La sécurité et la veille ou de la sécurité dans la veille.

Olivier Servas

LA SECURITE ET LA VEILLE OU DE LA SECURITE DANS LA VEILLE

Olivier Servas,
Coordinateur sécurité CNRS / UREC
Olivier.Servas@mines.inpl-nancy.fr

Adresse professionnelle
Ecole des Mines de Nancy△Parc de Saurupt△F-54042△Nancy cedex

Résumé : La sécurité de votre système de veille doit s'intégrer dans votre système d'information et surtout ne pas l'altérer. Les mécanismes de sécurité mis en oeuvre sont ceux que l'on utilise régulièrement, même si cela paraît paradoxal de concilier l'anonymat et la gestion événementielle. Cet ensemble repose sur différents acteurs et différents niveaux de confiance.

Summary: The security of your watch system must be integrated into your information system but should not be a source of alteration. The mechanisms of security implemented are those that are commonly used even though this may seem of paradox to conciliate anonymous and event management. All these rely on different actors at various level of confidence.

Mots clés : sécurité, système d'information, système de veille

Keywords: security, information system, watch system

La sécurité et la veille ou de la sécurité dans la veille

1 - INTRODUCTION

Pour le «Veilleur» Internet est une intelligence collective en marche. Celui-ci confortablement installé dans son fauteuil, depuis son domicile ou son lieu de travail, utilise son système de veille sans (ou presque) limite dans le monde d'Internet. D'une information à une autre, il effectue sa veille.
Tout semble satisfaire notre «Veilleur» du résultat, sous réserve de certaines conditions. D'une part il faut que ce système de veille s'intègre parfaitement avec la politique de sécurité du système d'information dans lequel il se trouve. Et, surtout il ne doit en aucun cas diminuer le niveau de sécurité. D'autre part que sa recherche ne soit absolument pas confidentielle et anonyme.
La nature ouverte de l'Internet et son utilisation mondiale avec des millions d'usagers d'origine culturelle, linguistique et sociale différente n'apporte pas ou peu de confiance, d'où la nécessité de mettre en œuvre une politique de sécurité[1], de la suivre et de l'améliorer.
Les menaces, plus ou moins évidentes comme le piratage, les virus, les vers, la négligence, les écoutes, l'ingénierie sociale et autres ne sont pas éphémères. Des entités comme le CERT RENATER[2] en repèrent un grand nombre régulièrement qui peuvent mettre en péril toutes vos données et votre système d'information. Nul n'est à l'abri.
Le développement des accès Internet et des technologies utilisées (équipements et logiciels) expose les entités universitaires, de recherche, tout comme les entreprises, à davantage de risques. Une simple intrusion peut coûter beaucoup de temps et d'argent. Les dommages causés par ces différentes menaces, au-delà des dépenses faites pour revenir à l'état initial, doivent inclure les coûts de pertes de confiance des utilisateurs ou consommateurs, les possibles poursuites judiciaires, les pertes sur les propriétés intellectuelles et brevets, les actifs de la société.
La sécurité repose sur tous les acteurs de votre système. Elle ne doit pas être comprise comme une réduction fonctionnelle, mais comme une analyse du risque. Généralement beaucoup de bon sens donne un bon résultat, même si nous évoquons bon nombre d'équipements et un arsenal d'outils nécessaires pour contrer l'ensemble de ces menaces. Que faire si le pire devait arriver ?

2 - DEFINITION ET RAPPEL SUR LA SECURITE DE VOTRE SYSTEME D'INFORMATION

La sécurité est un état d'esprit confiant et tranquille qui résulte du sentiment, bien ou mal fondé, que l'on est à l'abri de tout danger[3]. Dans notre cas pour que cette situation soit objective, elle doit remplir les conditions qui permettent de réaliser et d'apporter une authentification, des autorisations, de la confidentialité, de l'intégrité, de la traçabilité, de la non répudiation et l'imputabilité.
Pour mettre en œuvre ces conditions dans votre système d'information, cela passe par une solution globale, c'est à dire l'action de l'ensemble des responsables en adéquation avec la participation des usagers car cela peut conduire à différents changements. Quel type de confiance on accorde et à qui? Cela passe par la connaissance et la maîtrise de votre système d'information pour mettre en œuvre ces conditions et de ses accès physiques. A cela il faut éduquer les acteurs par la sensibilisation à ces mesures, de bien comprendre la finalité et d'inclure de la formation[4] pour les appliquer. Les solutions techniques n'apportent pas toutes les réponses, il faut associer un cadre déontologique (la netiquette[5]), légal via le droit juridique, avec une charte[6] en adéquation avec votre règlement intérieur (nul n'est censé ignorer la loi). Il y a nécessairement un compromis entre la valeur du «protégé» et le coût de la protection, donc il faut savoir quoi protéger, par qui et avec quoi.

