# Se prémunir contre les menaces provenant de ses propres employés

**Travail de diplôme réalisé en vue de l'obtention du diplôme HES**


par :

**Henrique MARQUES**


Conseiller au travail de diplôme :

**Gérard INEICHEN**

**Lieu, date de dépôt**


**Haute École de Gestion de Genève (HEG-GE)**

**Filière IGS**

# Déclaration

Ce travail de diplôme est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor en informatique de gestion. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de diplôme, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de diplôme, du juré et de la HEG.

« J'atteste avoir réalisé seul(e) le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 27 novembre 2008

Henrique Marques

# Remerciements

Je remercie tout d'abord Monsieur Gérard Ineichen qui m'a guidé tout au long de ce travail en me donnant de précieux conseils et chemins à suivre. Je remercie de même Yaya et Sónia Ouattara qui ont eu la gentillesse de vérifier l'orthographe et les tournures de phrase ainsi que Monsieur Pascal Lemonnier, ingénieur informaticien chez MIB S.A., qui a répondu aux quelques questions que j'ai posé afin de m'éclaircir sur certains points. Et enfin, je remercie toute la communauté des forums informatique qui, par son expérience, m'a aidé lors de certaines difficultés rencontrées.

# Sommaire

D'après plusieurs études menées par des spécialistes de la sécurité réseau, la majorité des attaques informatiques d'une entreprise proviennent de l'intérieur même de celle-ci. La raison est que de nos jours, tout employé doit avoir un accès constant à Internet, à sa messagerie et à des ressources sensibles. Ceci lui confère une énorme responsabilité dont il n'est pas toujours conscient ou sensibilisé. De par un acte de maladresse ou de malveillance, il peut être responsable d'énormes pertes pour l'entreprise pouvant compromettre sa viabilité.

Ce travail de diplôme s'adresse avant tout aux gérants d'entreprises de petite ou moyenne taille (PME). Sans être des experts en réseau, ils pourront appliquer des recommandations et procédures pour assurer une sécurité plus efficace et à moindre coût de leurs ressources informatiques face aux menaces provenant de leurs propres employés.

Dans un premier temps, nous décrirons les menaces et les vecteurs par lesquels celles-ci s'introduisent au sein d'un réseau d'entreprise. En effet, même si l'employé est le vecteur principal, il menace la sécurité des données par l'intermédiaire d'une technologie telle Internet ou la messagerie par exemple.

Les entreprises ne peuvent qu'entreprendre la mise en place de moyens techniques basiques tels qu'un firewall ou antivirus offrant une bonne protection du périmètre du réseau mais qui s'avèrent complètement inefficaces face aux attaques internes. C'est pour cela que dans un deuxième temps, nous mettons en évidence l'importance des mesures organisationnelles à instaurer pour sensibiliser chaque employé et des mesures techniques pour correspondre au mieux avec la politique de sécurité de l'entreprise.

Nous soulignons pour terminer l'importance de contrôler que la sécurité reste optimale et d'agir en cas de problème. C'est pour cela que nous avons développé une application qui permet, pour chaque poste de l'entreprise, de vérifier s'il correspond au niveau de sécurité souhaité.

# Table des matières

# Liste des Tableaux



# Liste des Figures

# Introduction

Indispensable à l'efficacité de toute entreprise, l'informatique est un domaine en perpétuelle évolution. Ainsi, le SII (Système d'Information Informatisé) doit être disponible à tout moment pour que l'entreprise puisse avoir l'avantage concurrentiel. Il en découle de nouveaux matériels informatiques, de nouveaux logiciels mais surtout un accès en permanence au web, cette gigantesque source de données accessible à tous. Tout cela provoque des failles que les pirates informatique n'hésitent pas à exploiter.

Lorsqu'on parle de pirate informatique, la plupart des gens ont l'image du jeune génie de l'informatique vivant à des milliers de kilomètres, cloisonné dans sa cave et essayant de dérober des données sensibles à de grosses multinationales pour son plaisir personnel. Et pourtant, une grande partie des attaques portées aux ressources informatiques des entreprises viennent de personnes bien plus proches : leurs propres employés.

# 1. Les entreprises et la sécurité

La plupart des entreprises n'ont pas une réelle conscience des menaces qui pèsent sur leur SII. Ne mettant pas en place une politique de sécurité, elles s'exposent aux attaques pouvant ainsi mettre en péril leur activité, voire leur survie selon le type de données dont il s'agit.

Cette méconnaissance du risque encouru est surtout visible dans les PME ou start-up. Elles pensent qu'elles n'intéressent pas les pirates informatiques du fait de n'être que de petites infrastructures ayant peu d'informations à voler. Pourtant, certains hackers s'introduisent dans des réseaux non pas pour y voler des informations importantes, mais seulement pour leur plaisir personnel pendant que d'autres se font la main sur de plus petites infrastructures avant d'en attaquer de plus grosses.

Pour avoir une vue d'ensemble plus concrète, analysons les résultats obtenus suite à une étude[1] menée en 2006 par le MELANI (La Centrale Suisse d'enregistrement et d'analyse pour la sûreté de l'information) en partenariat avec le Centre de recherche sur la politique de sécurité de l'EPFZ. L'enquête a été réalisée auprès d'entreprises de toutes tailles dans toute la Suisse et dans les secteurs secondaire et tertiaire (industrie et services). 4916 entreprises ont été contactées dont 562 ont répondu par e-mail ou par courrier à un questionnaire de 36 questions entre le 15 mars et le 13 avril 2006.

Les premières questions visaient à déterminer si l'entreprise avait été victime de menaces informatiques durant l'année 2005. Le résultat démontre que 72% des entreprises ayant pris part à l'enquête signalent avoir effectivement été attaquées. Le détail est disponible en Annexe 1.

L'enquête a aussi montré les risques d'incidents en fonction de la taille de la société comme démontré en Annexe 2. On peut voir dans ce graphique que même si les grosses entreprises sont les plus touchées par les attaques, les petites et moyennes n'en demeurent pas moins victimes.

Le questionnaire portait également sur des mesures techniques adoptées par les entreprises afin de se prémunir de ces attaques (anti-virus, pare-feu, anti-spyware, etc..). Une grande majorité (99,6%) dit utiliser au moins l'une de ces mesures pour se protéger.

---

[1] Source : « Sécurité informatique dans les entreprises suisses », Manuel Suter, Center for Security Studies, 2006

Concernant les mesures organisationnelles (Politique de sécurité, mis à jour des logiciels, formation du personnel), le graphique en Annexe 3 présente les résultats obtenus.  On peut clairement remarquer que la plupart des entreprises n'ayant qu'une petite infrastructure n'ont pas mis en place de mesures organisationnelles. Or, à quoi sert-il d'utiliser une solution antivirale ou un firewall si n'importe quel utilisateur interne a accès à toutes les données sur les serveurs ou si chacun peut télécharger des fichiers sur Internet sans aucune restriction.

Ceci renforce l'opinion des plus grands spécialistes en réseau qui soulignent que la majorité des attaques menées sur les ressources informatiques d'une entreprise proviennent de l'intérieur de celle-ci.

# 2. Les menaces

Nous allons décrire ici les types de menaces auxquelles une entreprise est exposée, résultant d'un mauvais comportement des employés et d'une infrastructure insuffisamment sécurisée pour s'en prémunir.

## *2.1 Les virus*

Selon Fred Cohen, créateur du premier virus informatique, « Un virus est un programme qui modifie d'autres programmes, afin d'y inclure une copie de lui-même ». Un virus est donc un petit logiciel qui se présente sous la forme d'un fichier exécutable (*.exe), d'une macro, d'un script, etc. afin de se reproduire et de contaminer le plus grand nombre de fichiers possibles. Une fois cette période d' « incubation » terminée, il s'exécute et réalise l'opération pour laquelle il a été conçu et qui peut être dévastatrice. En effet, non seulement un virus peut être nuisible à un PC (affichage étranges, ralentissement du poste, destruction de fichiers, reformatage du disque dur, etc.) comme il peut aussi contaminer d'autres postes via le réseau (local ou Internet). Chaque nouveau fichier contaminé devient à son tour une nouvelle source d'infection. Ces virus peuvent se classer selon six catégories :

- *Les virus de boot* se placent dans le secteur d'amorçage d'un disque qui, comme son nom l'indique, sera lu en premier lors du démarrage du PC. Le virus remplace le code qui se trouve à ces emplacements et prend le contrôle du poste.
- *Les virus d'application* ont comme mission de contaminer les fichiers exécutables en y insérant les instructions nécessaires à leur expansion et à leurs actions. Sont appelé des virus résidents ceux qui restent actifs en permanence dans la mémoire de l'ordinateur pour y contaminer toute application chargée et virus non-résidents ceux qui recherchent des fichiers correspondant aux critères qu'auront défini leur créateurs pour les infecter.
- *Les virus Bounty Hunter* attaquent l'anti-virus afin de le désactiver pour pouvoir opérer en tout sérénité.
- *Les virus furtifs* interceptent les appels au système d'exploitation en prenant le contrôle des interruptions. C'est-à-dire que quand l'anti-virus essaie de vérifier si le fichier est contaminé, le virus détecte l'interruption et renvoie une image saine de celui-ci à l'anti-virus qui n'y verra que du feu.

- *Les virus polymorphes* qui, pour échapper à l'anti-virus, change de signature après chaque infection en cryptant d'une façon différente leur code. L'anti-virus aura ainsi énormément de mal à détecter si le fichier est sain ou pas.
- Et enfin, les *macrovirus* sont des virus qui sont écrits en utilisant des langages de macro-commandes comme VBA Script par exemple (inclus dans la plupart des logiciels de bureautique tels que Word, Excel ou Outlook). Ces scripts servent normalement à automatiser le travail mais les pirates ont su les exploiter pour infecter des pièces jointes des e-mails par exemple et ainsi répandre le macrovirus très rapidement à travers le monde.

Les pirates n'hésitent pas à créer des virus qui appartiennent à plusieurs de ces catégories afin d'accroître le pouvoir destructeur de ceux-ci. Cependant, les virus ne peuvent se propager que par l'intervention d'un utilisateur. C'est pourquoi elle devient l'une des principales menaces internes sur lesquelles il faut porter une attention toute particulière.

## *2.2 Les vers*

Contrairement au virus, un ver est un programme autonome qui n'utilise pas de support pour se propager car il s'auto-reproduit au travers le réseau. Le ver se propage sans recourir à l'infection de fichiers sains et donc sans que l'utilisateur ait à exécuter un fichier contaminé. Ces vers se servent principalement de la messagerie pour se répandre en s'expédiant automatiquement aux adresses trouvées dans les carnets de contacts. Compte tenu du fait que le mail peut provenir d'une personne de confiance, l'employé aura beaucoup plus tendance à voir ce que contient la pièce jointe (un simple double clic sur celle-ci active le vers).

## *2.3 Les chevaux de Troie (Troyen)*

Tenant son nom du fameux cheval de bois dissimulant les guerriers grecs, cet importun est un logiciel dissimulé dans un autre programme ou fichier (utilitaire, jeux, audio-vidéo, etc.) qui tente d'ouvrir des ports TCP ou UDP sur le poste de l'employé. Ceci va lui permettre d'effectuer dans le plus grand secret des tâches comme la destruction de fichiers, le vol de données, etc. sans que l'utilisateur ne s'en rende compte.

## *2.4 Logiciels espions (Spywares)*

Le Spyware est un petit programme intégré à un autre ou s'installant au même moment que celui-ci à l'insu de l'utilisateur. Ce programme va par la suite recueillir des

informations personnelles telles les logiciels installés sur le poste, les sites visités, les fichiers enregistrés sur le disque dur, etc. et utiliser la connexion Internet de l'employé pour les envoyer à son créateur. Certains logiciels bien connus utilisent cette méthode pour pouvoir « profiler » les utilisateurs. Un type de Spyware est le Keylogger qui lui, va enregistrer secrètement les informations tapées au clavier pour envoyer au créateur de celui-ci. Certains n'enregistrent que les frappes soumises à certaines conditions (lorsqu'une session SSL est ouverte par exemple).

## *2.5 Les attaques*

Ici, nous exposons quelques attaques qu'un employé malveillant serait en mesure d'opérer en exploitant des failles de configuration, de logiciel ou même de l'OS au cœur même de l'entreprise pour des raisons de vengeance par exemple. Il est bien entendu impossible de recenser toutes les attaques auxquelles les ressources du réseau pourraient faire face, mais la plus significative est celle du déni de service.

Le déni de service est un type d'attaque qui a pour but de rendre indisponible ou de ralentir un service. La technique est de saturer la cible de requêtes (ICMP, TCP, etc.) afin de la submerger. Les principaux types d'attaques de déni de service sont :

- *ICMP flood* qui sature le réseau et les PC de requêtes ICMP qui permettent de faire un ping.
- *Smurfing* qui consiste à usurper l'adresse IP d'un autre poste et à envoyer sous cette fausse identité une requête à un grand nombre d'ordinateurs. En y répondant, ceux-ci provoquent la saturation de la bande passante et des ressources de la machine dont l'employé aura pris l'adresse.
- *Mail bombing* qui permet de rendre indisponible le système de messagerie. La technique est d'envoyer une multitude de courriels avec des pièces jointes afin de saturer l'espace disque du serveur messagerie et la bande passante de son accès à Internet.
- *Lock Flood* est une attaque qui va générer de multiples événements (tentatives d'accès, etc.) qui seront consignés dans les logs qui vont augmenter de taille et prendre énormément d'espace dans le serveur cible.

## 2.6 Le SPAM


Ce nom tient son origine d'une publicité américaine de pâté (Shoulder of Pork and hAM) des années 1930 dont le mot SPAM était répété maintes fois. Plus tard, les Monthy Pythons parodièrent cette annonce en utilisant à tout bout de champs ce mot ce qui lui permettra par la suite de rentrer dans l'histoire informatique.

En effet, le SPAM désigne l'envoi massif et souvent répété d'emails publicitaires à des personnes qui n'ont pas exprimé le souhait de recevoir ce type de messages. Le SPAM en lui-même n'est pas une menace mais il peut tout à fait contenir des virus ou autres. Compte-tenu de l'essor très important de ces « pourriels », la bande passante du réseau et l'espace disque du serveur mail en prennent un grand coup sans parler du temps que prennent les serveurs pour trier les bons e-mails du reste. Il faut savoir que le SPAM représente environ la moitié des e-mails échangés et certains pays dépensent des milliards pour lutter contre ce fléau.

## 2.7 L'ingénierie sociale

« Les mathématiques sont impeccables, les ordinateurs faillibles, les réseaux médiocres et les gens pires que tout »[2]. Bien que très souvent négligée, une des plus grandes menaces sécuritaires d'une entreprise est la psychologie humaine. Les hackers se servent de ce qu'on appelle l'ingénierie sociale (Social Engineering en anglais) pour accéder aux ressources de l'entreprise. Abusant de la naïveté ou de la confiance d'une personne, ils obtiennent des informations sensibles qui leur permettent d'attaquer par l'intérieur. Contrairement aux attaques citées plus haut, l'ingénierie sociale ne nécessite pas de dispositif particulier, la seule force de conviction est la clé de voûte de ce type d'attaque.

Pour se procurer ces informations, les hackers utilisent le téléphone, le courrier, Internet, des rencontres personnelles mais surtout l'e-mail. Ils obtiennent ainsi divers renseignements comme des informations sur le matériel, le réseau, les logiciels, des mots de passe et nom de session etc. En collectant diverses informations, ils tissent

[2] « Secrets et mensonges, Sécurité numérique dans un monde en réseau », Bruce Schneier, Vuibert Informatique, 2001

une véritable toile de données qui vont leur permettre d'investir en toute impunité les ressources réseau de l'entreprise tout en évitant d'être pris la main dans le sac par des firewalls, contrôle d'accès ou d'authentification.

En général, le hacker commence par se renseigner sur sa cible potentielle (le plus souvent un employé qui n'est pas dans le service informatique) en recherchant des informations basiques sur celle-ci comme le nom, prénom, statut, numéro de téléphone, etc. Par la suite, il téléphone ou envoie un e-mail à l'entreprise en essayant de joindre sa cible tout en ayant préparé un rôle et un discours au préalable (par exemple un problème technique survenu sur un serveur). Ayant gagné la confiance de l'employé, l'attaquant peut obtenir les informations désirées.

Une variante de ces attaques est la technique du Pishing ou hameçonnage. Celle-ci consiste à rediriger la personne qui ouvre un e-mail ou surfe sur Internet vers une page piégée demandant des informations telles un numéro de compte bancaire ou une authentification login/password. Le site en question étant la réplique parfaite de celui auquel l'employé pensait accéder, il n'hésite pas y informer les champs de saisie. Ces pages piégées peuvent de même introduire divers virus sur le poste. Internet Explorer 7 intègre dans son navigateur un filtre anti-hameçonnage qui permet de vérifier si la page est factice, ce qui est une excellente manière de se prémunir de ce fléau.

La meilleure façon de se prémunir contre l'ingénierie sociale consiste à sensibiliser ses employés. Il faut donc en faire une référence dans sa politique de sécurité (cf. point 4.1 « La politique de sécurité ») et organiser des formations obligatoires en mettant l'accent sur le fait de ne jamais divulguer un login ou mot de passe session par téléphone ou mail sans connaître personnellement la personne.

