (possédant les traces de l'activité virale) et copie ces traces dans un répertoire formalisé de la ressource réseau. Ainsi, la production des indicateurs est basée sur les traces archivées par l'équipe Sécurité et ne nécessite plus la présence de celles-ci sur le réseau, dont la gestion est laissée aux équipes techniques.

- **Exporter les résultats** : permet d'extraire les données exploitées vers un fichier Excel à la destination choisie par l'utilisateur.
- **Export automatique mensuel** : Chaque mois, le lancement de cette fonction met à jour le tableau de bord annuel dont l'emplacement est formalisé. En début d'année, elle s'assure également de créer un nouveau tableau de bord.

Cette interface utilise la technologie Gimp Tool Kit (Gtk) et répond au critère de simplicité et de lisibilité posée au commencement du projet.

II.5.3 Techniques de programmation

Ne souhaitant pas noyer le lecteur sous les détails techniques, je vais, dans cette partie, m'attacher à décrire le plus synthétiquement possible les méthodes que j'ai utilisées pour mettre en place les fonctionnalités identifiées au point II.5.1.

Tout d'abord, l'application est entièrement écrite en langage Perl. Ce langage est très populaire pour sa lisibilité et ses fonctions avancées de manipulation de fichiers. Ce choix a d'ailleurs été dicté par la présence du langage Perl au sein de la majorité des scripts utilisé tant dans les équipes techniques que dans l'équipe Sécurité.

Récupération et centralisation des traces

Cette première tâche est celle qui a demandé le plus d'interaction avec les équipes techniques. Elle a été l'occasion de découvrir la structure du réseau MAAF et a permis un certain nombre d'optimisation du stockage en limitant la production de traces au strict nécessaire.

Le système WebWasher a été le plus simple à traiter, car ses traces étaient d'ors et déjà disponibles via une ressources réseau.

Le système Antigen a demandé quelques opérations techniques afin de formaliser une production et une mise à disposition journalière des traces.

Le système SAV Reporter a demandé plus de travail du fait que la récupération des traces devait passer par l'interrogation de l'interface de consultation (la base de données n'étant pas accessible).

L'essentiel du travail de programmation concernait ensuite la récupération intelligente des traces, afin de ne prendre que le strict nécessaire et toujours jusqu'à J -1.

Possibilité d'exploitation sur une période donnée, saisie par l'utilisateur

La possibilité est donnée à l'utilisateur de choisir la période sur laquelle il souhaite réaliser l'exploitation. Il est donc possible d'exploiter une seule journée comme une année complète, la seule limitation se situant au niveau de la disponibilité des traces pour la période choisie. Ainsi le système ne dispose d'aucune traces précédent juin 2006, date de démarrage du projet (toutefois ces données manquantes ont été reportées dans le nouveau tableau de bord à partir de l'ancienne exploitation).

Corrélations d'informations entre les différents systèmes

L'intérêt d'automatiser une tâche est de produire des résultats difficilement productibles manuellement. La première tâche du logiciel est donc de regrouper les résultats pour la messagerie qui sont issus de trois types de fichiers différents : les fichiers « reports » qui contiennent le comptage des messages entrants et sortants et les fichiers WebWasher et Antigen qui contiennent la liste des virus trouvés par ces systèmes. Ces résultats sont présenté à l'utilisateur dans la liste en haut à gauche de l'application.

Lorsque c'est possible, le logiciel corrèle les informations des virus entre les systèmes Antigen et WebWasher afin de constituer la liste des virus de la messagerie (*en bas à gauche de l'application*).

Correction des erreurs de cohérence Norton

Comme nous l'avons vu dans l'analyse du logiciel SAV Reporter, un certain nombre de doublons sont présents dans les traces de ce système. Le logiciel effectue des contrôles précis sur les données sources et identifie celle qui correspondent à des doublons. Les doublons ne sont alors pas pris en considérations.

Ce travail était également l'occasion de redéfinir les critères d'exploitation des traces Norton. En effet, le système ne fait pas directement la différence entre une inspection de virus nouvellement arrivé et une inspection de virus en quarantaine. Ce fonctionnement fausse les résultats en augmentant grandement le nombre d'infections pour certains virus. Un cadre d'exploitation a donc été mis en place pour déterminer quelles sont les infections considérées comme intéressantes.