# 3. Les vecteurs de menaces

Tout comme un voleur a plusieurs alternatives pour entrer dans une maison afin de la cambrioler, un virus ou autre a plusieurs vecteurs par lesquels passer pour semer la terreur. Cependant, l'employé, que ce soit involontaire ou par malveillance, est toujours le principal responsable de la concrétisation des menaces citées. Voici une classification des vecteurs par lesquels le danger peut venir et quels types de menaces rôdent sur les ressources informatiques de l'entreprise par l'utilisation de celles-ci :

Tableau 1 : Menaces selon les vecteurs

| Vecteurs | Menaces |
|---|---|
| Navigation Internet | Du fait de naviguer sur des sites douteux ou faire des téléchargements, l'employé peut introduire des *Virus, Vers, Chevaux de Troie ou Spyware.* |
| Messagerie | Ouvrir des pièces jointes ou cliquer sur un lien dans un message provenant d'un expéditeur inconnu peut provoquer des *Virus, Vers, Chevaux de Troie ou Spyware*. De plus, le *SPAM* incrémente le pouvoir de cette menace. |
| Branchement d'un PC personnel | Un ordinateur portable inconnu qui se branche dans le parc informatique de l'entreprise peut contenir des *Virus, Vers, Chevaux de Troie ou Spyware*. |
| Logiciels Personnels | Beaucoup d'employés aiment utiliser leurs propres logiciels. Des *Virus, Chevaux de Troie ou Spyware* peuvent très bien s'y cacher. |
| Médias amovibles | A l'ère du média amovible, les *Virus, Vers* |

| | |
|---|---|
| | *Chevaux de Troie et Spyware* sont à la fête. Les employés branchent leurs clés USB, IPod ou disques externes sans même imaginer ce qu'il peut contenir. |

Il y a aussi des menaces dont le seul vecteur est l'employé lui-même. Par maladresse ou malveillance, il peut affecter la sécurité des données de l'entreprise.

| | |
|---|---|
| Employé | Un employé ayant un mot de passe peu robuste ou étant victime d'*Ingénierie Sociale* peut laisser la porte ouverte aux ressources de l'entreprise. Aussi, un employé mécontent qui veut se venger pourrait établir des *Attaques* sur le réseau depuis l'intérieur. |

# 4. Mesures organisationnelles

Comme on a pu le remarquer dans le premier chapitre de ce travail dénommé « Les entreprises et la sécurité », il est inutile de mettre en œuvre des mesures techniques si par derrière, chaque employé ayant un accès aux ressources n'a pas conscience des énormes responsabilités qui en découlent. La sensibilisation et la formation des employés sont une démarche essentielle pour mener à bien la lutte contre les menaces internes.

## *4.1 La politique de sécurité*

Une politique de sécurité définit des axes à suivre et les règles que tout le monde doit respecter afin d'assurer la sécurité des ressources du réseau. Elle doit être d'une forme aussi simple que possible pour que tout un chacun puisse la comprendre et l'adopter. L'objectif de cette politique est d'énoncer des résultats attendus et non des moyens par lesquels les obtenir car c'est à partir de cette politique qu'une architecture, des procédures et des outils sont mis en place pour répondre aux objectifs de sécurité de l'entreprise. C'est pour cela qu'une politique de sécurité peut rester similaire au fil des années malgré les avancées technologiques. Il est tout de même conseillé de faire une revue générale tous les deux ans afin de recadrer la politique avec les nouvelles mesures de l'entreprise. Le sujet de ce travail étant les menaces internes, la politique de sécurité sera de même portée sur les règles et processus afin de se prémunir de ce type de menaces.

Cette politique de sécurité inclut une charte qui précise et engage la responsabilité des employés. Pour les PME d'une dizaine d'employés, une charte est suffisante pour assurer un bon niveau de sécurité. Bien entendu, cette charte devra être signée par les personnes concernées pour que l'engagement soit bien réel. Elle a plutôt un rôle de prévention et d'éducation des employés et non de répression. Ceci risquerait fortement de provoquer des réactions négatives et par conséquent de faire que les employés ne prêtent aucune attention à la politique de sécurité.

Même si cette charte ne joue pas un rôle d'outil de sécurité, elle permet de fixer un cadre légal et de bons usages des ressources de l'entreprise optimisant ainsi le rôle des outils matériels et logiciels qu'il faudra mettre en parallèle.

Pour rédiger une bonne charte concernant les menaces internes, ainsi que le propose P. Holbrook et J. Reynolds[3], l'on doit se poser les questions suivantes pour chaque vecteur cité plus haut :

- Qui est autorisé à utiliser les ressources informatiques ?
- Quelles sont les utilisations normales de ces ressources ?
- Qui est autorisé à donner des droits aux autres utilisateurs ?
- Qui doit avoir les privilèges d'administrateur ?
- Quels sont les droits des utilisateurs et leurs responsabilités ?
- Quels sont les droits des administrateurs et leurs responsabilités ?

La partie la plus difficile, une fois la politique et/ou la charte mise en place, est de la faire respecter. Il faut pour cela mener une campagne d'information et de formation de ses employés (typiquement une formation pour lutter contre l'ingénierie sociale). Cette politique est la pierre angulaire de la sécurité réseau de l'entreprise. Attirer l'employé en faisant une campagne amusante et intéressante afin que le message passe plus facilement est donc vivement recommandé. Une bonne propagation de la politique de sécurité au sein de l'entreprise permet de se protéger au mieux contre les menaces internes et d'éviter la cyber-surveillance abusive.

## *4.2 La Cyber-Surveillance*

Une charte de sécurité n'est pas obligatoire au sein de l'entreprise du moment que celle-ci ne met pas en œuvre des logiciels pouvant porter atteinte à la vie privée de l'employé. Par contre, si elle veut installer des logiciels de surveillance des employés concernant l'utilisation des outils informatiques ou même des journaux de log, il faut obligatoirement prévenir ceux-ci en le mentionnant dans la charte.

Si cela n'est pas mentionné, il peut y avoir de graves conséquences au niveau pénal. En effet, une surveillance abusive des employés peut les amener à intenter une action en justice pour atteinte à la personnalité (cf. art. 15 et 25 LPD), pour violation de l'interdiction de surveiller le comportement des employés (cf. art. 59, al 1, lit. a de la loi sur le travail, LTr, RS 822.11), ou même pour soustraction de données personnelles (cf. art. 179novies CP).

Des applications ou matériaux informatiques utilisés, même s'ils n'ont pas une vocation à surveiller les actions des employés, conservent cependant dans leur log un certain

[3]Source : RFC 1244 Site Security Handbook dans son point 2 (http://www.ietf.org/rfc/rfc1244.txt)

nombre d'informations. Typiquement les logiciels de gestion de travail en groupe comme Lotus Notes ou Microsoft Exchange consignent qui fait quoi, quand et avec qui dans les agendas partagés. Ou même les firewalls ou proxy qui enregistrent également un certain nombre d'informations comme les tentatives d'accès à tel ou tel site, les heures de connexion, etc. Alors que d'autres sont conçus spécifiquement pour la surveillance des postes ou des applications comme les logiciels de contrôle d'accès à Internet ou d'analyse de messagerie, etc.

Il convient donc d'être en règle avec la loi en consultant par exemple le « Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail »[4].

[4] Uhttp://www.edoeb.admin.ch/themen/00794/01124/01125/index.html?lang=frU

# 5. Mesures techniques

Il y a des millions de manières différentes de mettre en œuvre une politique de sécurité. Ce n'est pas en installant un antivirus et un pare-feu que les données seront suffisamment protégées. Nous tenterons ici d'exposer les façons les moins onéreuses, les plus faciles et efficaces possibles d'implanter différentes mesures techniques afin de protéger au maximum l'entreprise des menaces internes selon les vecteurs cités plus haut.

## *5.1 Utilisation d'Internet*

L'usage non-professionnel d'Internet au sein de l'entreprise augmente considérablement au fil des années. Il s'agit notamment de la visite de sites communautaires, sites de vidéos et autres. D'ailleurs, la majorité du temps passé sur Internet est dans un but purement personnel. Cela baisse évidemment la productivité de l'entreprise mais surtout augmente le risque de contamination des postes par la navigation sur des sites douteux qui pourraient contenir des éléments à télécharger cachant un virus ou autre. Des mesures doivent être prises à ce niveau pour éviter au maximum que l'employé accède à ce genre de page Internet.

### 5.1.1 Le proxy

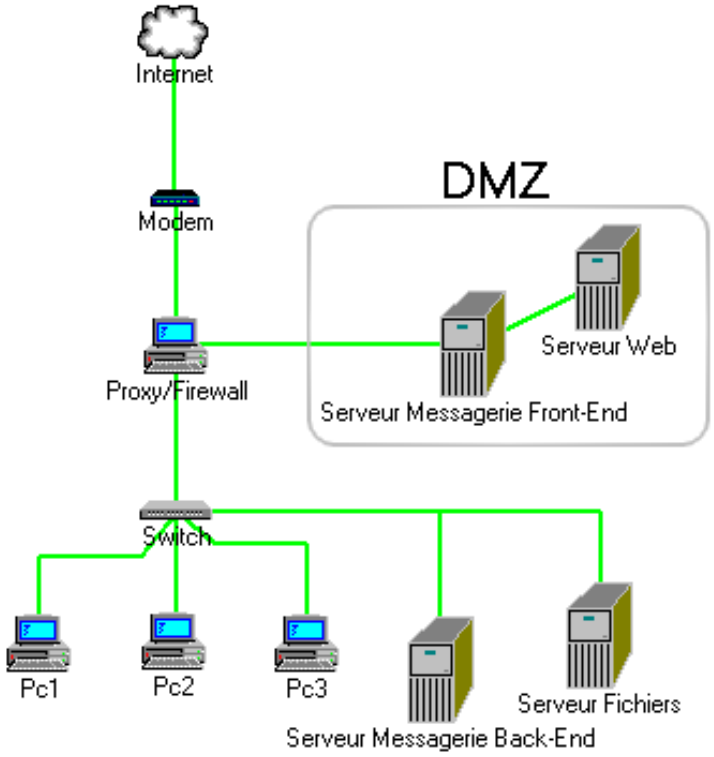
La meilleure façon de gérer les connexions à Internet depuis un poste interne est d'utiliser un serveur mandataire, plus communément appelé un proxy. Lorsque l'employé voudra se connecter sur Internet à l'aide d'un browser qui sera configuré pour utiliser ce proxy, celui-ci va se connecter d'abord au serveur proxy et lui relayer sa requête HTTP. Le proxy se connecte alors au serveur web demandé et lui transmet la requête. Le serveur web donne ensuite sa réponse au proxy qui va à son tour la transmettre à l'employé. Ce système permet de cacher la structure interne aux yeux du monde extérieur, de n'exposer qu'une seule adresse IP du fait que tous les postes communiquent avec ce proxy mais aussi de ne pas divulguer d'informations sur les postes. S'ajoute à ces fonctions un disque dur pour que le proxy puisse mettre en mémoire cache les pages dernièrement consultées. Ceci va permettre aux employés d'accéder très rapidement à ces pages déjà consultées (en général, un employé consulte toujours les même pages lorsqu'il s'agit de navigation professionnelle) et de réduire ainsi l'utilisation de la bande passante vers Internet et les délais d'affichage. Il faut par contre que le proxy compare régulièrement les données stockées en cache avec les données distantes afin d'être à jour.

La fonction qui nous intéresse principalement ici est le filtrage des connexions à Internet. Étant donné que ce proxy est le point de passage obligatoire pour toutes les demandes de connexion, on peut assurer un suivi en enregistrant les requêtes HTTP des employés. Le proxy va ainsi analyser cette requête et l'autoriser ou la refuser selon un de ces types de filtrage :

- La liste blanche qui définit les seuls sites autorisés à être consultés
- La liste noire qui définit les sites prohibés à la consultation
- Le filtrage de contenu qui gère la connexion selon la réponse du serveur demandé conformément à une liste de critères (typiquement des mots-clés).

Le plus efficace est de mettre ce proxy sur une machine dédiée (un ordinateur) entre le réseau interne et le réseau externe.

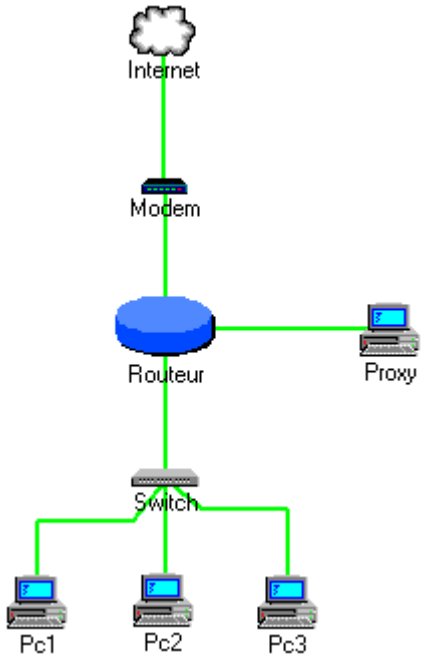
Figure 1 : Architecture proxy total




Pour cela, deux architectures sont envisageables. Cette première définit que le proxy, couplé avec le firewall, se trouve entre le switch et le modem ce qui fait qu'absolument tout ce qui veut accéder à Internet devra d'abord passer par ce proxy sans exception. Les serveurs en zone démilitarisée (DMZ)[5] sont eux aussi liés au proxy.

[5] La DMZ est une zone isolée par un firewall qui contient tous les serveurs dont les utilisateurs ont besoin d'un accès depuis l'extérieur (la messagerie ou le site web par exemple). La sécurisation n'y est cependant pas suffisante pour y stocker des informations sensibles.

Figure 2 : Architecture proxy partiel




Cette architecture-ci permet quant à elle de faire en sorte que certains protocoles, certains PC, etc. puissent aller sur Internet sans avoir à passer par le proxy (si on veut par exemple que les requêtes HTTP d'un PC administrateur ne soient pas relayées vers le proxy). Le proxy ne fait pas office de firewall ici donc il faut en installer un à part soit sur le routeur, soit sur une machine dédiée.

Une solution proxy très intéressante est Jana Server qui est un proxy gratuit, performant et s'installant justement sur un PC qui sera lui connecté à Internet. Ce proxy intègre, entre autres, un moniteur d'évènements et des logs pour voir sur quels sites les employés ont surfé ainsi qu'une administration à distance. Le téléchargement est disponible sur cette page :

http://www.janaserver.de/start.php?lang=en&menue=download

Un tutoriel extrêmement simple sur la configuration du proxy et des postes clients pour que chaque application assure que la connexion au web se fasse à travers le proxy est disponible à l'adresse suivante :

http://www.informatique-facile.net/dossiers/dossier_10_partager+votre+connexion+internet+avec+jana+server.html .

### 5.1.2 L'antivirus

Outre la mise en place de ce proxy pour bloquer l'accès aux sites dangereux et ainsi éviter que l'employé ne télécharge des virus, il est indispensable d'installer un antivirus sur chaque poste dont le PC qui fait office de proxy.

Les antivirus fonctionnent, pour la plupart, par contrôle de signatures. Lorsque l'antivirus scanne les fichiers avant utilisation ou lors d'une vérification du contenu du disque dur, il vérifie que la signature du virus n'est pas présente dans sa base de données dans laquelle sont stockées toutes les signatures de chaque virus référencé. La signature est une suite d'octets qui caractérise de façon unique le virus. Si cette signature est présente dans la base, le virus est alors soit supprimé, soit mis en

quarantaine selon ce que désire l'utilisateur. L'inconvénient de la méthode est qu'il est impossible de détecter de nouveaux virus ou une mutation d'un virus déjà référencé. C'est pour cela que l'antivirus doit être mis à jour très régulièrement. D'autres méthodes comme la recherche dans les fichiers non pas d'une signature mais l'utilisation de fonctions caractéristiques des différentes familles de virus (envoi d'e-mails, exploitations de failles, etc.) ainsi que l'analyse du comportement du virus (augmentation de taille des fichiers par exemple) sont aussi intégrées dans certains moteurs.

L'on doit vérifier alors que l'antivirus répond à chacun de ces critères :

- Analyse des fichiers entrant sur les disques durs ainsi que des transferts ftp et p2p
- Mises à jour permanentes de la base de signatures pour prendre en compte les tous nouveaux virus
- Possibilité de programmer une analyse complète des postes à intervalles réguliers
- Facilité d'administration, de déploiement et de mises à jour
- Fonction permettant de détecter et supprimer tout troyen, spyware et vers
- Certification du type ICSA ou Checkmark qui assurent par divers tests que l'antivirus est très efficace
- Capacité d'analyser tout type de fichier même des *.zip ou *.rar
- Possibilité d'envoyer un fichier potentiellement infecté au laboratoire de l'éditeur via Internet pour l'analyser

Si ce n'est pas le cas, des solutions comme McAfee, Kasperky, Symantec, Sophos ou GData sont envisageables. Chacune d'elles remplit ces conditions avec toutefois quelques différences de performances. Pour se forger une bonne opinion, le mieux est de se rendre sur le site http://www.av-comparatives.org dans la section « *Comparatives* ». Cet organisme de comparaisons antivirus basé en Autriche est un des plus sérieux. Les personnes désirant avoir une comparaison entre tel ou tel antivirus les contactent par e-mail. Un rapport complet ainsi que les résultats des différents tests leur sont ainsi envoyés et sont disponibles sur le site. Les tests sont extrêmement rigoureux (la méthodologie complète est téléchargeable sur le site) et les

résultats sont donnés sous forme d'un pourcentage sur le nombre de virus, troyen, vers, etc. bloqués.

## *5.2 La messagerie*

Un des plus gros vecteurs de virus et autres logiciels espions est sans nul doute la messagerie. Le périmètre étant ici les menaces internes, nous traiterons alors d'un moyen pour éviter que les employés puissent ouvrir un e-mail contaminé qui affecterait les ressources informatiques de l'entreprise.

Il y a deux possibilités pour une entreprise de gérer la messagerie, soit elle possède son propre serveur interne de messagerie, soit c'est son fournisseur d'accès à Internet (FAI) qui gère toute cette partie. Dans le premier cas, il faut sécuriser le serveur afin d'éviter qu'il soit assailli par des virus et pourriels. Dans le deuxième, il faut juste s'assurer que le FAI gère correctement l'aspect sécurité.

### 5.2.1 Le serveur de messagerie interne

Il y a deux aspects à prendre en compte pour sécuriser le serveur de messagerie. Commençons par parler d'une solution gratuite pour lutter contre le SPAM puis d'un antivirus capable d'éradiquer tout vers ou autre.

#### *5.2.1.1 Lutter contre le SPAM*

La meilleure solution pour bloquer les SPAM est de le faire au niveau du serveur messagerie pour éviter d'envoyer au poste de l'employé des messages inutiles. Ainsi on permet de réduire l'utilisation de la bande passante mais surtout d'augmenter la sécurité car ce n'est pas l'employé qui fait le filtrage au moment de la réception (qui pourrait donc lire des messages qu'il ne devrait pas), mais bien le serveur qui, par des filtres élaborés, permet d'intercepter les pourriels le plus en amont possible. Cependant, une bonne configuration du logiciel de messagerie de l'employé est nécessaire au cas où le SPAM aurait cassé toutes les barrières.

La plupart des entreprises utilisant le serveur de messagerie Exchange Server de Microsoft, la meilleure solution est de se pencher sur les outils qui y sont proposés gratuitement et qui sont parfaitement efficaces.

Il faut, dans un premier temps, installer le service pack 2 pour pouvoir bénéficier de toute l'infrastructure anti-spam de Microsoft. Il est en général proposé automatiquement mais si ce n'est pas le cas, on le trouve sur le site de Microsoft[6].

L'infrastructure de lutte anti-spam Exchange Server repose sur trois niveaux[7] :

- **Le filtrage de connexion** est le filtrage le plus efficace car il empêche que le message indésirable entre dans le serveur. Ce filtrage va analyser pour chaque connexion SMTP[8] entrante sa probabilité qu'elle soit vecteur de SPAM et ainsi bloquer les connexions douteuses. Pour ce faire, il existe des listes rouges en temps réel (real-time block lists soit RBL[9]) qui répertorient des adresses IP connues pour être sources de SPAM. La procédure est simple; lorsqu'un hôte se connecte au serveur Exchange sur le port TCP 25 (celui utilisé par le SMTP), celui-ci envoie une requête de type DNS[10] avec l'IP de l'hôte qui se connecte au fournisseur de RBL. Le fournisseur de son côté vérifie dans sa base de données et répond par un code spécifiant si l'hôte figure sur une de ses listes. Le code de retour va donc traiter l'email selon sa valeur. Par défaut, tout code de retour est traité. Alors que le code 127.0.0.1 signifie que l'adresse IP de l'hôte ne figure pas dans une des listes et que donc la connexion est acceptée, les codes 127.0.0.2 (relais ouvert) à 127.0.04 (source de SPAM confirmée) vont bloquer la connexion SMTP au serveur Exchange. Un bon serveur de RBL est *sbl-xbl.spamhaus.org* de SpamHaus.

---

[6] http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=535BEF85-3096-45F8-AA43-60F1F58B3C40

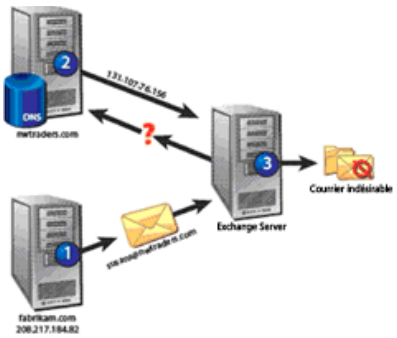
[7] Source : « Techniques de lutte anti-spam dans un environnement Exchange », www.microsoft.com, 2006

[8] SMTP (Simple Mail Transfer Protocole) est un protocole qui permet le transfert d'e-mails depuis le poste de l'employé vers le serveur de messagerie et entre serveurs de messagerie. Il s'occupe donc de transporter le message vers le serveur correspondant.

[9] Une RBL est une base de données où sont stockées les adresses IP connues pour être source de SPAM. Les entreprises fournissant des RBL surveillent en permanence Internet pour détecter les IP de spammeurs et les rajoutent à leur base dans différentes listes.

[10] Le Domain Name System permet d'établir une correspondance entre une adresse IP et un nom de domaine tel google.com. Ainsi, il nous suffit de taper www.google.com au lieu d'écrire l'adresse IP du site dans la barre URL.

Figure 3 : Filtrage de protocole



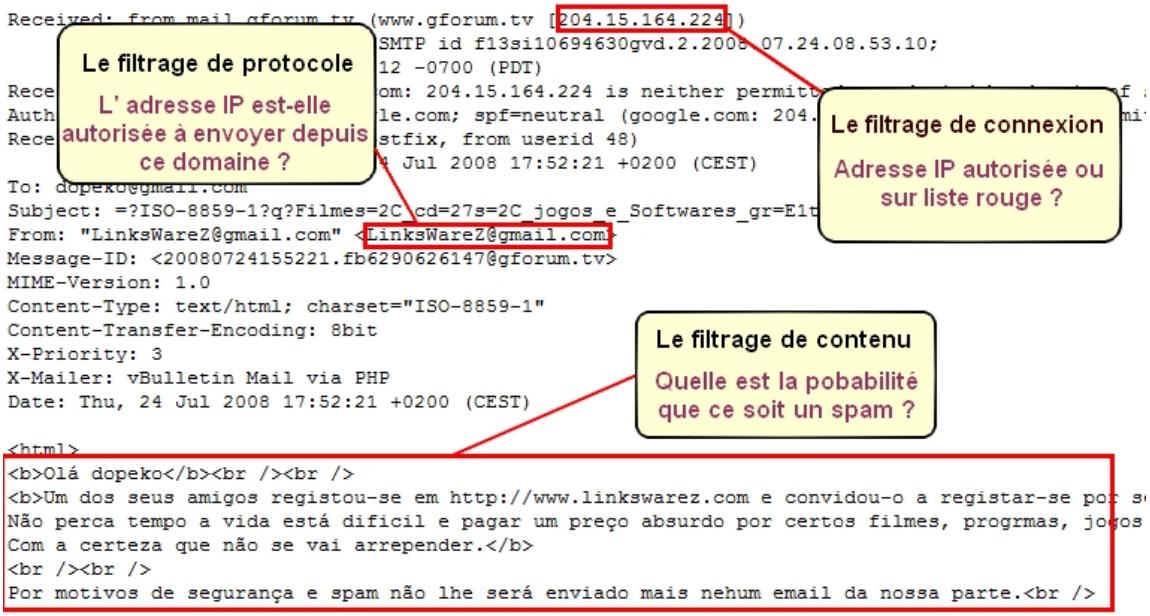

Source : Techniques de lutte anti-spam dans un environnement Exchange, www.microsoft.com

- **Le filtrage de protocole** est la deuxième couche de défense. C'est au niveau du protocole SMTP que le SPAM va être bloqué. Le filtrage tente de s'assurer que l'hôte qui envoie le message est autorisé à le faire en fonction du nom de domaine spécifié dans l'adresse (@hotmail.com par exemple). En effet, un expéditeur pourrait prendre le nom d'une organisation de confiance (banque, etc.) pour tromper l'employé afin de lui soutirer des informations vitales (cf. point 2.7 sur l'ingénierie sociale). C'est pour cela que l'environnement *ID de l'expéditeur* a été mis en place. Ce protocole valide l'origine de l'e-mail en tenant compte de l'adresse IP de l'expéditeur par rapport au propriétaire légitime du domaine expéditeur. Préalablement, il faut que l'entreprise chez qui le serveur vérifie l'adresse IP ait un enregistrement SPF (Security Policy Framework). Celui-ci liste les adresses IP autorisées à envoyer des e-mails depuis ce serveur. Lorsqu'on reçoit un e-mail, le serveur Exchange va interroger le serveur DNS sur l'enregistrement SPF du domaine en question pour vérifier si l'adresse IP de l'expéditeur est autorisée à envoyer des messages depuis celui-ci. Il est possible de définir une règle en cas d'échec de la vérification (supprimer, rejeter ou accepter le message). Le nombre d'organisations disposant d'enregistrements SPF étant important, cette technique est extrêmement efficace.

- **Le filtrage de contenu** est la dernière couche de protection. Il consiste à analyser le contenu du message pour trouver des indices permettant de voir si c'est un message indésirable. Sur les serveurs Exchange, le filtre de messages intelligents (IMF) a été créé afin de distinguer les messages légitimes du SPAM sur la base de millions de messages. Cette distinction se fait grâce à un suivi de plus de 500'000 caractéristiques des e-mails entrants. Ces caractéristiques sont basées sur la contribution volontaire des centaines de milliers d'abonnés au service Hotmail qui ont classé des millions d'e-mails selon qu'ils étaient du courrier légitime ou du SPAM. Si un spammeur envoie un message à un serveur disposant du IMF, celui-ci évalue le texte du message selon le filtre mis à jour bi-hebdomadairement et attribue à chacun d'eux un indice de niveau de confiance SCL (entre 1 et 9) stocké dans les propriétés du message en fonction

de la probabilité que ce soit un pourriel. Par la suite, selon la configuration des seuils de la personne qui s'occupe du serveur, le message sera soit bloqué au niveau du serveur, soit envoyé dans le dossier SPAM de l'application cliente, soit envoyé dans la boîte de réception de l'application cliente. Par exemple, si le SCL est supérieur à 6, alors le déplacer dans le dossier SPAM du logiciel de messagerie du poste client. Le pishing (cf. point 2.7 sur l'ingénierie sociale) est aussi traité de cette manière pour être éliminé.

Figure 4 : Exemple de SPAM




Pour configurer le serveur Exchange, l'on peut se rendre à cette adresse sous *Solutions* :

http://www.microsoft.com/france/technet/security/midsizebusiness/topics/serversecurity/fightingSPAM.mspx .

Comme dit plus haut, il faut de même bien paramétrer le logiciel de messagerie client pour que celui-ci traite le courrier qui atteint les postes des employés. C'est très souvent Outlook qui est installé sur les postes clients en adéquation avec le serveur Exchange. Il faut pour cela activer le mode Microsoft Exchange en mode cache[11] (des comptes du type POP3 ou IMAP pour une connexion à un serveur de messagerie externe sont aussi pris en compte par le filtre de courrier indésirable).

[11] Permet d'avoir une copie de la boîte aux lettres sur le PC. Cette copie permet un accès très rapide aux données et une mise à jour constante avec le serveur Exchange. Pour configurer Outlook afin de le prendre en compte :

UhttpU://office.microsoft.com/fr-fr/outlook/HP010223431036.aspxU

Outlook dispose de plusieurs fonctionnalités permettant au client même de gérer le courrier qui pourrait être indésirable. Dans un premier temps, il faut qu'Outlook soit mis à jour pour disposer de toutes ses fonctionnalités en allant sur le site d'Office Online :

http://office.microsoft.com/fr-fr/downloads/CD101995361036.aspx

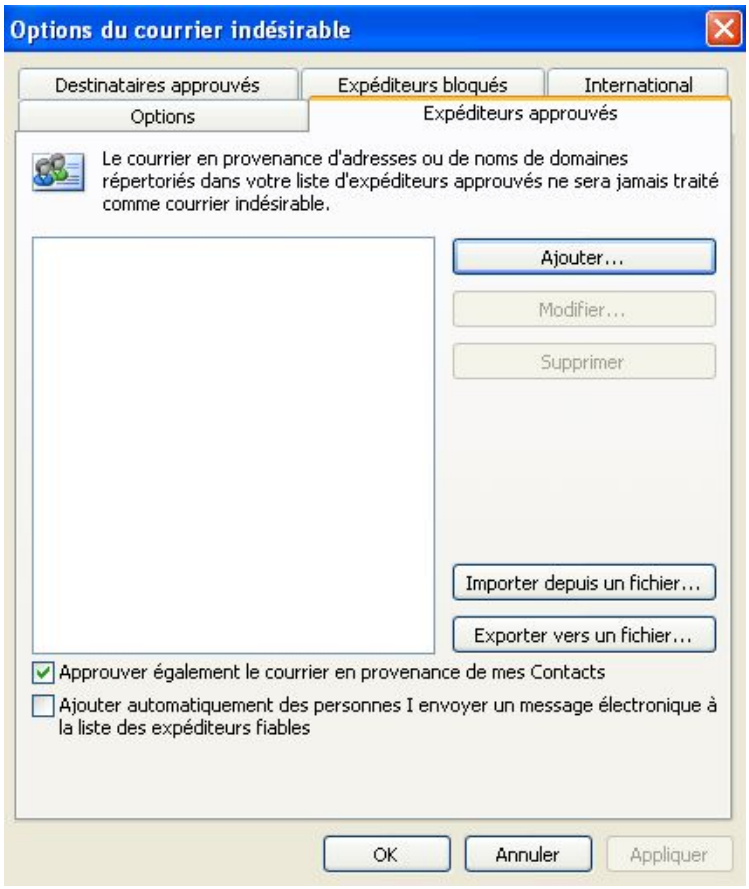
L'utilisateur dispose ainsi de la dernière version du filtre de courrier indésirable qui place automatiquement les messages jugés indésirables selon le contenu dans un dossier nommé « *Courrier Indésirable* ». A noter que dans un environnement tel que Windows Vista, le plugin Windows Update y est installé ce qui met à jour automatiquement tous les produits Office. Ci-dessous le lien pour télécharger ce plugin :

http://update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=fr

En allant dans le menu *Action* puis *Courrier Indésirable,* il est possible de changer les options de celui-ci. Il y a différents niveaux de protection. Les plus recommandés sont *Faible* et *Élevé*. Si on choisit le niveau faible (par défaut), une partie du courrier indésirable sera interceptée et donc l'employé en recevra tout de même quelques uns. L'avantage ici est qu'il ne risque pas de voir des messages « non-indésirables » passer dans le dossier du courrier indésirable. Le niveau Élevé quant à lui bloque la quasi-totalité. Il faudra par contre faire attention à vérifier dans le dossier du courrier indésirable pour s'assurer qu'aucun message « non-indésirable » ne s'y est glissé.

Même si le filtre bloque les messages de manière automatique, il peut aussi être intéressant de mettre en place une liste d'expéditeurs ou de domaines autorisés ou bloqués.

Figure 5 : Fenêtre Outlook du Courrier Indésirable




En cochant la case *Approuver également le courrier en provenance de mes Contacts,* tous les contacts de votre carnet d'adresse seront vus comme expéditeurs approuvés. Une liste d'expéditeurs bloqués peut aussi être mise en place selon le même système. Il est aussi possible d'ajouter un expéditeur ou domaine dans la liste des approuvés ou même des bloqués en faisant un clic droit sur le message puis *Courrier Indésirable.* L'onglet *International,* lui, permet de bloquer des emails étrangers selon le pays de provenance ou de l'encodage de l'email.

Quelle que soit la configuration du seuil SCL fait au niveau du serveur et du filtre de courrier indésirable, les expéditeurs des listes approuvées iront dans la boîte de réception du moment que le message a passé le filtrage de connexion et de protocole.

#### *5.2.1.2 Le relais ouvert*

Le relais ouvert est une configuration du serveur de messagerie qui permet au spammeur de l'utiliser comme plateforme pour ses activités. Il envoie à ce serveur un message qui sera destiné à des milliers de destinataires dans des domaines différents. Ce serveur configuré en relais ouvert ne s'assure donc pas que le courrier en provenance de l'extérieur lui est bien destiné et encore moins si les messages envoyés

proviennent bien des employés de l'entreprise. Ceci va provoquer des temps de réponse très longs, causer du désagrément aux destinataires et provoquer le risque de se retrouver sur la liste des spammeurs (la blacklist) si des gens mal intentionnés utilisent le serveur. Pour vérifier si un serveur Exchange est un relais ouvert et pour le désactiver, l'on peut suivre les instructions sur :

http://support.microsoft.com/kb/324958/fr.

#### *5.2.1.3 L'antivirus pour serveur de messagerie*

Concernant la protection des virus, il est préférable d'avoir un éditeur d'antivirus différent sur chaque point névralgique du réseau (serveur fichiers, serveur messagerie, postes, etc.) afin d'augmenter la probabilité qu'un éventuel virus soit stoppé au plus tôt puisque chaque produit propose des stratégies différentes d'analyse sur des bases de signatures propriétaires. De plus, si un des antivirus cesse de fonctionner, les ressources du réseau ne seront pas totalement à découvert.

L'antivirus au niveau du serveur de messagerie est extrêmement important. C'est pourquoi il est conseillé d'avoir recours à des solutions très performantes mais payantes plutôt qu'à des antivirus gratuits n'offrant pas une protection optimale. L'investissement sera parfaitement amorti au long des années car il aura permis d'éradiquer une grosse partie des menaces internes.

Il y a deux antivirus très utilisés qui ont été développés dans le but de protéger le serveur Exchange de tout virus, vers, spyware, troyen ou exploitation d'une faille de l'OS ou logicielle. Ces deux solutions offrent une intégration optimale sur l'environnement Exchange car étant conçues spécifiquement pour celui-ci. D'un côté on a Forefront Security de Microsoft et de l'autre, GFI Mail Security.

Chacune de ces solutions antivirales intègrent plusieurs moteurs antivirus différents qui scannent tout le courrier entrant. Ainsi, lorsqu'un virus émane, il y a beaucoup plus de probabilités que celui-ci soit détecté très rapidement car l'antivirus sélectionne automatiquement la combinaison optimale de moteurs. Chacun d'eux étant différent, tel ou tel sera plus rapide et plus à même de détecter tel ou tel virus. De plus, un moteur peut très bien être en train de se mettre à jour sans pour autant préjudicier la sécurité du serveur. D'ailleurs, l'antivirus va mettre à jour automatiquement chaque moteur en allant piocher sur les sites propriétaires les toutes dernières bases de signatures. Ceci est un aspect qui démarque ces deux antivirus de la concurrence.

Forefront utilise entre autres les moteurs de Kaspersky Labs, Norman Data Defense, Sophos et VirusBuster, et GFI les moteurs de BitDefender, Norman Virus Control,

Kasperky Labs, AVG et McAffee. Tous ces moteurs sont certifiés et reconnus dans le milieu de la sécurité informatique.