Enfin, TBvirus remonte dans les résultats le type de poste infectés selon trois critères :

- poste situé dans une agence MAAF;
- poste situé au siège social;
- serveur.

Export des données exploitées au format Excel

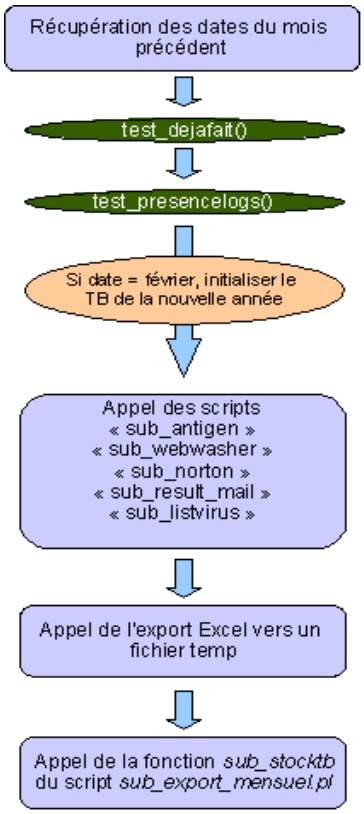
Le format Microsoft Excel n'est pas un format ouvert. Générer un fichier excel à partir d'un logiciel nécessite donc d'utiliser les composants Microsoft et, en particulier, la librairie de fonctionnalités *Object Linking and Embedding*. Sans entrer dans les détails, cette librairie permet la création et la manipulation de documents au format Excel et plus particulièrement la génération de graphiques dans ces fichiers.

Toutefois, l'utilisation de cette librairie en langage Perl n'est pas supportée par Microsoft et est donc le fruit du travail de contributeurs bénévoles. L'apprentissage de son utilisation fut donc assez complexe, faute de documentation officielle à ma disposition.

Traitement et mise à jour automatique d'un tableau de bord

Le contenu et la démarche concernant le tableau de bord annuel seront détaillés dans le point suivant. Au niveau programmation, le développement de cette fonctionnalité s'est révélé de loin le plus complexe de tout le projet.

En effet, afin d'assurer un maximum de cohérence dans l'exploitation, la mise à jour et la maintenance de ce tableau de bord, un certain nombre de contrôle sont effectués :



1. La fonction permet d'ajouter, dans le tableau de bord annuel, les résultats pour le mois précédent;
2. Afin de ne pas corrompre le fichier, un certain nombre de données sont mises à blanc et modifiées lors de l'exploitation. Un test est effectué pour contrôler que ces données sont toujours à blanc et donc que l'exploitation n'a pas déjà été faite;
3. Il est important de s'assurer que l'exploitation mensuelle se fera avec toutes les données requises car, par défaut, l'application ne met pas de message d'erreur sur une données manque lors de l'exploitation d'une période (ceci afin d'exploiter de large période);
4. En cas de nouvelle année (mois == février), TBvirus initialise un nouveau tableau de bord comprenant la génération de toutes les feuilles et de tous les graphiques. Ainsi, le travail mensuel est accéléré.
5. Un traitement similaire à celui fait par la fonction « Lancer » est ensuite appelé, les résultats sont exportés vers un fichier Excel temporaire;
6. Les données du fichier temporaire sont lues et copiés dans le tableau de bord annuel;
7. La feuille de synthèse est mise à jour, en particulier les listes de virus dont les occurrences sont modifiées. Les TOP 5 des virus de la messagerie et des fichiers sont recalculés.

Le travail effectué sur cette fonctionnalité représente environ le tiers du travail de développement effectué sur l'application, soit 6 jours complets.

Incluant la période d'auto-formation au langage Perl, la réalisation technique de ce projet aura représenté un peu plus d'une vingtaine de jours de travail. J'ai essayé, tout au long du projet, de garder en tête le fait que je ne serais pas le mainteneur du logiciel. C'est pourquoi j'ai essayé de commenter le code le plus efficacement possible, et j'ai également réalisé une documentation fonctionnelle et technique diffusée à

l'équipe sécurité.