De son côté, GFI Mail Security gère la détection de troyens en détectant en temps réel ce que pourrait faire l'exécutable et compare ses actions (accès au carnet d'adresses par exemple) à une base de données d'actions malicieuses. Il nettoie de même tout code de script au sein d'un email (qui pourrait déclencher un vers) avant de l'envoyer au poste de l'employé et il détecte tout spyware grâce à une base de données de logiciels espions. Cette solution offre aussi la possibilité de surveiller en temps réel ce qui a été mis en quarantaine (un fichier qui a une possible infection) pour voir ce qu'on désire en faire. Bien entendu, une administration est possible depuis n'importe quel poste ayant Internet. Le téléchargement de ce produit et les prix sont disponibles à l'adresse suivante : http://www.gfsfrance.com

Forefront Security offre les mêmes services mais par contre ne permet que de détecter les vers grâce, toujours, à une comparaison avec une liste de vers connus mais sans s'occuper ni des troyens ni des spywares.  Ceci est la grande différence entre ces deux antivirus. C'est pourquoi GFI Mail Security nous semble plus indiqué car il est attesté chez les plus grands certificateurs d'antivirus comme ICSA Labs et  Westcoast Labs, et ne nécessite pas l'installation supplémentaire d'un anti-spyware et troyen sur le serveur de messagerie.

### 5.2.2 Le serveur de messagerie externe

Si l'entreprise par contre fait confiance à un FAI pour la gestion de la messagerie, il faut s'assurer celui-ci gère convenablement la sécurité de son serveur de messagerie et utilise une technologie anti-spam performante. Téléphoner ou visiter le site Internet du fournisseur permettra d'avoir des renseignements sur ce sujet. Voici les quelques points essentiels à vérifier :

- Un antivirus performant sur les serveurs messagerie mis à jour très régulièrement
- Un filtre anti-spam Bayésien (filtre qui s'adapte automatiquement selon des mots-clés) et/ou Blacklist (contient les adresses des serveurs de spammeurs)
- Un filtre permettant de vérifier l'existence du serveur de messagerie qui est censé avoir émis le message
- Une analyse du titre et du corps du message pour déceler le SPAM en fonction de certains mots-clés

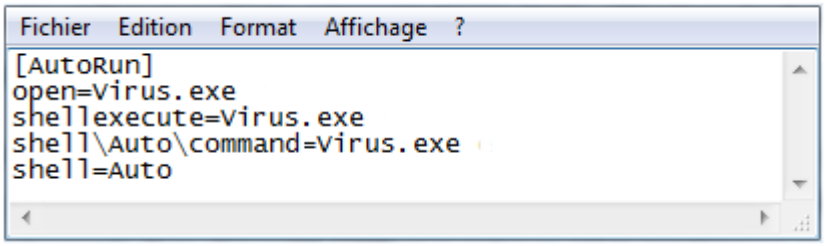
Il faut aussi prendre en compte la configuration du client Outlook comme vu plus haut afin de se prémunir le plus efficacement possible du courrier indésirable.

## 5.3 Les médias amovibles

Les clés USB, les disques dur externes, les CD/DVD ou même le lecteur de musique mp3 sont aussi une menace pour la sécurité informatique de l'entreprise. Dès que l'employé branche un de ces périphériques sur un port USB ou insère le CD dans le lecteur, un petit programme peut se lancer et mettre à mal les ressources de l'entreprise.

Pour éviter ce genre de désagrément, il suffit de désactiver l'autorun de ces périphériques. L'*autorun.inf* est un fichier inséré dans la clé USB par exemple qui détermine que faire à l'ouverture du périphérique. Si ce fichier n'existe pas, c'est l'explorateur Windows qui s'ouvrira. Ceci est surtout utilisé dans les CD pour installer automatiquement tel ou tel programme. Bien entendu, le dispositif peut contenir un virus, un spyware ou troyen désigné dans l'autorun pour le lancer automatiquement. Voici un exemple d'autorun d'un périphérique infecté :

Figure 6 : Exemple de fichier d'autorun




En double-cliquant sur le volume de la clé USB par exemple, Windows va chercher à exécuter « Virus.exe » qui infectera le poste de l'employé. Si par contre « Virus.exe » a été détecté par l'anti-virus et supprimé, cet autorun pointera vers un fichier inexistant et le double-clic sur le périphérique ne fonctionnera plus (la simple suppression du fichier *autorun.inf* résout ce problème).

Nous proposons donc d'utiliser le fichier « noAutorun.reg »[12] pour désactiver, grâce aux droits administrateurs, toute détection du fichier autorun.inf sur le poste, puis de redémarrer celui-ci (pour le réactiver, utilisez « okAutorun.reg »[13]).

[12] Code source en Annexe 4 sous noAutorun.reg

[13] Code source en Annexe 4 sous okAutorun.reg

Un autre phénomène appelé Pod Slurping que l'on peut traduire par « IPod qui aspire », permet à n'importe qui de récupérer toutes les informations d'un poste par le seul branchement d'un dispositif USB sur celui-ci. Une expérience a été menée par Abe Usher afin de démontrer aux responsables réseaux le danger encouru. Ce consultant spécialiste dans la sécurité réseau a créer une application nommée « slurp.exe » qui a pour but justement de copier en quelques secondes toutes les données d'un poste vers un dispositif USB de façon automatique. Il a imaginé le scénario dans lequel une personne malveillante (qui pourrait donc être un salarié) profiterait de la pause de midi pour brancher son IPod dans un poste sur lequel il désire acquérir toutes les informations contenues. Il a pu ainsi, en 65 secondes, copier l'intégralité du PC. S'il disposerait d'une heure, il pourrait facilement acquérir 20'000 fichiers sur une douzaine de postes. Le but de cette expérience a été de faire prendre conscience aux entreprises des risques liés aux dispositifs amovibles.[14]

Plus classique, un virus lancé à partir d'un périphérique externe peut se propager et ainsi infecter un grand nombre de ressources.

Se prémunir de ces menaces va dépendre de la gestion des comptes des employés de l'entreprise. Soit il y a une gestion locale, c'est-à-dire un compte utilisateur et un compte administrateur sur chaque poste. Ceci est la configuration classique lors de l'installation de Windows. Soit il s'agit d'une gestion centralisée qui est utilisée grâce à des serveurs faisant tourner des environnements tels Active Directory. Le premier cas est surtout employé dans les entreprises n'ayant que très peu de PC et d'employés voulant se connecter sur ceux-ci. Une gestion centralisée des identifiants et authentifiants de chaque personne ne serait pas utile. Alors que la deuxième possibilité, elle, devrait être mise en place pour gérer un parc informatique plus grand et où il serait intéressant de pouvoir tout gérer à partir d'un seul endroit.

Nous allons donc détailler ici, en plus de la désactivation de l'autorun, une bonne technique pour éviter au maximum le branchement sauvage et parfois dangereux de périphériques externes selon les deux cas de figure.

---

[14] Source : « *Quand l'IPod se prend pour un aspirateur à fichiers* », Emmeline Ratier, Uwww.jounaldunet.comU, 2006

### 5.3.1 Gestion locale des comptes des employés

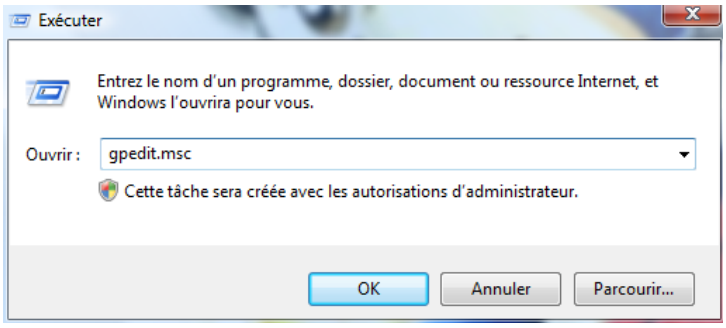
S'il est définit dans la politique de sécurité qu'aucun dispositif externe ne peut être utilisé sur les postes de l'entreprise, le plus simple reste de passer sur chaque PC, de se connecter en tant qu'administrateur, et de suivre ces instructions :

- Pour les périphériques USB, il s'agit de changer une valeur dans la base de registre Windows permettant de désactiver leur détection. Il suffira de copier sur le bureau le fichier « noUSB.reg »[15] et de cliquer dessus pour que tout dispositif externe soit ignoré. Pour finir, il faut redémarrer le PC afin que les changements sur la base de registre soient pris en compte (pour réactiver la détection, cliquer sur okUSB.reg[16])
- Pour bloquer la détection de CD ou DVD, la meilleure solution est décrite à la page 31

Ces solutions ne sont cependant pas idéales. Ces médias amovibles étant très pratiques et couramment utilisés, il est souvent préférable de contrôler leur utilisation au lieu de les bannir.

Pour cela, les environnements Windows XP et Windows Vista permettent d'accéder à une console d'édition de stratégies de groupe locale. Celle-ci va permettre de mettre en place des restrictions d'utilisation de Windows et de ses composants principaux par rapport aux utilisateurs sans avoir à manipuler la base de registre. Sur chaque poste que l'on veut appliquer des règles de restriction et avec les droits administrateur, il faut aller sur l'exécuteur et taper :

Figure 7 : Commande pour console GPO




Aller ensuite dans *Configuration de l'ordinateur - Modèles d'administration – Système – Installations de périphérique - Restriction d'installation de périphériques,* diverses

[15] Code source en Annexe 4 sous noUSB.reg

[16] Code source en Annexe 4 sous okUSB.reg

stratégies ou GPO (Group Policy Object) sont alors possibles. Etant des stratégies dans le dossier Configuration de l'ordinateur, ces GPO seront activées sur l'ordinateur quel que soit l'employé qui s'y connecte. Chacune d'elles offrent trois options (non-configuré (par défaut), activé, désactivé).

Si l'on désire bloquer l'installation de nouveaux périphériques, que ce soit USB, CD/DVD ou autres mais en laissant le droit à la session administrateur de le faire, il faut activer la stratégie *Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie* puis activer la stratégie *Autoriser les administrateurs à passer outre les stratégies de restriction d'installation de périphérique.* Ainsi, en se connectant en tant qu'administrateur sur un poste et installant les pilotes d'une clé, l'employé pourra utiliser cette dernière sur l'ordinateur en question.

Pour une gestion plus fine des périphériques, il est important de connaître le processus mis en œuvre par Windows pour installer un nouveau périphérique[17]. Chacun d'eux possède deux identifiants :

- Une classe d'installation qui définit la classe (possédant un numéro d'identification GUID et un nom) dont le périphérique est membre. Cette classe regroupe tous les appareils du même type (USB, Bluetooth, CD-Rom, Floppy Disk, etc. cf. : http://msdn.microsoft.com/en-us/library/ms791134.aspx).

- Une ou plusieurs chaînes d'identification qui sont définies par le constructeur lors de sa fabrication. Ces mêmes chaînes se retrouvent sur le PC dans un fichier « *.inf » faisant partie du package de pilotes. Lorsqu'on branche un périphérique sur le port USB ou autre, celui-ci envoie ses chaînes au système d'exploitation qui recherche le package de pilotes possédant la ou les mêmes chaînes pour installer les pilotes correspondants.

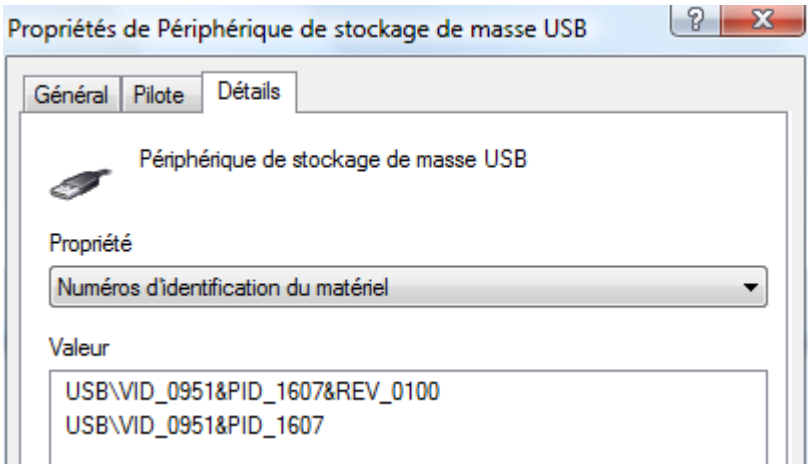
Ce qui nous intéresse ici, c'est plutôt l'installation de périphériques USB puisque les lecteurs de CD/DVD sont de toute façon déjà installés sur chaque poste (à la page 31, une autre GPO permettant de bloquer l'accès en lecture aux CD ou DVD est expliqué). Nous allons donc nous pencher sur la stratégie permettant de faire une restriction des périphériques USB spécifiques grâce à leur chaîne d'identification.

---

[17] Source : « *Gestion des périphériques USB sous Windows Vista* », Joachim Gomard, Uwww.laboratoire-microsoft.orgU,

Lorsque l'on branche un dispositif USB, il faut aller dans le *Panneau de configuration* puis *Gestionnaire des périphériques,* ouvrir l'arborescence de *Contrôleur de bus USB* puis cliquer droit sur *Périphérique de stockage de masse USB* et allez dans *Propriétés*. Ensuite aller dans l'onglet détails et sélectionner comme propriété *Numéro d'identification du matériel.* La ou les chaînes d'identification s'affichent :

Figure 8 : Chaînes d'identification USB




Il faut ensuite copier la première chaîne d'identification. Dans l'éditeur de stratégie de groupe locale (dans le dossier des restrictions d'installation de périphériques comme vu plus haut) l'on a maintenant le choix entre deux types de stratégies :

- La stratégie du refus d'installation de tous les périphériques amovibles sauf ceux que j'autorise explicitement
- La stratégie de l'acceptation de l'installation de tous les périphériques amovibles sauf ceux que je refuse explicitement

Pour la première, il faut activer la stratégie *Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie* et activer la stratégie *Autoriser l'installation de périphériques correspondants à l'un de ces ID de périphérique.* Cette dernière nécessite que l'on copie la chaine d'identification dans la liste des périphériques acceptés *(Afficher – Ajouter et ctrl-V)*. Ainsi, seuls les périphériques décrits dans la liste pourront être utilisés.

Concernant la deuxième, il faut désactiver la stratégie *Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie* et activer la stratégie *Empêcher l'installation de périphériques correspondants à l'un de ces ID de périphérique.* Cette dernière nécessite que l'on copie la chaine d'identification dans la

liste des périphériques non-acceptés *(Afficher – Ajouter et ctrl-V)*. Ici, les périphériques décrits dans la liste ne pourront pas être utilisés.

La première stratégie paraît plus vraisemblable. L'on peut ainsi mettre à disposition par exemple des clés USB aux employés dont l'installation est autorisée et qui soient strictement utilisées dans le cadre du travail.

Pour finir, on peut écrire dans l'invite de commande *gpupdate /force* pour activer les stratégies mises en place sans avoir à redémarrer le PC.

Tout ceci va donc permettre d'éviter l'**installation** de périphériques. Ce qui veut dire que si le pilote du dispositif était déjà installé sur le poste avant l'établissement de ces règles, sa détection sera possible quelles que soient ces dernières. Tout pilote déjà installé sur le poste de l'employé que l'on souhaite bloquer doit donc être désinstallé avant d'utiliser ces stratégies.

Concernant les lecteurs CD/DVD, une GPO sur *Configuration utilisateur – Système – Accès au stockage amovible* est disponible. En activant *CD et DVD : refuser l'accès en lecture,* toute personne se connectant sur le poste sera dans l'impossibilité de lire les CD et les DVD.

### 5.3.2 Gestion centralisée des comptes des employés

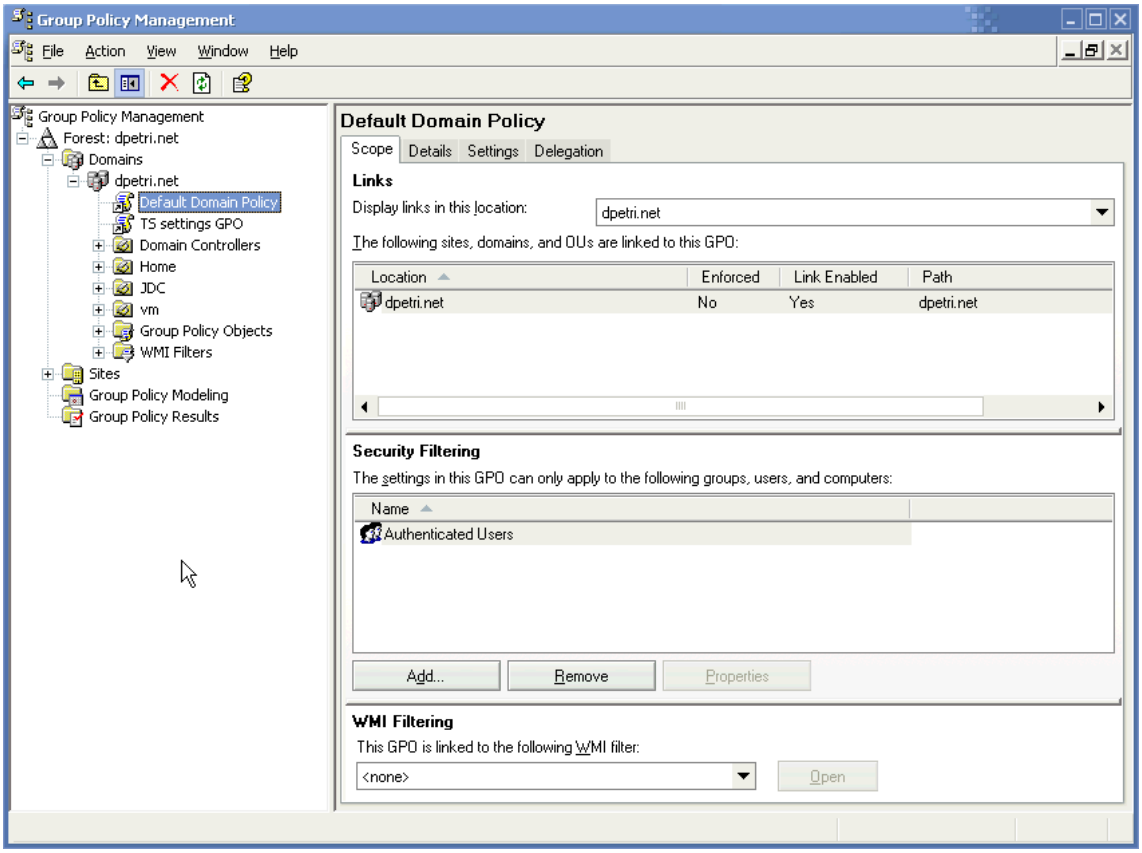
Dans les PME d'une dizaine à une cinquantaine de postes, une centralisation de toutes les informations des utilisateurs et postes est très conseillée, voire indispensable. Active Directory par exemple est un serveur qui centralise toutes ces ressources sur un ou plusieurs domaines. En général les entreprises de la taille citées ici sont mono-domaine. Ce domaine va donc contenir les comptes de tous les employés ainsi qu'un compte (ou plusieurs) possédant des droits administratifs. Ceci est très avantageux dans le sens où il est maintenant possible de configurer ses GPO depuis un seul poste et ceci pour tout le domaine. Il est donc facile de faire des restrictions selon la session de l'employé quel que soit le PC où il se connecte.

Une nouvelle console, appelée GPMC pour Group Policy Management Console, a été développée afin de centraliser les tâches de gestion et administration des GPO pour un environnement Active Directory. Elle n'est cependant pas fournie avec le système d'exploitation, il faut donc la télécharger à cette adresse  pour Windows XP:

http://www.microsoft.com/downloads/details.aspx?FamilyID=f39e9d60-7e41-4947-82f5-3330f37adfeb&displaylang=fr

Puis cliquer sur gpmc.msi et le tour est joué. Pour lancer la console, taper *gpmc.msc* dans l'exécuteur.

Figure 9 : Console GPMC




Ci-dessous l'adresse pour Windows Vista :

http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=9ff6e897-23ce-4a36-b7fc-d52065de9960

Puis suivre les instructions disponibles sur ce lien pour l'activer :

http://www.darksideofthecarton.com/2008/04/25/using-the-group-policy-management-console-gpmc-in-vista-sp1/

En déroulant l'arborescence *Domaines*, le nom de domaine de l'entreprise va apparaître. En allant sur *Objets de stratégie de groupe* on peut créer sa GPO (en la nommant GPO Ports USB par exemple) exactement de la même manière comme vu plus haut. Ce tutoriel vidéo très bien fait explicite clairement la marche à suivre pour créer une GPO pour le domaine : http://www.laboratoire-microsoft.org/videos/5363/

### 5.3.3 Solution logicielle

Une autre approche est d'utiliser une solution logicielle. Pour cela, DeviceLock de SmartLine permet de bloquer ou autoriser depuis un PC administrateur l'accès des utilisateurs ou groupes d'utilisateurs aux ports USB et aux CD/DVD. Ce logiciel permet aussi d'autoriser la détection de certains périphériques indépendamment du fait d'avoir bloqué toute détection, d'accorder à un employé un accès transitoire grâce à un code d'accès, de mettre des périphériques en lecture seule, d'obtenir un log complet des activités des périphériques, etc. Cette solution est plus « user-friendly » bien qu'elle nécessite une petite administration. Son prix est dérisoire (environ 80 CHF) pour toutes les fonctionnalités qu'elle offre. On peut l'acquérir en allant sur ce site :

http://www.devicelock.com/fr/dl/

L'antivirus, lui, permet de lancer un scan des périphériques de stockage externes mais surtout de détecter tout virus ou autre sur ceux-ci pour éviter le problème des virus que l'employé pourrait enclencher en ouvrant un fichier depuis le périphérique. Il convient donc de vérifier que son antivirus intègre bien cette fonction.

## *5.4 Logiciels personnels*

L'installation sauvage de logiciels par les employés peut-être dangereuse. Beaucoup de logiciels gratuits (freewares) contiennent des spyware ou autres qui s'incrustent dans le PC au moment de l'installation. Un moyen de bloquer l'installation de logiciels est envisageable mais cela se fait au cas par cas. En désactivant la possibilité de brancher des médias amovibles et en faisant des restrictions sur la navigation Internet, on réduit déjà de beaucoup la possibilité d'installer des logiciels non-recommandables sur les postes des employés. Cependant, il est possible d'agir directement sur l'exécution des logiciels grâce aux GPO comme mentionné dans le sous-chapitre précédent.

Cette fois, ça se passe sous *Configuration de l'ordinateur – Paramètres Windows – Stratégies de restrictions logicielle*. En cliquant sur le fichier *Contrôle obligatoire,* il faut définir que la stratégie s'applique à tous les utilisateurs excepté les administrateurs locaux. Ainsi, on pourra installer des logiciels que l'on sait sains à la demande des employés en se connectant sur le PC en tant qu'administrateur. En entrant dans le dossier *Niveau de sécurité*, on a deux choix de stratégie :

- Rejeté : Tous les logiciels sont bloqués à l'exception de ceux que l'on désire débloquer

- Non Restreint (par défaut) : Tous les logiciels sont autorisés selon les droits de l'utilisateur à l'exception de ceux que l'on bloque

On peut choisir de mettre par défaut (en double-cliquant dessus et sur le bouton *par défaut)* l'un ou l'autre selon son point de vue.

Ensuite, dans le dossier *Règles supplémentaires,* en cliquant droit on peut définir différents types de règles et dire si elles seront *Rejeté* ou *Non-Restreint*. La solution que nous préconisons est d'utiliser une règle de chemin d'accès en mode *Non-Restreint*. En effet, en définissant le chemin d'accès des répertoires où l'employé a un accès en écriture et en y mettant comme niveau de sécurité *Non-Restreint*, on les autorise à exécuter tous les programmes sauf ceux qu'ils pourraient installer dans leur dossier. Ainsi, si un salarié désire installer quoi que ce soit, il devra avoir au préalable la permission de l'administrateur ; ce qui évitera une potentielle diffusion de virus ou autres sur le réseau.

## *5.5 Branchement d'un PC personnel*

Il est très courant qu'un employé veuille brancher un ordinateur portable sur le réseau de l'entreprise que ce soit à l'intérieur même de celle-ci ou à partir de l'extérieur. Celui-ci pouvant être contaminé du fait d'avoir passé quelques jours hors de l'entreprise et de ne plus être en conformité avec les mises à jour, il devient le vecteur involontaire d'une menace pour la sécurité des ressources. Heureusement, depuis quelques années le concept de contrôle d'admission sur le réseau interne de l'entreprise connaît un grand engouement.

Le ESCV (Endpoint Security Compiancy Verification) propose une solution à cette problématique en vérifiant de manière automatique sa conformité à la politique de l'entreprise. Il va par exemple vérifier si les mises à jour de l'anti-virus ont été effectuées, s'il y a des virus ou autres présents sur le PC, s'il dispose des dernières versions des règles du firewall, etc. Du moment que cette inspection découvre une non-conformité, l'ordinateur portable est mis en quarantaine pour pouvoir être mis à jour et/ou désinfecté.

Pour cela, Microsoft a mis au point une technologie appelée Network Access Protection (NAP) qui peut être gérée par le système d'exploitation serveur Windows Server 2008 (ou Windows server 2003 R2) avec les clients Windows Vista ou Windows XP service pack 3.

NAP s'inscrit donc dans une optique de contrôler l'état de santé du portable et non pas sur une notion d'identité de l'employé pour autoriser ou bloquer l'accès aux ressources. Nous allons expliquer ici le principe général du fonctionnement de celui-ci sur un serveur Windows Server 2008 :

Lorsqu'un employé se connecte à un point d'accès pour accéder à ses ressources du réseau interne, il devra présenter son bilan de santé à un serveur distant. Celui-ci va déterminer, selon la politique de sécurité de l'entreprise, si l'employé se voit autorisé à communiquer avec l'intégralité des ressources informatiques dont il a accès ou seulement à une zone restreinte (zone de quarantaine). Pour cela, le NAP se base sur un ensemble d'éléments interconnectés permettant d'évaluer l'état de santé du PC qui se connecte et de transmettre ceci au serveur. Les éléments en question sont les suivants[18] :

- *SHA* (System Health Agent) : sur le poste de l'employé, des agents analysent différents critères de l'état du système
- *SoH* (Statement of Health) : chaque SHA enregistre les critères dans un SoH
- *SSoH* (System Statement of Health) : tous ces enregistrements sont fusionnés pour créer un bulletin d'état du système qui sera transmis au serveur distant
- *EC* (Enforcement Client) : est le module client qui va envoyer les SSoH au serveur distant
- *ES* (Enforcement Server) : est le module serveur qui récupère le SSoH du client
- *NPS* (Network Policy Server) : est le serveur Radius qui supporte le NAP
- *SHV* (System Health Validator) : est la version serveur des SHA. Il va vérifier la configuration des clients grâce à son SoH et définir leur conformité avec la politique de l'entreprise

Imaginons maintenant le scénario où un PC d'un employé qui n'a pas son antivirus à jour se connecte sur le réseau de l'entreprise :

1. Chaque *SHA* génère un bulletin d'état *SoH* qui indique l'état de cet agent. Le *SHA* destiné à contrôler l'antivirus va marquer dans son *SoH* que celui-ci n'est pas à jour
2. Tous les *SoH* sont fusionnés pour former le bulletin d'état du système *SSoH*

[18] Source : « Windows Server 2008 : Network Access Protection », Alexandre Villoing, Alexandre Wetta, Uwww.labo-microsoft.comU

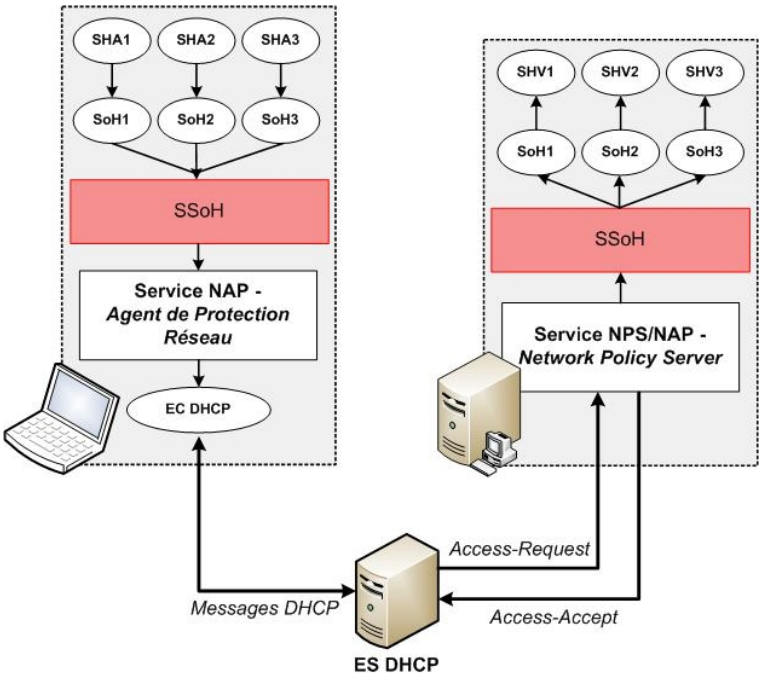
3. Le *SSoH* est transmis par le service NAP au client réseau EC selon la méthode de connexion (DHCP[19], VPN[20], 802.1x[21], etc.)
4. Le *SSoH* est réceptionné par le serveur réseau *ES* correspondant
5. Le serveur réseau *ES* envoie une demande d'accès au serveur NPS/NAP en lui transmettant le *SSoH* du poste de l'employé
6. Celui-ci décompose le *SSoH* en *SoH*
7. Chaque *SoH* est transmis au validateur d'état *SHV* correspondant. Le *SoH* concernant la mise à jour de l'antivirus est donc envoyé à son SHV
8. Les *SHV* informent du résultat des analyses (l'antivirus n'est pas à jour).
9. Selon les règles créées sur le serveur *NPS*, l'accès est accordé ou refusé avec éventuellement la consigne nécessaire permettant au client de se mettre en conformité avec la politique de sécurité
10. Le serveur d'accès *ES* transmet à l'employé les informations spécifiant que l'antivirus n'est pas à jour et connecte son poste sur des ressources d'un réseau isolé sur lequel il pourra mettre à jour son antivirus avant d'avoir un accès total au reste de ses ressources informatiques

[19] Dynamic Host Configuration Protocol est un protocole qui permet d'assigner automatiquement une adresse IP à un poste dès qu'il se branche sur le réseau.

[20] Virtual Private Network est un système permettant de connecter un ordinateur distant sur le réseau de l'entreprise. En donnant son identifiant, l'employé pourra accéder à toutes les ressources dont il possède les droits.

[21] 802.1x est un protocole qui permet de contrôler qui accède au réseau de l'entreprise et comment.

Figure 10 : Schéma de la technologie NAP




Source : Windows Server 2008 Network Access Protection, www.labo-microsoft.com

Bien que très efficace, cette technologie nécessite une mise en place assez complexe et du matériel comme un serveur Windows Server 2008 qui contient le service NPS. Celui-ci permet au serveur Windows Server 2008 de faire office de serveur Radius (serveur qui centralise les authentifications et les autorisations des employés en s'appuyant sur Active Directory). Il faut aussi, selon la connexion désirée, mettre en place du matériel et de la configuration et bien sûr configurer les stratégies de connexion NPS et les postes clients pour qu'ils supportent la technologie NAP.

Cette solution va donc être coûteuse autant par l'achat du matériel que par l'appel d'un spécialiste qui est indispensable pour installer le système. Cette gestion automatique et transparente des admissions sur le réseau est envisageable, voire indispensable pour une PME dont les employés se connectent couramment avec divers ordinateurs externes au parc informatique et qu'il est impossible de contrôler manuellement que chaque PC soit conforme à la politique de sécurité.

Dans le cas contraire, il faut penser à bien définir dans la charte et imposer que chaque portable voulant se connecter sur des ressources du réseau ait les mises à jour logicielles, antivirus et Windows actualisées, le pare-feu activé, etc.

## *5.6 L'Employé*

### 5.6.1 Mots de passe

Le mot de passe est encore très souvent le plus grand point faible de la sécurité. Les hackers voulant accéder aux ressources de l'entreprise peuvent faire des attaques de force brute sur les mots de passe permettant l'accès à des données sensibles. Cette méthode consiste à tester toutes les combinaisons possibles selon la longueur du mot de passe. Il est aussi possible d'utiliser la technique de l'attaque par dictionnaire où ils testent une liste de termes les plus couramment utilisés. Etant donné que l'employé est invité à définir un mot de passe pour accéder à son poste, il est très important, en plus de mettre en évidence une politique de mots de passe, de définir quelques techniques afin de s'assurer de la robustesse de ceux-ci.

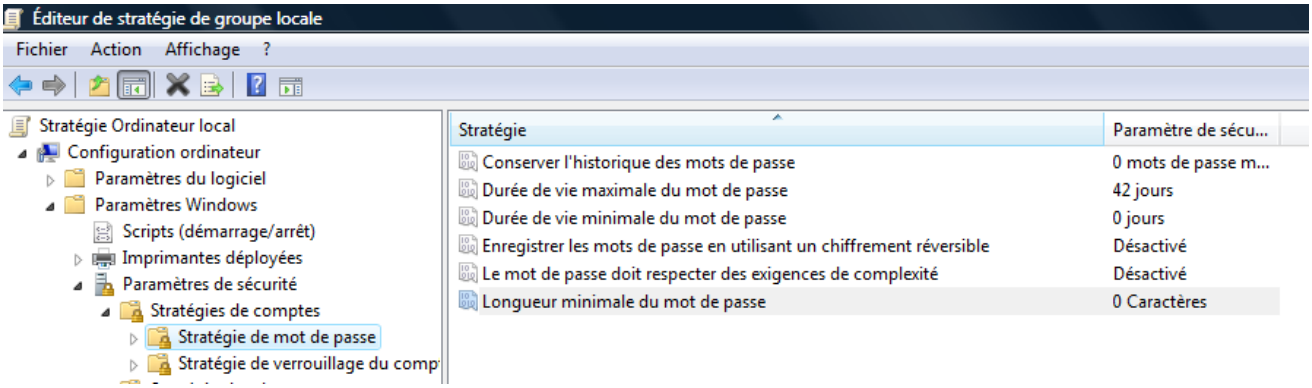
Une bonne politique de mots de passe est la clé de voûte de la sécurité de l'entreprise. L'on doit donc penser à mettre dans la charte les points suivants :

- Ne pas utiliser des mots de passe de moins de 7 caractères car plus le mot de passe est court, plus facilement il sera cassable par force brute
- Alterner majuscules et minuscules et utiliser des caractères spéciaux
- Eviter des mots de passe qui sont proches de l'employé comme son nom, celui d'un proche, sa date de naissance, etc. car ils seraient facilement devinables par l'attaquant
- Eviter les mots du dictionnaire, des prénoms de vedettes, noms de lieux, etc. qui seraient vite découverts par une attaque de dictionnaire
- Ne jamais écrire les mots de passe sur un post-it collé à l'écran par exemple
- Changer régulièrement de mot de passe

Tout ceci doit être respecté à la lettre tout en gardant à l'esprit que le mot de passe devrait être difficile à trouver mais facile à retenir. Pour cela, certaines techniques sont envisageables comme mélanger un nombre à un mot. Par exemple la date de naissance avec le nom de quelqu'un, le tout avec quelques caractères spéciaux (08S11A85RA !). Il est aussi possible de définir une méthode selon une phrase clé comme un titre de film par exemple. Imaginons la phrase « James Bond Quantum of Solace » et on définit que l'on prend les deux premières lettres de chaque mot qu'on alterne avec le nombre de caractères de celui-ci : ja5bo4qu7of2so6.