II.5.4 Tableau de bord annuel

Jusqu'à maintenant, j'ai essentiellement parlé de collecte et traitement de traces informatiques. Hors, cela ne représente qu'une partie certes indispensable du travail mais également inutile si les informations récupérées ne sont pas correctement exploitées.

Je vais ici présenter la formalisation du tableau de bord annuel, document qui est généré automatiquement par le logiciel TBvirus selon des critères précisément définis.

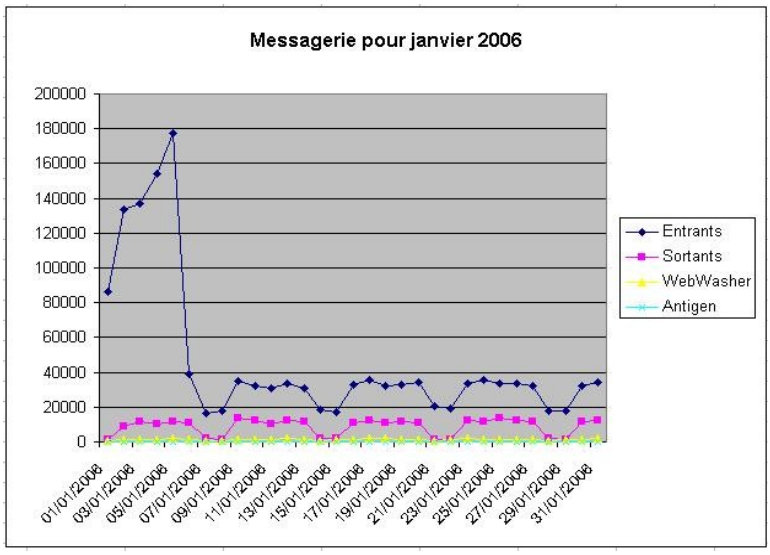
Comme je l'ai déjà précisé lors de la présentation de la norme ISO-27001, l'objectif des indicateurs n'est pas de contrôler le niveau de sécurité de l'entreprise mais bien de contrôler le niveau d'efficacité des logiciels de protections. Pour contrôler ce niveau d'efficacité, l'exploitation des traces seules ne suffit pas. Il faut disposer d'un retour « humain » que les systèmes informatiques ne peuvent évidemment pas fournir. A MAAF Assurances, ce retour humain est présent sous la forme du service « SVP », la hot-line.

Toute étude menée via les indicateurs de l'activité virale nécessite donc de faire le lien avec le nombre d'appels SVP enregistré pour des problèmes de spam ou de virus. Ce chiffre est fourni par le service en question et n'est donc pas inclut dans le tableau de bord annuel automatiquement.

Les indicateurs choisis ont pour règles d'être simples, précis et visuels. Il est communément admis que créer des graphiques illisibles en corrélant des données sans rapports évident ne sert à rien et peut même conduire à un mauvais pilotage des ressources.

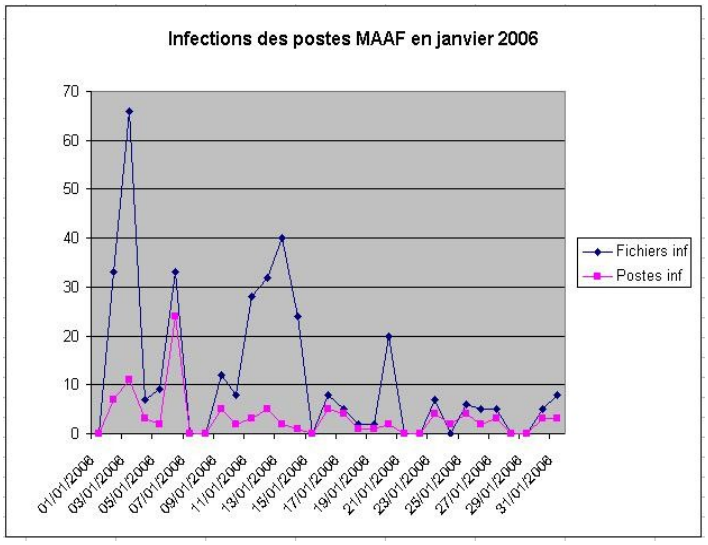
Dans le cas du tableau de bord annuel, les indicateurs sont au nombre de cinq. Ils sont présents dans la feuille de synthèse pour l'année en cours et dans chaque feuilles mensuelles pour le mois concerné.

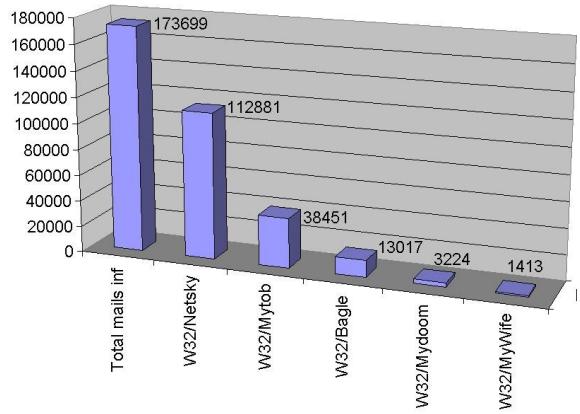
- **Totaux de la messagerie** : ce graphique est constitué de 4 courbes, chacune d'elles est produite à partir d'un total journalier, a savoir : mails entrants; mails sortants; virus détecté par WebWasher et virus détecté par Antigen;



- **Top 5 des virus de la messagerie** : il présente le total

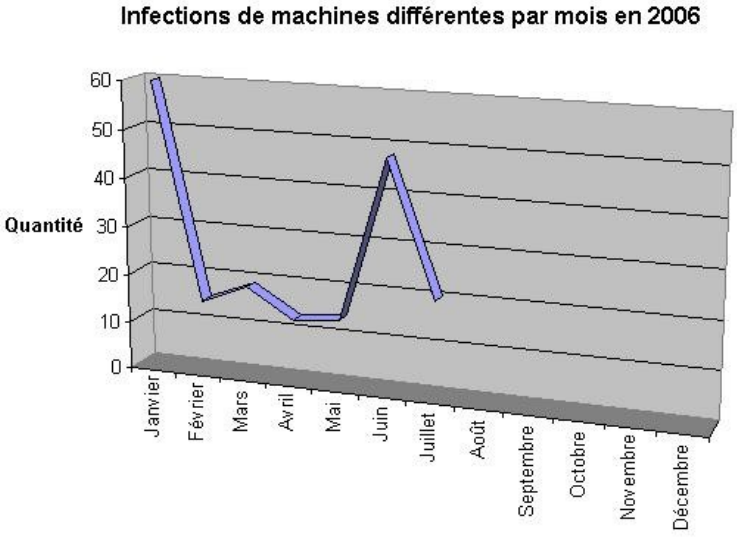
de mails infectés et les infections faites par les 5 versions majeures des virus les plus répandus. Afin d'avoir une vision claire de l'étendu d'un virus, les variantes sont regroupées sous un seul nom (ex: W32/Netsky.saMM et W32/Netsky.q.dam sous regroupés sous le nom W32/Netsky);





Top 5 des virus pour l'année 2006 (en cours)

- **Infections des postes/serveurs** : cette courbe (voir ci-dessus) est composée de deux chiffres journaliers : le nombre de fichiers infectés et le nombre de postes infectés. Le tableau de bord contient également la quantité de machines infectées par provenance et par jours,
- **Top 5 des virus des fichiers** : identique au Top 5 des virus de la messagerie à la différence que les variantes ne sont pas regroupées, faute de syntaxe le permettant.
- **Infections de machines différentes** : ce graphique propose une vision mensuelle de la quantité de machines différentes infectées. Ainsi, une machine infectée plusieurs fois dans le mois ne sera comptabilisée qu'une seule fois.



Le document Excel du tableau de bord contient également un grand nombre d'informations détaillées qui permettent une lecture plus approfondie des indicateurs.

II.5.5 Validation

Le développement s'est déroulé en deux phases: une première phase de programmation basée sur les spécifications identifiées, et une deuxième phase d'amélioration/correction basée sur les résultats des tests effectués.

Le protocole de test est simple : utiliser l'application avec un minimum d'informations concernant son fonctionnement. Les diverses fonctionnalités ont été testées par Monique BUREAU à la fin du mois de Juillet.