Les employés utiliseront ces techniques dans un premier temps mais laisseront vite tomber. Il est pour cela très important de faire comprendre aux employés que la politique de mots de passe est indispensable et d'en faire une obligation. Pour ce faire, une GPO est disponible sous *Configuration Ordinateur - Paramètres Windows - Paramètres de Sécurité - Stratégies de compte - Stratégie de mot de passe.*

Figure 11 : Stratégie de mots de passe




Il est donc possible de définir la durée de vie, la longueur et les exigences proposées par Microsoft (on peut les voir sous l'onglet *Expliquer*) du mot de passe.

### 5.6.2 Les attaques internes

Un employé malveillant peut mener une attaque sur des ressources de l'entreprise depuis l'intérieur. Le pare-feu n'assure qu'une protection périphérique pour empêcher des attaques depuis l'extérieur alors que les antivirus /antispyware ne prémunissent que d'une partie de celles-ci.

C'est pour cela que la solution IDS (Intrusion Detection System) a été inventée. Ce système de détection d'intrusions se décompose en deux types :

Le H-IDS (Hosted-based IDS) est un logiciel qui s'installe sur les postes ou serveurs à protéger. Ce système examine les informations des journaux de log du système d'exploitation et des applications en recherchant dans ceux-ci des entrées qui concordent avec des règles de détection préconfigurées et lance une alarme en cas de correspondance. Le H-IDS détecte aussi les appels au noyau du système d'exploitation lorsque la signature d'un de ces appels correspond à une signature d'attaque connue.

Le N-IDS (Network-based IDS) se place sur une machine dédiée et analyse tout le trafic du réseau afin de détecter des anomalies. Ce système se base plutôt sur les

protocoles et paquets qui circulent sur le réseau et par conséquent n'examine pas les processus qui se déroulent sur chaque machine.

Dans notre cas, celui de l'employé qui attaque depuis son poste une ressource de l'entreprise, la meilleure solution est d'installer un H-IDS qui est plus approprié pour les attaques d'utilisateurs légitimes. En effet, le système basé sur l'hôte s'intéresse davantage à qui a le droit de faire quoi et quand peut-il le faire et donc supervise l'état d'un réseau interne. Il sera par conséquent en mesure de détecter toute tentative d'attaque par déni de service sur la machine où elle est installée.

Une solution open-source appelée OSSEC[22] est disponible. En l'installant en mode « server », il suffit de le mettre sur une machine qui recherche toutes les alertes venues des machines sur lesquelles on l'a installé en mode « agent ». On a ainsi un contrôle centralisé de son HIDS ; ce qui est indispensable pour être à même de réagir en cas d'attaque. Un manuel complet d'installation est disponible à l'adresse suivante :

http://www.ossec.net/main/manual/#install (en anglais)

Les applicatifs et le système d'exploitation doivent aussi être protégés de toutes attaque sur des failles. Pour les programmes, regarder sur leur site les derniers patchs à installer pour qu'ils soient à jour (la plupart des logiciels proposent de se mettre à jour automatiquement). Concernant Windows, le plugin Windows Update[23] doit être activé sur chaque poste pour que les failles du système d'exploitation soient réparées régulièrement

# 6. Contrôler la sécurité

Chaque employé est responsable de la sécurité de son poste et de ceux dont il a un accès. Il doit être attentif et agir efficacement en cas d'infection d'une ressource informatique. Pour cela, une fois les politiques rédigées et les mesures techniques désirées mises en place, il est nécessaire d'écrire des procédures détaillées pour savoir qui fait quoi en cas de problème. Prenons l'exemple de la découverte d'un virus sur un poste par un employé :

- Arrêter toute utilisation de l'ordinateur et enlever la prise réseau

[22] Uhttp://www.ossec.net/main/downloads/U

[23] Uhttp://update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=frU

- Placer une note sur l'écran indiquant de ne pas utiliser le poste
- Contacter le responsable en charge de l'antivirus
- Noter l'heure de l'infection ainsi que le type d'activité observée et l'action qui a précédé l'enclenchement de celle-ci
- Le responsable de l'antivirus déconnecte le câble réseau du poste pour prévenir toute contagion
- Le responsable vérifie que l'antivirus est à jour et qu'il fonctionne correctement
- Le responsable analyse les alertes générées puis lance un scan complet du poste et supprime tout virus trouvé

Il faut aussi que le responsable de chaque moyen technique nécessitant l'installation d'une application consulte régulièrement le tableau de bord afin d'interpréter les alertes et agir en conséquence. Pour les applications installées sur chaque poste (typiquement l'antivirus et/ou le firewall clients), il faut désigner un responsable qui s'assure du niveau de sécurité en plus de l'employé lui-même. Il n'est malheureusement pas du tout pratique de devoir passer sur chaque poste pour s'assurer que le niveau de sécurité y est suffisant surtout si l'entreprise possède une multitude d'ordinateurs. C'est pour cette raison que nous avons réalisé un logiciel appelé Security Board.

## *6.1 Le prototype*

Le Security Board[24] est une application qui permet de centraliser pour un poste donné certaines informations afin de s'assurer qu'il corresponde à la politique de sécurité instaurée au sein de l'entreprise. Il faut avant toute chose s'assurer que le firewall de chaque poste accepte les connexions distantes. Aller sur chaque poste, coller le fichier okWMI.cmd[25] et cliquer dessus (pour désactiver l'accès distant, cliquer sur noWMI.cmd[26]).

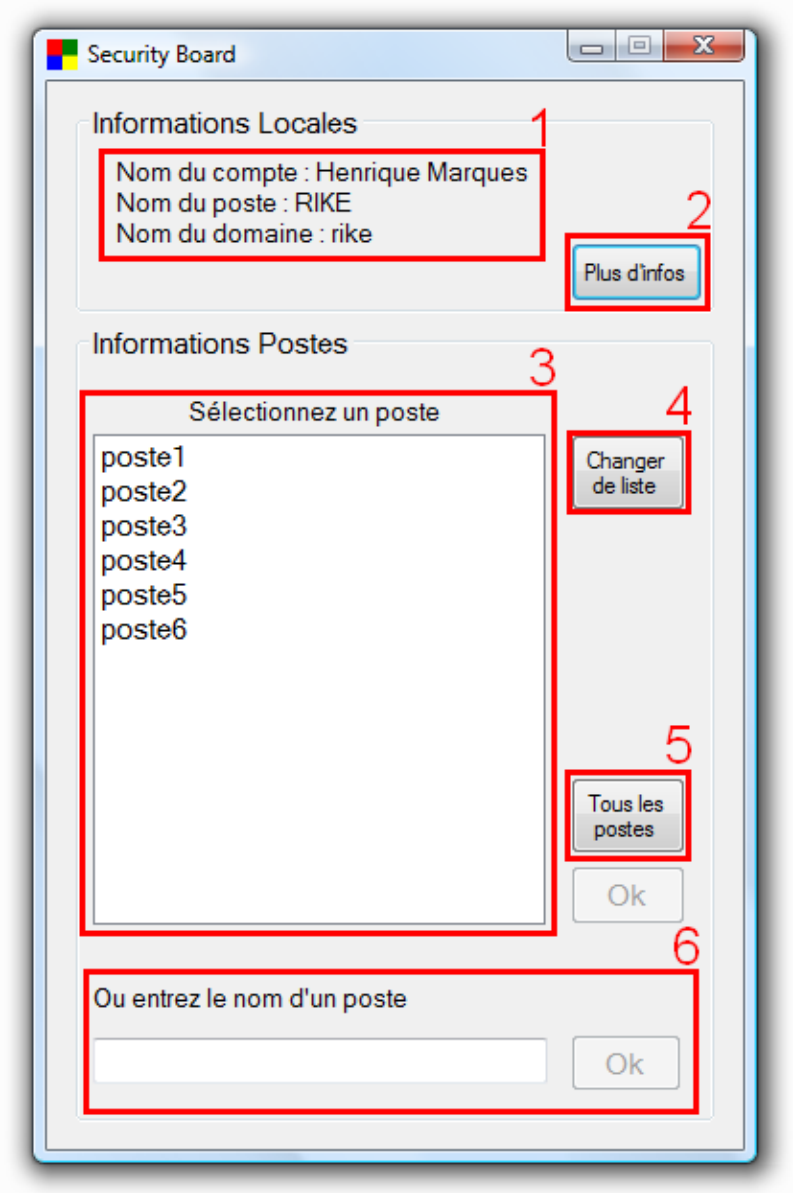
En cliquant sur SecurityBoard.exe, le menu suivant apparaît :

[24] Code Source en Annexe 5

[25] Code source en Annexe 4 sous okWMI.cmd

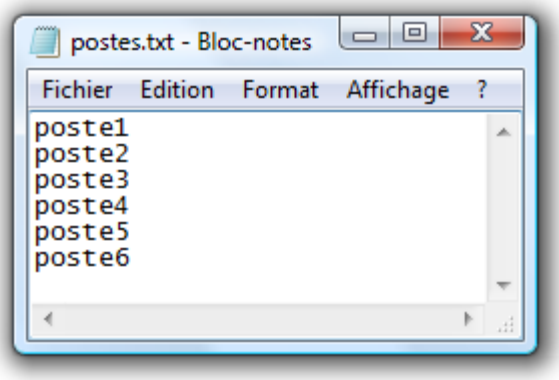
[26] Code source en Annexe 4 sous noWMI.cmd

Figure 12 : Ecran d'accueil du Security Board




1. Quelques informations du poste sur lequel l'application a été lancée
2. En cliquant sur *Plus d'infos*, on accède au tableau de bord de la sécurité du poste sur lequel l'application tourne
3. Dans le fichier *postes.txt* qui doit être placé dans le même dossier que l'application *SecurityBoard.exe,* on peut écrire le nom des postes de son réseau. Il faut impérativement que ce soit un par ligne comme ceci :

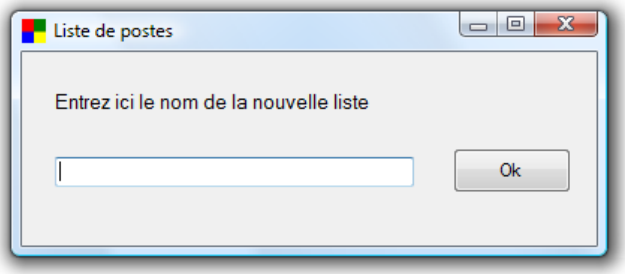
Figure 13 : Liste des postes en *.txt




Il suffira ainsi de cliquer sur le poste désiré puis sur le bouton *Ok* pour pouvoir accéder au tableau de bord de la sécurité du poste en question.

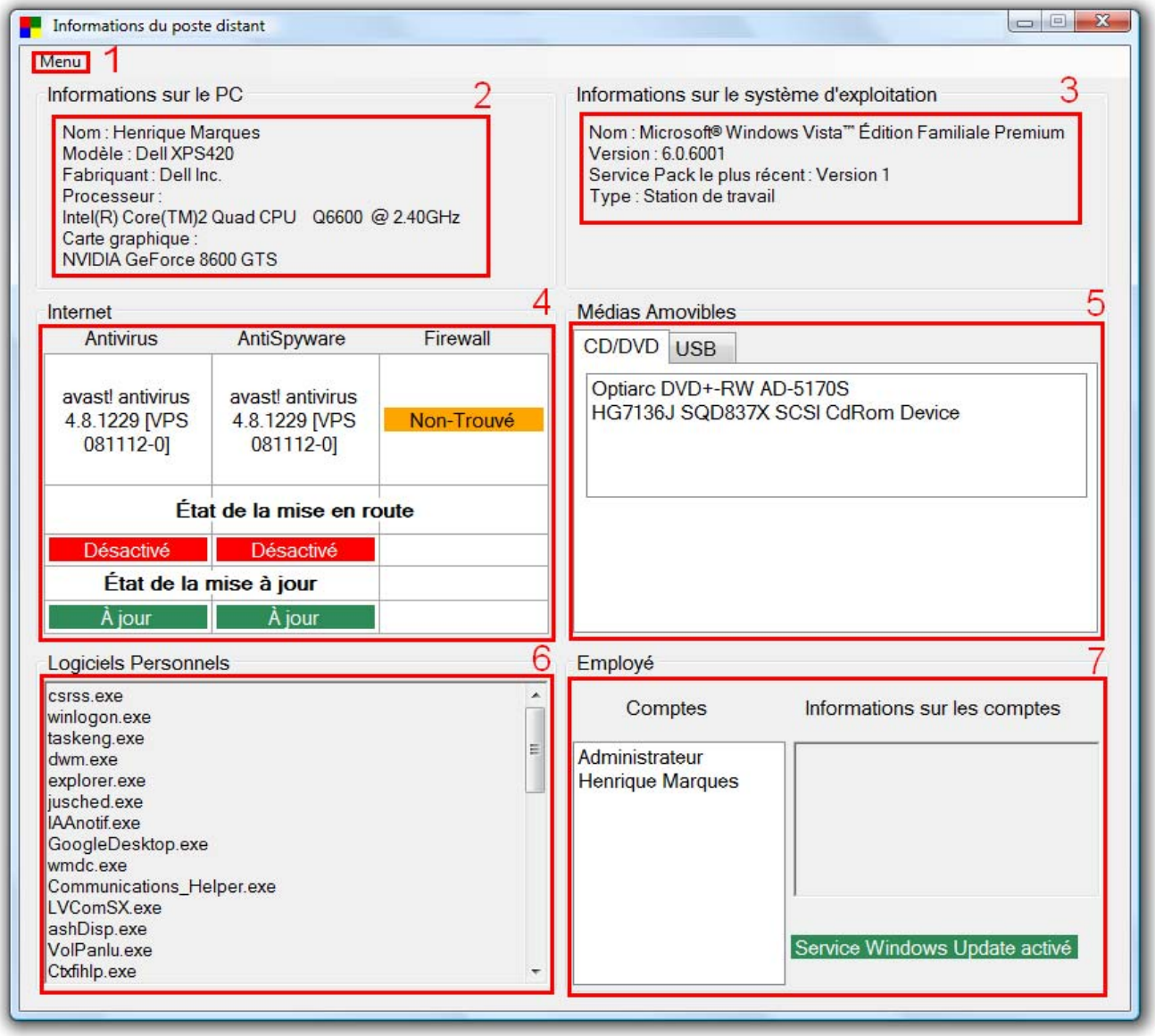
On peut de même créer une ou plusieurs listes de postes : ouvrir le bloc-notes Windows, y insérer les noms des postes et enregistrer le fichier en *.txt dans le même dossier que SecurityBoard.exe.

Figure 14 : Fenêtre de changement de liste




4. Cliquer sur *Changer de liste*. En informant le champ avec le nom du fichier (par exemple postes2) et en cliquant sur *Ok*, une nouvelle fenêtre s'ouvre avec les postes de la nouvelle liste
5. En cliquant sur *Tous les postes*, le tableau de bord de sécurité de chaque poste de la liste s'ouvrira
6. On a aussi la possibilité d'entrer directement le nom du poste dans ce champ

Figure 15 : Fenêtre des informations du poste distant




Le tableau de bord de la sécurité est présenté sous forme de vecteurs de menaces comme exposé tout au long de ce travail de diplôme. Ce sont les vecteurs Internet, Médias Amovibles, Logiciels Personnels et Employé qui sont représentés ici :

1. Ce menu permet de rafraîchir le tableau de bord ainsi que de le fermer
2. L'on dispose ici d'informations sur le PC
3. Ces informations permettent d'avoir une vue d'ensemble sur le système d'exploitation du poste. Il faut s'assurer que le dernier service pack est installé sur le poste (Service Pack 3 pour Windows XP et Service Pack 1 pour Windows Vista). Le champ type permet de savoir s'il s'agit d'un poste de travail, d'un serveur ou d'un contrôleur de domaine. En effet, il est aussi possible d'interroger ces deux autres types de machine

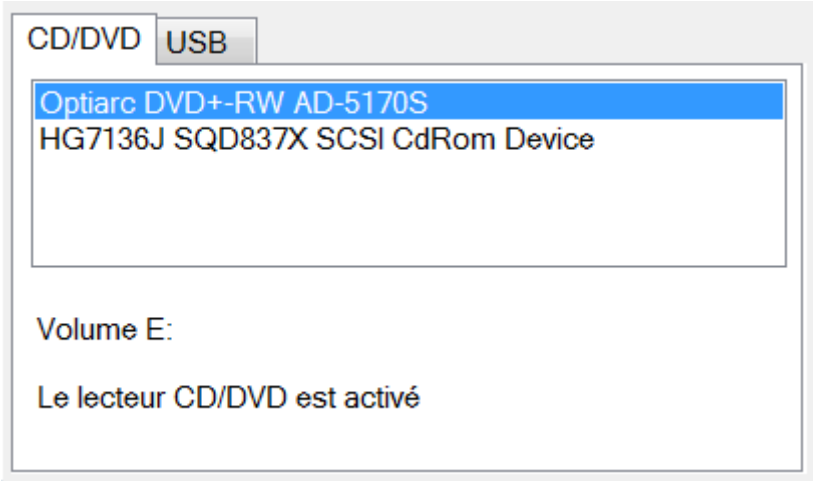
4. Pour le vecteur Internet, l'on peut voir ici des informations sur l'antivirus, l'antispyware (informations non-disponibles sous Windows XP) et le Firewall installé sur le poste. Pour l'*État de la mise en route* il y a deux états possibles :
    a. **Activé** : la protection est en fonctionnelle et donc vérifie qu'aucun virus, spyware n'infecte le poste. Le Firewall, lui, bloque les connections indésirables.
    b. **Désactivé** : il y a ici une grande menace puisque la protection n'est pas fonctionnelle. Il faut la réactiver dans les plus brefs délais

    Concernant l'*État de la mise à jour*, il peut être soit ***À jour*** soit ***Périmé***. Dans ce dernier cas l'antivirus ou l'antispyware n'a pas sa base virale à jour et le poste est donc exposé aux nouveaux virus ou spyware. La mise à jour se fait normalement automatiquement mais si on constate que l'état est toujours à ***Périmé*** après quelques rafraîchissements, il faut prendre les mesures nécessaires (le Firewall n'a pas besoin de mises à jour d'une base de données).