Ces tests ont essentiellement permis d'identifier deux types de problèmes:

- Programmation : les inévitables *bugs* dus à l'écriture de code. La majorité des problèmes a été résolue et concernait essentiellement les conversions de dates et l'écriture dans les fichiers Excel. Étant donné qu'il est impossible de tout identifier sur le moment, une deuxième phase de test sera effectuée par Christophe MOREAU dans le courant du mois d'août. Les corrections des éventuels problèmes alors identifiés seront faites au début du mois de septembre.
- Données sources : des problèmes liés aux fichiers de traces ont également été identifiés. Leurs résolution à nécessité la migration de certaines traces vers un nouveau serveur de stockage.

Du fait du démarrage de l'exploitation en cours d'année, et afin d'assurer un maximum de cohérence dans le tableau de bord annuel, des modifications manuelles ont également été apportée pour le 1er semestre 2006. Ces modifications concernent le mode de traitement des données Symantec Norton et leur importation dans le tableau de bord.

Enfin, la stabilité du logiciel a été éprouvée au cours des tests de fonctionnement que j'ai réalisé. Le logiciel s'est comporté de façon stable même en cas de forte charge système. L'application a également été testée sur des versions plus récentes des systèmes Microsoft, à savoir Windows XP Service Pack 2 et Microsoft Office 2003. Son fonctionnement est identique sur ces systèmes que sur les systèmes Windows 2000 et Office 2000 utilisés par Maaf Assurances.

II.6 Évolutions

Ce type de logiciel répond a un besoin précis, clairement identifiée et avec des contraintes qui lui sont propres. Il a été conçut de façon a pouvoir intégrer simplement les éventuels changements du système Anti-Viral du réseau MAAF Assurances.

Le logiciel pourrait évoluer efficacement en intégrant un système de base de données et une interface de production de rapports et de graphiques plus souple, permettant les configurations. Le format de fichier Excel me semble également limité. Le logiciel Excel est extrêmement puissant et permet de réaliser simplement un grand nombre de tâche mais son utilisation via un logiciel tiers, comme c'est le cas avec TBvirus, est complexe et limite grandement les possibilités du produit de Microsoft. Une amélioration de l'export des résultats pourrait donc passer par l'utilisation d'un format standard « XML », comme

Open Document, qui a l'avantage d'être ouvert et donc beaucoup plus facilement manipulable.

Toutefois, TBvirus reste, de part le contexte entourant sa réalisation, un logiciel très ciblé. Une évolution intéressante passerait plutôt, selon moi, par la réalisation d'un tableau de bord global pour la sécurité du système d'information. Ce projet nécessiterait certainement des moyens bien plus important (budgets matériel et humains, équipe en charge de la maintenance, etc...) et un temps de développement également plus long, mais aurait l'intérêt d'offrir une vision globale de l'efficacité des systèmes de protections. J'ai essayé, tout au long des phases de programmation, de rendre les scripts de TBvirus réutilisables si jamais un tel projet venait un jour à paraître.

Conclusion

La prise de conscience, encore récente, des risques liés à l'utilisation massive des systèmes informatiques implique une augmentation toujours croissante de la charge de travail dévolue aux équipes Sécurité des grands comptes. Le groupe MAAF ne fait pas exception à la règle, et, s'il y a bien une chose que j'ai retenue de ces 14 semaines de stage, c'est que le travail ne manque pas. Les projets sont nombreux et certains sont hélas reportés par manque de temps pour les traiter.

La mise en place de la fonction de Correspondant Informatique et Libertés a, entre autres, pour objectif d'optimiser ce temps de travail, tout en conservant un contrôle indispensable sur les traitements déployés en production. La réalisation de cette mission m'a permis de découvrir un grand nombre d'aspects concernant la législation que nous ne voyons pas en formation. Travailler sur un système aussi complexe que le système Santé de MAAF Assurances m'a apporté une compréhension des tenants et aboutissants de la législation que j'étais loin de posséder au début du stage. D'un point de vue personnel, c'est un apport très appréciable.

La Direction Informatique et Télécommunications met un point d'honneur à maîtriser les indicateurs des systèmes qu'elle gère. Le projet « Indicateurs de l'activité virale » s'est complètement inscrit dans cette démarche. La réalisation des différentes phases, outre l'apprentissage d'un langage que je ne connaissais pas, m'ont permis d'aborder la gestion de projet et de bénéficier de l'expérience de MAAF Assurances en la matière.

J'ai également grandement apprécié la coopération avec les différentes équipes techniques. Il n'est pas toujours évident, en tant que stagiaire, d'ajouter une charge de travail supplémentaire à des personnes déjà fortement sollicitées. Hors ces dernières ont été très disponibles et agréables. Il est certain que sans leur coopération ce projet n'aurait pu aboutir.

Enfin, je tiens un dernière fois à remercier l'ensemble de l'équipe Sécurité : Monique BUREAU, Christophe MOREAU et Marcel POUPIN. Leur accueil a été très chaleureux et l'ambiance de travail particulièrement propice à la réalisation de l'ensemble des tâches qui m'ont été confiées.

Références bibliographiques

CNIL

- cnil.fr : le site officiel de la Commission Nationale Informatique et Libertés
- foruminternet.org : site de médiation de d'information
- societe.com : informations légales des entreprises

Indicateurs de l'activité virale

- forum-eurosec.com : forum sur la sécurité des systèmes d'informations
- Comment choisir les indicateurs ISO 27001 (Alexandre Fernandez, HSC)
- SQL Injection White Paper (Kevin Spett, SPI Dynamics)
- perl.com : le site officiel du langage perl
- Gtk2-Perl (Patrice Le Borgne, http://perso.orange.fr/gtk2-perl/Gtk2perl_tutoriel.html)
- Reading and Writing Excel files with Perl (Teodor Zlatanov, IBM)

ANNEXES A

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

COMMISSION NATIONALE DE
L'INFORMATIQUE ET DES LIBERTÉS
Cadre réservé à la CNIL

Date de réception : .....
N° de DCIL :.....
N° d'enregistrement :.....
G |_| P |_| E |_| S |_| M |_| EX |_|

DÉSIGNATION D'UN CORRESPONDANT À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Art. 22 III de la loi n°78-17 du 6 janvier 1978 modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
Art. 42 à 55 décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
La désignation doit être notifiée à la CNIL par lettre recommandée avec avis de réception.
Elle doit avoir été préalablement portée à la connaissance des instances représentatives du personnel par lettre recommandée avec avis de réception.
La désignation prend effet un mois après la date de réception de la notification par la CNIL.

1. Informations relatives au responsable de traitement

Nom de l'organisme, du service ou de la personne responsable de traitement * Sigle : …….......
.. ..
.....
Activité* : .....
*SIREN** |__|__|__|__|__|__|__|__|__| *APE** |__|__|__|__| Forme (SA, SARL etc.).....
Adresse* : ... .
.....
.....
BP |__|__|__|__| Cedex |__|__|__|__| Code postal* |__|__|__|__|__| Ville/Pays ..Niort / France.....
Téléphone* |__|__|__|__|__|__|__|__|__|__| **Télécopie** |__|__|__|__|__|__|__|__|__|__|
Représentant légal (Nom, qualité)* :
.....
.....
Adresse électronique *:* .....@.....

* Les champs marqués par * doivent être obligatoirement renseignés

2. Informations relatives au correspondant

Statut professionnel du correspondant

Cochez la case correspondante

[ ] Correspondant salarié : l*e correspondant est un salarié du responsable de traitement mentionné au 1.*

[ ] Correspondant mutualisé : cochez cette case si le correspondant se trouve dans l'un des cas suivants :

1. L*e correspondant est un salarié du responsable de traitement mentionné au 1 et est désigné également pour d'autres entités du groupe de sociétés auquel appartient ce responsable de traitement.*
2. *Le correspondant est un salarié du groupement d'intérêt économique auquel appartient le responsable de traitement*
3. *Le correspondant est désigné par un organisme professionnel ou un organisme regroupant les responsables de traitement dans un même secteur d'activité.*

[ ] *Correspondant externe*[3] *:* *Le correspondant n'est dans aucun des cas mentionnés ci-dessus.*

Renseignements relatifs à la personne physique exerçant les fonctions de correspondant

Nom, prénom* ..***BUREAU Monique***.....

Fonctions[4]/profession* ..***Responsable de la Sécurité des Systèmes d'Information***.....

Nom de l'employeur (si le responsable de traitement mentionné au 1. n'est pas l'employeur):.....