    Dans le cas où l'éditeur du logiciel de protection n'a pas fourni les données nécessaires pour que celui-ci soit reconnu via ce type d'application, il y aura le message ***Non-Trouvé***. Cela signifie que le Security Board n'a pas trouvé le logiciel de protection et qu'il faut vérifier sur le poste en question qu'il y en ait bien un. Le firewall de Windows ne sera pas reconnu par exemple.

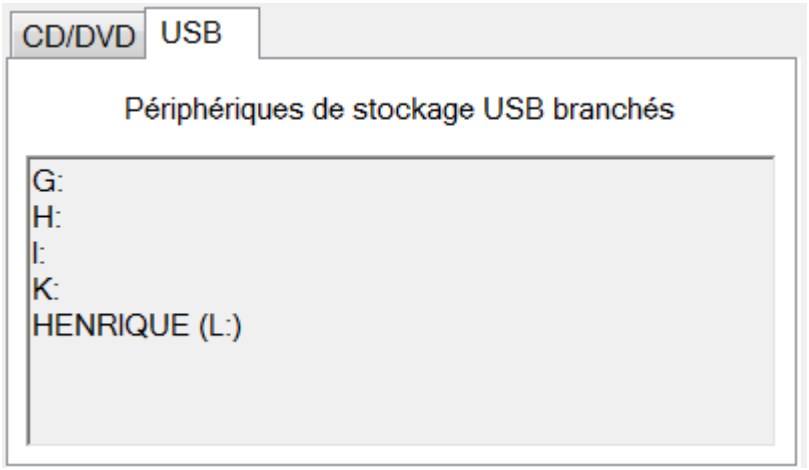
5. Pour le vecteur Médias Amovibles on aura un aperçu sur :
    a. Les périphériques de CD et DVD où l'on pourra voir le volume de chacun ainsi que son état (activé ou désactivé). Si la stratégie est de désactiver chaque périphérique CD/DVD sans passer par une GPO, on aura ici la confirmation que le périphérique est bien débranché.

Figure 16 : Liste des périphériques CD/DVD




b. Les périphériques de stockage USB branchés sur le poste. On peut vérifier ici que sa politique de gestion des médias USB est bien respectée.

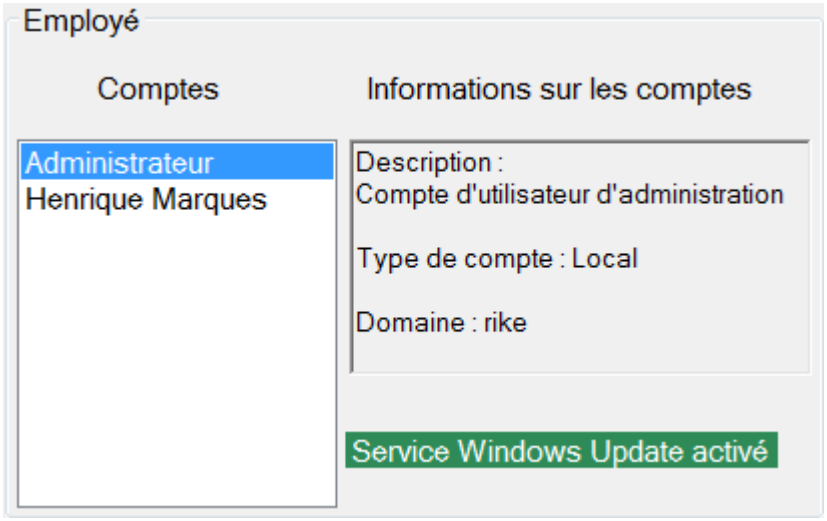
Figure 17 : Liste de périphériques de stockage USB




6. Concernant le vecteur des Logiciels personnels, la liste présentée affiche l'ensemble des processus qui tournent en ce moment sur le poste. On peut de cette façon s'assurer qu'aucun logiciel indésirable n'est en train d'être exécuté.

7. Et enfin, pour le vecteur Employé, chaque compte du poste est répertorié avec sa description, sont type (local ou en domaine) et le nom du domaine. Pour Windows Vista, il y a en plus la possibilité de vérifier que le plugin Windows Update est installé et en service. Dans le cas ou celui-ci est désactivé, Windows n'est pas mis à jour est peut-être victime d'une attaque sur diverses failles.

Figure 18 : Fenêtre du vecteur « Employé »



# Conclusion

La sécurité des ressources de l'entreprise est une affaire de tous ses protagonistes. En effet, la suppression des menaces venues de ses propres employés nécessite une réelle prise de conscience de chacun sur le danger qu'elles peuvent représenter face à la pérennité de l'entreprise. Bien que les moyens techniques offrent une barrière solide, c'est surtout les mentalités et les manières d'interagir avec le système d'information informatisé qu'il faut transformer à l'ère des nouvelles technologies de l'information.

Ce travail nous a fait réaliser que la mise en place de moyens afin d'assurer la sécurité des ressources d'un réseau d'entreprise n'est pas forcément onéreuse et n'est pas seulement destinée à des professionnels de la sécurité. Nous avons pu nous confronter à plusieurs points de vue sur les menaces internes mais elles convergent toutes vers le fait qu'il s'agit du principal risque de sécurité informatique. Nous espérons alors que les personnes à la tête d'une entreprise ayant lu ce travail ont pu être sensibilisées et y ont trouvé des marches à suivre efficaces pour diminuer au maximum les menaces venant de leurs propres employés.

# Bibliographie

## Livres


Calé, S., Touitou, P., *La sécurité informatique réponses techniques, organisationnelles et juridiques*, Paris, Editions Lavoisier, 2007

Favre, B., Goupille, P.-A., *Guide pratique de sécurité informatique : mise en œuvre sous Windows et Linux*, Paris, Editions Dunod, 2005

Llorens, C., Levier, L., *Tableaux de bord de la sécurité réseau*, Paris, Editions Eyrolles, 2003

Maiwald, E., *Sécurité des réseaux*, Paris, Editions Campus Presse, 2001

Stebben, G., Everett Church, R., Levine J.-R, *Sécurité Internet pour les nuls*, First Editions, 2003

Cobb, C., *Sécurité des réseaux pour les nuls*, First Editions, 2003


## Sites Internet


http://www.laboratoire-microsoft.org

http://lab-windows.fr

http://www.labo-microsoft.com

http://support.microsoft.com

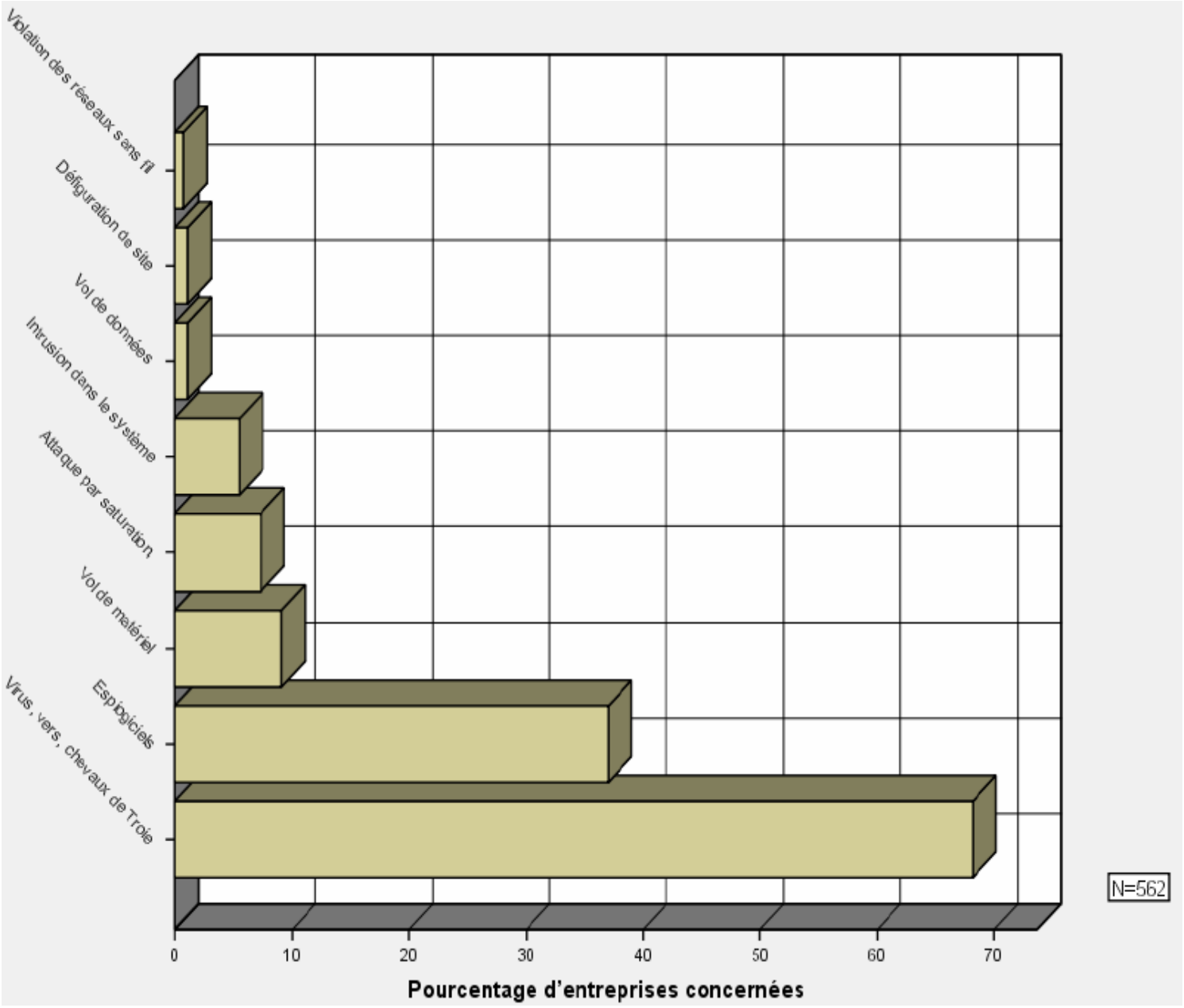
http://www.journaldunet.com

http://www.commentcamarche.net

http://technet.microsoft.com

# Annexe 1

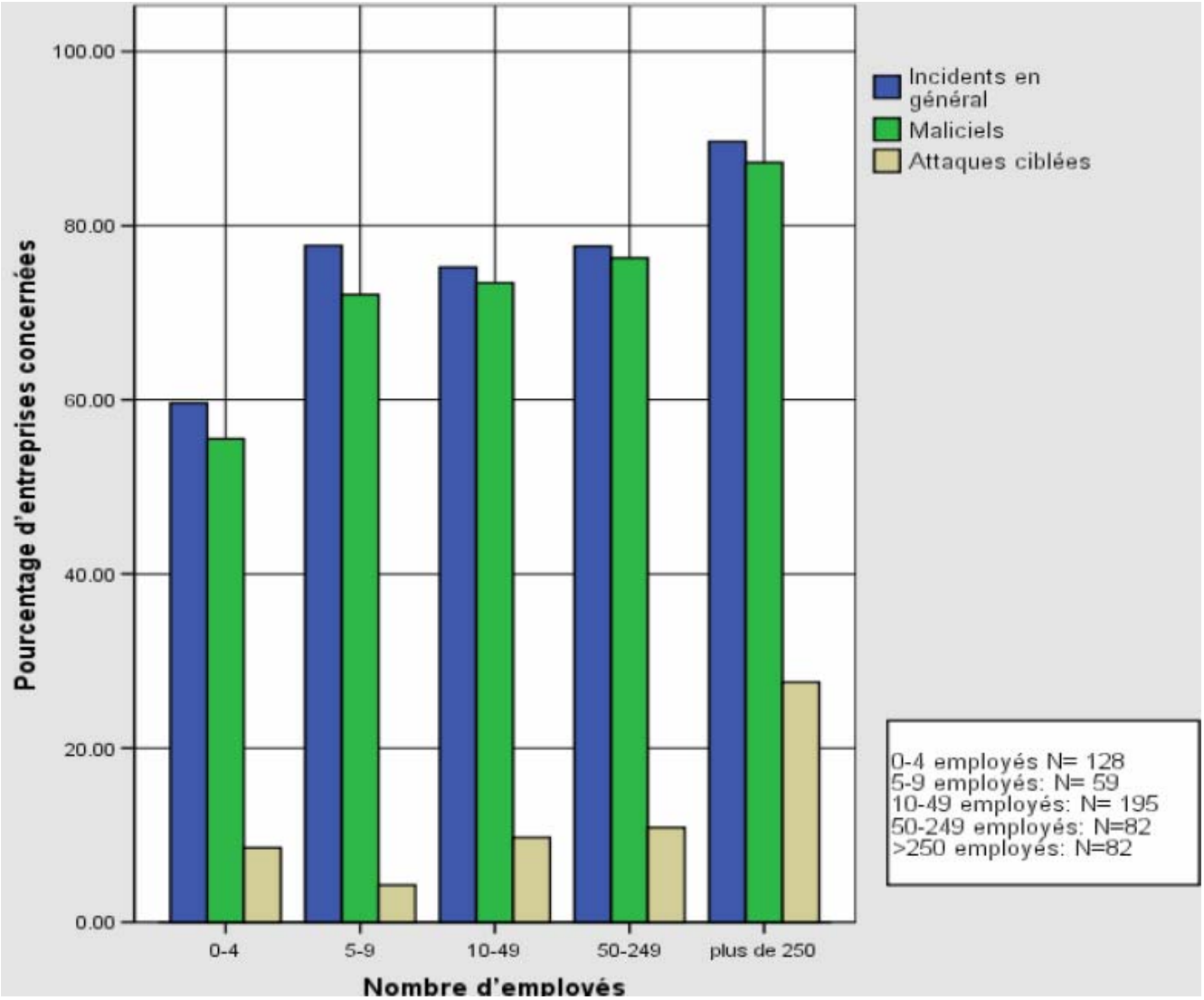
# Fréquence d'incidents




Source : Étude MELANI (2006, p. 11-12)

# Annexe 2

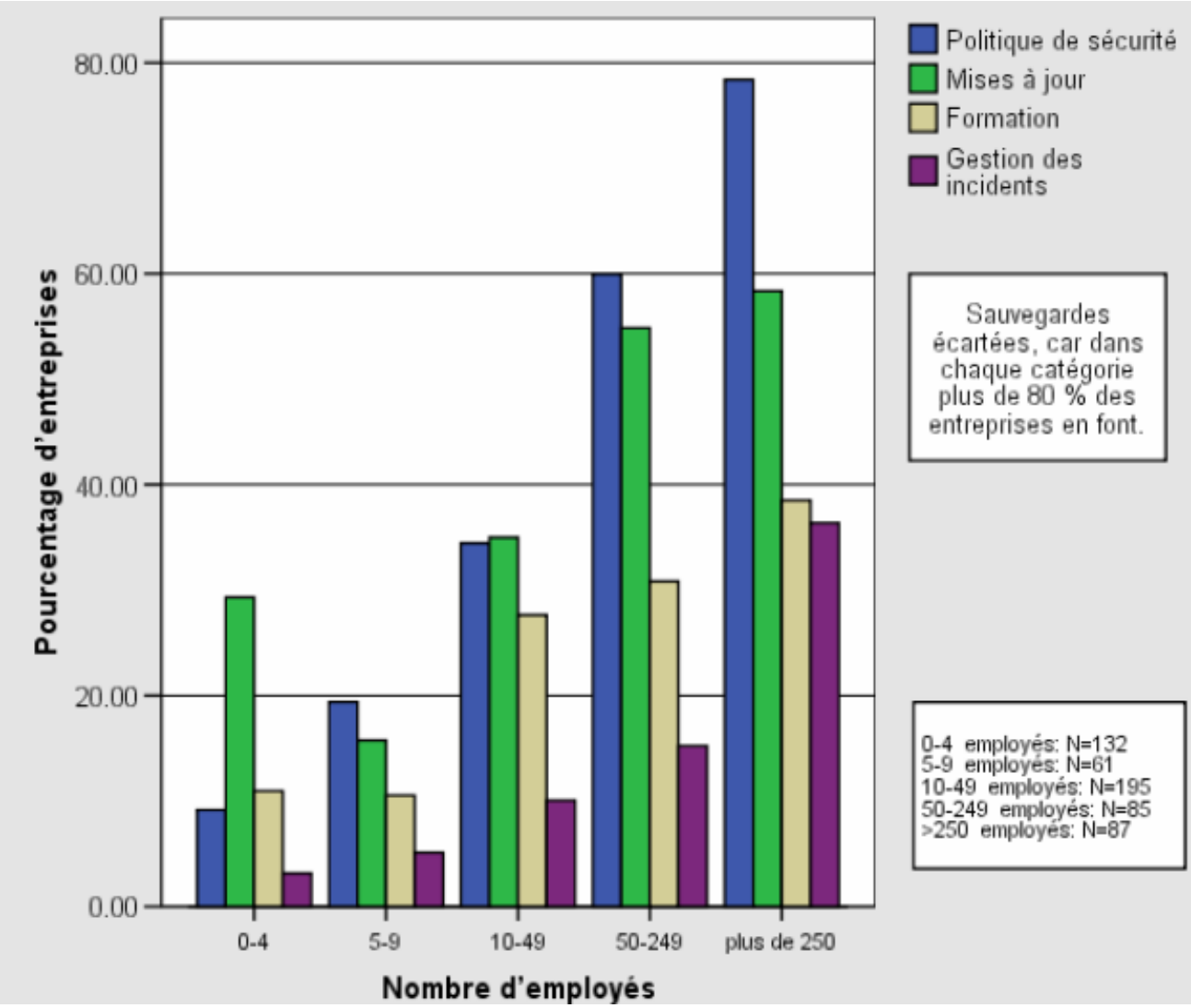
## Risque d'incidents en fonction de la taille de l'entreprise




Source : Étude MELANI (2006, p. 14-15)