GIE EURODEM..***(Direction Informatique et Télécommunication, groupe MAAF Assurances)*** .....

Adresse professionnelle (si différente de celle du responsable de traitement mentionné au 1.) :.....

Chauray.....

.....

BP |__|__|__|__| Cedex |__|__|__|**_9_**| Code postal |**_7_|_9_|_0_|_8_|_4_**| Ville/Pays ..***Niort/ France***.....

Téléphone* |**_0_|_5_|_4_|_9_|_3_|_4_|_3_|_9_|_4_|_5_**| Télécopie |__|__|__|__|__|__|__|__|__|__|

Adresse électronique* : ***monique.bureau@maaf.fr***

Renseignements complémentaires lorsque le correspondant est une personne morale :

Nom de l'organisme* Sigle : .....

.....

.....

SIREN* |__|__|__|__|__|__|__|__|__| APE* |__|__|__|__| Forme (SA, SARL etc.)*.....

Activité/profession exercée* :

.....

Représentant légal*

.....

Adresse*

.....

.....

.....

BP |__|__|__|__| Cedex |__|__|__|__| Code postal* |__|__|__|__|__| Ville/Pays .....

Téléphone* |__|__|__|__|__|__|__|__|__|__| **Télécopie** |__|__|__|__|__|__|__|__|__|__|

Adresse électronique *:* ..... @.....

* Les champs marqués par * doivent être obligatoirement renseignés

3 Article 44 décret n° 2005-1309 : ce choix n'est possible que si **moins** de 50 personnes (par ex. service informatique, services opérationnels) ont accès aux traitements concernés ou sont chargés de leur mise en oeuvre.

4 Indiquer les fonctions exercées en plus de celles de correspondant.

3. Les traitements concernés par la désignation

La désignation d'un correspondant entraîne une dispense de l'accomplissement des formalités préalables relatives aux traitements relevant des articles 22 à 24 de la loi du 6 janvier 1978 (régime de la déclaration). Quel que soit le type de désignation, les traitements relevant des régimes de demande d'autorisation ou d'avis auprès de la CNIL ne sont pas dispensés de l'accomplissement des formalités préalables.

[X] Désignation étendue : Le correspondant exerce ses missions[5] pour tous les traitements mis en oeuvre par le responsable de traitement, quel que soit le régime de formalités applicable.
ou
[ ] Désignation générale : le correspondant n'exerce ses missions que pour les seuls traitements qui, en l'absence de correspondant, devraient faire l'objet d'une déclaration auprès de la CNIL (traitements relevant des articles 22 à 24 de la loi du 6 janvier 1978).
ou
[ ] Désignation partielle : le correspondant n'est désigné que pour certains traitements ou catégories de traitements (traitements relevant des articles 22 à 24 de la loi du 6 janvier 1978) énumérés ci-après (par exemple : traitements relatifs aux ressources humaines, traitements relatifs aux clients et prospects...) :
-.....
-.....
-.....
-.....
-.....
-.....
Suite sur papier libre [ ]

Nombre de personnes chargées de la mise en oeuvre des traitements ou ayant directement accès aux traitements concernés par la désignation
[ ] inférieur à 50 personnes [ ] supérieur ou égal à 50 personnes

* Les champs marqués par * doivent être obligatoirement renseignés

5 Art.49 du décret du 20 octobre 2005 - Le correspondant veille au respect des obligations prévues par la loi du 6 janvier 1978 susvisée pour les traitements au titre desquels il a été désigné. A cette fin, il peut faire toute recommandation au responsable des traitements. Il est consulté, préalablement à leur mise en oeuvre, sur l'ensemble des nouveaux traitements appelés à figurer sur la liste prévue par l'article 47 [liste des traitements dispensés du fait de la désignation]. Il reçoit les demandes et les réclamations des personnes intéressées relatives aux traitements figurant sur la [liste]. Lorsqu'elles ne relèvent pas de sa responsabilité, il les transmet au responsable des traitements et en avise les intéressés. Il informe le responsable des traitements des manquements constatés avant toute saisine de la Commission nationale de l'informatique et des libertés. Il établit un bilan annuel de ses activités qu'il présente au responsable des traitements et qu'il tient à la disposition de la commission.
Article 50 du décret du 20 octobre 2005 - Le responsable des traitements peut, avec l'accord du correspondant à la protection des données à caractère personnel, lui confier les missions mentionnées à l'article 49 pour la totalité des traitements qui dépendent du responsable. Dans ce cas, la notification prévue à l'article 43 [notification à la CNIL] en fait mention.