# Annexe 3

## Utilisation des mesures organisationnelles en fonction de la taille de l'entreprise




Source : Étude MELANI (2006, p. 21-22)

# Annexe 4

# Codes Sources

## noAutorun.reg

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer]

"NoDriveTypeAutoRun"=dword:000000ff
```

## okAutorun.reg

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer]

"NoDriveTypeAutoRun"=dword:00000080
```

## noUSB.reg

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR]

"Start"=dword:00000004
```

## okUSB.reg

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR]

"Start"=dword:00000003
```

## okWMI.cmd

```
netsh firewall set service RemoteAdmin enable
```

## noWMI.cmd

```
netsh firewall set service RemoteAdmin disable
```

# Annexe 5

# Code Source de l'application SecurityBoard.exe

## fenAdmin.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Management;
using System.IO;

namespace Security_Board
{
    public partial class fenAdmin : Form
    {
        public static string liste = "postes";
        public fenAdmin()
        {
            InitializeComponent();

            lblAdmin.Text = "Nom du compte : " + Environment.UserName + "\r\n" + "Nom du poste : " + Environment.MachineName +
                "\r\n" + "Nom du domaine : " + Environment.UserDomainName;
            listePostes();


        }

        public void listePostes()
        {
            string ligne = null;
            StreamReader fluxInfos = null;

            try
            {

                using (fluxInfos = new StreamReader(liste + ".txt"))
                {
                    ligne = fluxInfos.ReadLine();
                    while (ligne != null)
                    {
                        lbPostes.Items.Add(ligne);
                        ligne = fluxInfos.ReadLine();
                    }//while
                }//using
            }//try

            catch (Exception)
            {
                MessageBox.Show("La liste des postes est introuvable. Veuillez mettre le fichier de la liste des postes dans le même dossier que SecurityBoard.exe");
            }//catch
        }//lisePostes

        private void btnOk_Click(object sender, EventArgs e)
        {
            String strEmp = tbEmp.Text;

            try
            {
                fenEmp fe = new fenEmp(strEmp);
                fe.Visible = true;
            }
```

```
            catch (Exception)
            {
                MessageBox.Show("Cet ordintateur est introuvable. Veuillez entrer un nom de poste valide.");
            }//catch

        }

        private void btnInfos_Click(object sender, EventArgs e)
        {
            try
            {
                fenAdminInf fe = new fenAdminInf();
                fe.Visible = true;
            }
            catch (Exception)
            {
                MessageBox.Show("Votre poste n'est pas atteignable. Veuillez vérifier la configuration du Firewall.");
            }//catch

        }

        private void btnOkPostes_Click(object sender, EventArgs e)
        {
            String strEmp = Convert.ToString(lbPostes.SelectedItem);
            try
            {
                fenEmp fe = new fenEmp(strEmp);
                fe.Visible = true;
            }
            catch (Exception)
            {
                MessageBox.Show("Cet ordintateur est introuvable. Vérifiez sa disponibilité sur le réseau ou supprimez le de
la liste.");
            }//catch

        }

        private void tbEmp_TextChanged(object sender, EventArgs e)
        {
            btnOk.Enabled = true;
        }

        private void lbPostes_SelectedIndexChanged(object sender, EventArgs e)
        {
            btnOkPostes.Enabled = true;
        }

        private void btnSelec_Click(object sender, EventArgs e)
        {
            int nbPostes = lbPostes.Items.Count;
            String[] tab = new String[nbPostes];
            lbPostes.Items.CopyTo(tab, 0);
            try
            {
                for (int i = 0; i < tab.Count(); i++)
                {
                    fenEmp fe = new fenEmp(tab[i]);
                    fe.Visible = true;
                }//for
            }
            catch (Exception)
            {
                MessageBox.Show("Un poste parmis la liste est introuvable. Vérifiez sa disponibilité sur le réseau ou
supprimez le de la liste.");
            }//catch
        }

        private void btnListe_Click(object sender, EventArgs e)
        {
            fenListe feL = new fenListe();
            feL.Visible = true;
        }

    }//fenAdmin

}//SecurityBoard
```

## fenListe.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;


namespace Security_Board
{
    public partial class fenListe : Form
    {
        public fenListe()
        {
            InitializeComponent();


        }

        private void btnOk_Click(object sender, EventArgs e)
        {

            fenAdmin.liste = tbListe.Text;
            this.Close();
            fenAdmin feA = new fenAdmin();
            feA.Visible = true;


        }
    }
}
```

## fenEmp.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Management;



namespace Security_Board
{
    public partial class fenEmp : Form
    {

        ManagementScope chemin;
        ObjectQuery requete;
        ManagementObjectCollection collObj;
        ManagementObjectSearcher requeteExec;
        String strEmp;


        public fenEmp(String stEmp)
        {
            InitializeComponent();
            strEmp = stEmp;
            sCAntivirus();
            sCFireWall();
            cimvComputerSystem();
            cimvProcessor();
            cimvDisplayConfiguration();
            cimvOperatingSystem();
            cimvUserAccount();
```

```
            cimvService();
            cimvCDROMDrive();
            cimvLogicalDisk();
            cimvOperatingSystemIfVista();
            cimvOperatingSystemIfXP();
        }//fenEmp

        public void connectionWMI(String cheminS, String requeteS)
        {

            chemin = new ManagementScope(@"\\" + strEmp + @"\root\" + cheminS);
            requete = new ObjectQuery("SELECT * FROM " + requeteS);
            requeteExec = new ManagementObjectSearcher(chemin, requete);
            collObj = requeteExec.Get();


        //return collObj;



        }//connectionWmi

        public void sCAntivirus()
        {
            try
            {
                connectionWMI("SecurityCenter", "AntivirusProduct");

                    foreach (ManagementObject mo in collObj)
                    {
                        String active = mo["onAccessScanningEnabled"].ToString();
                        String maj = mo["productUptoDate"].ToString();
                        lblNomAntivir.Text = mo["displayName"].ToString();
                        if (active == "True") { lblEnableAntivirus.Text = "Activé"; lblEnableAntivirus.BackColor = Color.SeaGreen;
} else { lblEnableAntivirus.Text = "Désactivé"; lblEnableAntivirus.BackColor = Color.Red; }
                        if (maj == "True") { lblMajAntivirus.Text = "À jour"; lblMajAntivirus.BackColor = Color.SeaGreen; } else {
lblMajAntivirus.Text = "Périmé"; lblMajAntivirus.BackColor = Color.Red; }


                    }//foreach


                if (lblNomAntivir.Text == "")
                {
                    lblNomAntivir.Text = "Non-Trouvé"; lblNomAntivir.BackColor = Color.Orange;
                    lblEnableAntivirus.Text = "";
                    lblMajAntivirus.Text = "";
                }

            }//try
            catch (ManagementException e1)
            {
                MessageBox.Show(e1.Message);
            }//catch

        }//sCAntivirus

        public void sCFireWall()
        {
            try
            {
                connectionWMI("SecurityCenter", "FirewallProduct");

                foreach (ManagementObject mo in collObj)
                {
                    String active = mo["enabled"].ToString();
                    lblFirewall.Text = mo["displayName"].ToString();
                    if (active == "True") { lblEnableFirewall.Text = "Activé"; lblEnableFirewall.BackColor = Color.SeaGreen; }
else { lblEnableFirewall.Text = "Désactivé"; lblEnableFirewall.BackColor = Color.Red; }
                    //if (maj == "True") { lblMajSpy.Text = "A jour"; lblMajSpy.BackColor = Color.SeaGreen; } else {
lblMajSpy.Text = "Périmé"; lblMajSpy.BackColor = Color.Red; }

                }//foreach
                if (lblFirewall.Text == "") {
                    lblFirewall.Text = "Non-Trouvé"; lblFirewall.BackColor = Color.Orange;
                    lblEnableFirewall.Text = "";
```

```
                lblMajFirewall.Text = "";
            }

        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
        }//catch

    }//sCFireWall

    public void sCSpyware()
    {
        try
        {
            connectionWMI("SecurityCenter", "AntiSpywareProduct");
            foreach (ManagementObject mo in collObj)
            {
                String active = mo["productEnabled"].ToString();
                String maj = mo["productUptoDate"].ToString();
                lblSpy.Text = mo["displayName"].ToString();
                if (active == "True") { lblEnableSpy.Text = "Activé"; lblEnableSpy.BackColor = Color.SeaGreen; } else {
lblEnableSpy.Text = "Désactivé"; lblEnableSpy.BackColor = Color.Red; }
                if (maj == "True") { lblMajSpy.Text = "À jour"; lblMajSpy.BackColor = Color.SeaGreen; } else {
lblMajSpy.Text = "Périmé"; lblMajSpy.BackColor = Color.Red; }

            }//foreach
            if (lblSpy.Text == "")
            {
                lblSpy.Text = "Non-Trouvé"; lblSpy.BackColor = Color.Orange;
                lblEnableSpy.Text = "";
                lblMajSpy.Text = "";
            }

        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
        }//catch

    }//sCSpyware

    public void cimvComputerSystem()
    {
        try
        {
            connectionWMI("cimv2", "Win32_ComputerSystem");
            foreach (ManagementObject mo in collObj)
            {
                lblPc.Text += "Nom : " + mo["Caption"].ToString() + "\r\n" + "Modèle : " + mo["Model"].ToString() + "\r\n" +
"Fabriquant : " + mo["Manufacturer"].ToString() + "\r\n";

            }//foreach

        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
        }//catch

    }//cimvComputerSystem

    public void cimvProcessor()
    {
        try
        {
            connectionWMI("cimv2", "Win32_Processor");
            foreach (ManagementObject mo in collObj)
            {
                lblPc.Text += "Processeur : " + "\r\n" + mo["Name"].ToString() + "\r\n";
            }//foreach

        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
```

```
    }//catch

}//cimvProcessor

public void cimvDisplayConfiguration()
{
    try
    {
        connectionWMI("cimv2", "Win32_DisplayConfiguration");
        foreach (ManagementObject mo in collObj)
        {
            lblPc.Text += "Carte graphique : " +"\r\n" + mo["Caption"].ToString();
        }//foreach

    }//try
    catch (ManagementException e1)
    {
        MessageBox.Show(e1.Message);
    }//catch

}//cimvDisplayConfiguration

public void cimvProcessVista()
{

    try
    {
        connectionWMI("cimv2", "Win32_Process");

        foreach (ManagementObject mo in collObj)
        {
            String sessionId = mo["SessionId"].ToString();
            if (sessionId == "1") { rtbPro.Text += mo["Caption"].ToString() + "\r\n"; }

        }//foreach

    }//try
    catch (ManagementException e1)
    {
        MessageBox.Show(e1.Message);
    }//catch

}//cimvProcessVista


public void cimvProcessXP()
{

    try
    {
        connectionWMI("cimv2", "Win32_Process");

        foreach (ManagementObject mo in collObj)
        {
            rtbPro.Text += mo["Caption"].ToString() + "\r\n";

        }//foreach

    }//try
    catch (ManagementException e1)
    {
        MessageBox.Show(e1.Message);
    }//catch

}//cimvProcessXP


public void cimvOperatingSystem()
{
    try
    {
        connectionWMI("cimv2", "Win32_OperatingSystem");
        foreach (ManagementObject mo in collObj)
        {
            lblOs.Text += "Nom : " + mo["Caption"].ToString() + "\r\n" + "Version : " + mo["Version"].ToString() + "\r\n"
                + "Service Pack le plus récent : Version " + mo["ServicePackMajorVersion"].ToString() + "\r\n";
```

```
            String typeOS = mo["ProductType"].ToString();
            if (typeOS == "1") { lblOs2.Text = "Type : " + "Station de travail"; }
            else if (typeOS == "2") { lblOs2.Text = "Type : " + "Serveur Active Directory"; }
            else { lblOs2.Text = "Type : " + "Serveur"; }
        }//foreach

    }//try
    catch (ManagementException e1)
    {
        MessageBox.Show(e1.Message);
    }//catch

}//cimvOperatingSystem


public void cimvOperatingSystemIfXP()
{
    try
    {
        connectionWMI("cimv2", "Win32_OperatingSystem where caption LIKE '%XP%'");
        foreach (ManagementObject mo in collObj)
        {
            lblEmpMaj.Text = "";
            lblSpy.Text = "Non supporté sous Windows XP";
            lblMajSpy.Text = "Non supporté sous Windows XP";
            lblEnableSpy.Text = "Non supporté sous Windows XP";
            cimvProcessXP();

        }//foreach

    }//try
    catch (ManagementException e1)
    {
        MessageBox.Show(e1.Message);
    }//catch

}//cimvOperatingSystemIfXP

public void cimvOperatingSystemIfVista()
{
    try
    {
        connectionWMI("cimv2", "Win32_OperatingSystem where caption LIKE '%VISTA%'");
        foreach (ManagementObject mo in collObj)
        {
            sCSpyware();
            cimvProcessVista();

        }//foreach

    }//try
    catch (ManagementException e1)
    {
        MessageBox.Show(e1.Message);
    }//catch

}//cimvOperatingSystemIfVista


public void cimvUserAccount()
{
    try
    {
        connectionWMI("cimv2", "Win32_UserAccount");
        foreach (ManagementObject mo in collObj)
        {
            String nomUser = mo["Name"].ToString();
            String desactive = mo["Disabled"].ToString();
            if (desactive == "False")
            {
                lbUsers.Items.Add(nomUser);
            }//if

        }//foreach
```

```
        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
        }//catch

    }

    public void cimvService()
    {
        try
        {
            connectionWMI("cimv2", "Win32_Service where caption = 'Windows Update'");
            foreach (ManagementObject mo in collObj)
            {

                String statut = mo["Started"].ToString();
                if (statut == "False")
                {
                    lblEmpMaj.Text = "Service Windows Update désactivé"; lblEmpMaj.BackColor = Color.Red;
                }
                else
                {
                    lblEmpMaj.Text = "Service Windows Update activé"; lblEmpMaj.BackColor = Color.SeaGreen;
                }//if

            }//foreach

            if (lblEmpMaj.Text == "") { lblEmpMaj.Text = "Plugin Windows Update non-installé"; lblEmpMaj.BackColor =
Color.Orange; }



        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
        }//catch

    }//cimvService

    public void cimvCDROMDrive()
    {
        try
        {
            connectionWMI("cimv2", "Win32_CDROMDrive");
            foreach (ManagementObject mo in collObj)
            {

                String nom = mo["Caption"].ToString();


                lbCd.Items.Add(nom);


            }//foreach

        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
        }//catch

    }//cimvCDROMDrive

    public void cimvLogicalDisk()
    {
        try
        {
            connectionWMI("cimv2", "Win32_LogicalDisk where Description = 'Disque amovible'");
            foreach (ManagementObject mo in collObj)
            {

                String nom = mo["Caption"].ToString();
```

```
                try
                {
                   String volume = mo["VolumeName"].ToString();
                   rtbUsb.Text += volume + " (" + nom + ")";

                }//try
                catch (NullReferenceException) { rtbUsb.Text += nom + "\r\n"; }


             }//foreach

          }//try
          catch (ManagementException e1)
          {
             MessageBox.Show(e1.Message);
          }//catch

       }//cimvLogicalDisk



       private void lbUsers_SelectedIndexChanged(object sender, EventArgs e)
       {
          rtbUser.Clear();
          try
          {
             String nomUserSelec = Convert.ToString(((System.Windows.Forms.ListBox)(sender)).SelectedItem);
             connectionWMI("cimv2", "Win32_UserAccount where Name='"+nomUserSelec+"'");

          foreach (ManagementObject mo2 in collObj)
          {
             String description = mo2["Description"].ToString();
             if (description == "") { rtbUser.Text += "Description : "+ "\r\n" + "Compte d'utilisateur standard" + "\r\n" + "\r\n"; }
             else {
                rtbUser.Text += "Description : " + "\r\n" + description + "\r\n" + "\r\n";
             }//if

             String domaineLoc = mo2["LocalAccount"].ToString();
             if (domaineLoc == "True") { rtbUser.Text += "Type de compte : Local" + "\r\n" + "\r\n"; }
             else
             {
                rtbUser.Text += "Type de compte : En domaine" + "\r\n" + "\r\n";
             }//if

             String domaine = mo2["Domain"].ToString();
             rtbUser.Text += "Domaine : " + domaine + "\r\n";



             /*String pswd = mo2["PasswordRequired"].ToString();
             if (pswd == "True") { lblEmpPass.Text = "Mot de passe demandé : Oui"; lblEmpPass.BackColor =
Color.SeaGreen;}
             else
             {
                lblEmpPass.Text = "Mot de passe demandé : Non"; lblEmpPass.BackColor = Color.Red;
             }//if*/



          }//foreach


          }//try
          catch (ManagementException e1)
          {
             MessageBox.Show(e1.Message);
          }//catch
       }

       private void lbCd_SelectedIndexChanged(object sender, EventArgs e)
       {

          try
          {
             String cdSelec = Convert.ToString(((System.Windows.Forms.ListBox)(sender)).SelectedItem);
```

```
            connectionWMI("cimv2", "Win32_CDROMDrive where Caption = '" + cdSelec +"'");

            foreach (ManagementObject mo2 in collObj)
            {

                try
                {
                    String volume = mo2["Drive"].ToString();
                    lbVolume.Text = "Volume "+volume;
                    lblCdSt.Text = "Le lecteur CD/DVD est activé";
                }//try
                catch (NullReferenceException) { lbVolume.Text = "Le lecteur CD/DVD est désactivé"; lblCdSt.Text = "";}



            }//foreach


        }//try
        catch (ManagementException e1)
        {
            MessageBox.Show(e1.Message);
        }//catch

    }

    private void rafraîchirToolStripMenuItem_Click(object sender, EventArgs e)
    {
        fenEmp fe2 = new fenEmp(strEmp);
        fe2.Show();
        this.Close();

    }

    private void fermerToolStripMenuItem_Click(object sender, EventArgs e)
    {
        this.Close();
    }//lbCd_SelectedIndexChanged


}//fenEmp
}//SecurityBoard
```