4. Les mesures prises en vue de l'accomplissement des missions du correspondant

Préciser toute mesure prise en vue de l'accomplissement des missions du correspondant*
mesures d'ordre organisationnel (création d'un service dédié, modalités de remontée de l'information ...)

Officialisation de la fonction, déjà assurée en interne, par Monique Bureau……

formation (du correspondant, et des personnels...)

Formation correspondant Informatique et Libertés suivie les 18 et 19/01/2006 (organisée par Comundi).……

actions de communication interne (lettre d'information interne, diffusion de notes)

Information sur revue interne sur la création de la fonction CIL……

Sensibilisation des utilisateurs via l'intranet interne……

actions de communication externe (communiqués, information sur le site de l'organisme, brochures)

……

moyens humains et matériels (affectation de personnel, dotation d'un budget spécifique ...)

Assistance par un consultant Informatique et Libertés externe (10 à 15j/an)……

autres mesures/précisions éventuelles :

Réalisation d'une cartographie Informatique et Libertés des traitements en cours…….

Prise en compte des aspects CNIL dans la méthodologie INCAS (adaptée au contexte de l'entreprise) de prise en compte de la sécurité dans les projets informatiques…….

……

.

Suite sur papier libre [ ]

5. Les qualifications professionnelles du correspondant

Qualifications professionnelles en rapport avec les fonctions de correspondant*….
Lorsque le correspondant désigné est une personne morale, veuillez préciser les qualifications respectives de la personne morale et de la personne physique exerçant les fonctions de correspondant
(expérience/ diplômes/ formation)

- ***RSSI depuis juillet 1998***……
- ***Formation CIL suivie les 18 et 19/01/2006***……
- ***Formation Informatique et Libertés suivie en 1998***……
- ***Responsable de la centralisation des déclarations CNIL du groupe MAAF Assurances depuis 1999***……
- ***Formation « Maîtriser le régime juridique des fichiers de traitements informatique » en février 1999***…….
- ……
- ……

Suite sur papier libre [ ]

Les champs marqués par * doivent être obligatoirement renseignés

6. Les engagements

Pour le responsable de traitement :

[**X**] *Je certifie l'exactitude et la sincérité des renseignements fournis dans le présent formulaire.*

Nom, Prénom : .....

Fonctions l'habilitant à signer :.....

A ..***Niort***.....

Le :..... Signature :

Pour le correspondant à la protection des données à caractère personnel :

[**X**] *Je déclare accepter les fonctions de correspondant à la protection des données à caractère personnel telles que prévues par l'article 22 de la loi du 6 janvier 1978 et décrites dans les articles 42 à 55 du décret du 20 octobre 2005 pour les traitements mentionnés au 3. du présent formulaire.*
Cette désignation est : **[X] étendue [ ] générale [ ] partielle**

[**X**] *En cas de désignation étendue :*
J'accepte expressément l'extension de mes missions aux traitements soumis à autorisation ou avis de la CNIL.Cette extension n'emporte toutefois pas dispense de l'accomplissement des formalités de demande d'autorisation ou d'avis auprès de la CNIL.

Nom, Prénom du correspondant ou, si le correspondant est une personne morale, de son représentant légal :
BUREAU Monique..... .....

A ..***Niort***.....

Le.....

Signature :.....

Les informations recueillies à l'aide du présent formulaire sont destinées à la CNIL pour l'instruction du dossier et la gestion des relations entre la CNIL et le correspondant.
Les informations relatives au responsable de traitement, à la désignation du correspondant et à l'étendue de la désignation pourront être communiquées à toute personne en faisant la demande.
Les personnes concernées par le traitement de ces informations peuvent exercer leur droit d'accès et de rectification auprès de la CNIL, en écrivant au 21, rue Saint Guillaume - 75340 Paris cedex 07.

Annexes B

PROJET "EFFICACITE DES ANTI-VIRUS"