2.1 – Méthodologie

Pour cela il existe différentes méthodes d'analyses comme la norme ISO 17799[7], l'analyse des risques[8],

[1] Une politique de sécurité au CNRS et opérations de sécurité réalisées http://www.urec.cnrs.fr/

[2] CERT RENATER, (Computer Emergency Response Teams Réseau National de télécommunication pour la Technologie, l'Enseignement et la Recherche) en cas d'alerte envoyer un message à certsvp@renater.fr http://www.renater.fr/

[3] La sécurité, définition du TLF (Trésor de langue Française)

[4] De la formation: Support de Cours SIARS (Sécurité Informatique Administrateurs Réseaux et Systèmes) ouvrage collectif CNRS Janvier 2001 Ecole thématique Vcars (Vers des communications et des applications réseaux plus sécurisés) septembre 2002

[5] Nettiquette:Les règles de la Netiquette. Note : Ceci est la traduction française du RFC 1855 Netiquette Guidelines d'octobre 1995. www.sri.ucl.ac.be/SRI/rfc1855.fr.html

[6] Charte CNRS: Usage des ressources informatique et des services internet http://www.cnrs.fr/Infosecu/Charte.pdf février 1999

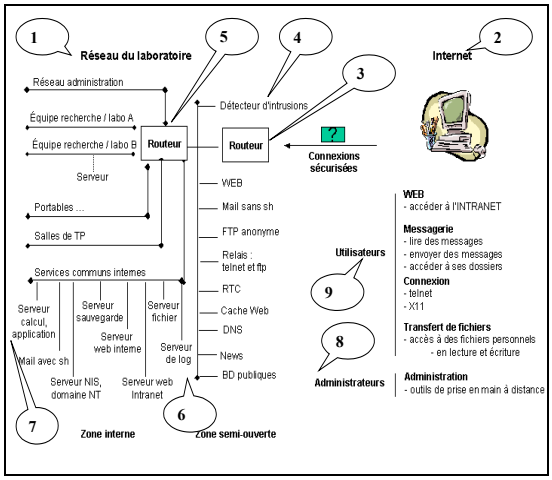
[7] La norme ISO 17799 est issue de la norme anglaise BS7799 créée en 1995 et révisée en 1999

la Méthode MEHARI[9], MARION[10], EBIOS[11] qui se décomposent en 4 parties: *L'étude du contexte, l'expression des besoins de sécurité, l'étude des risques, l'identification des objectifs de sécurité.*
Ces méthodes doivent permettre de structurer votre démarche pour atteindre les objectifs qui vous sont fixés ou pour créer vos différents scenarii si vos besoins sont divergents.

2.2 - Sécuriser votre architecture réseau

Cela consiste à structurer ou restructurer vos différentes ressources et, le cas échéant, de procéder à des séparations physiques avec des zones particulières (DMZ, zone semi-ouverte qui vous permet de placer des services communs, comme la messagerie qui est accessible de l'extérieur) et peut être de les rendre étanches avec d'autres parties de votre réseau par la mise en place de VLAN ou plus particulièrement de construire des réseaux logiques (par ports ou par adresse MAC) via les équipements commutateurs. D'autres équipements sont nécessaires pour vous permettre d'assurer du filtrage après la connaissance des flux entrants et sortants de votre réseau. Là encore, il ne s'agit pas d'entraver le fonctionnement des utilisateurs, mais de placer les règles fonctionnelles par exemple sur votre Routeur avec des ACLs (Acces List Control) dans un contexte statique[12], ou CBAC dans un contexte dynamique[13]. Ou encore avec d'autres équipements comme un pare feu (FIREWALL) et de vérifier ces règles avec des outils de simulation d'intrusion comme NESSUS[14], Internet Scanner[15]. Pour d'autres cas vous pourrez ajouter et utiliser des protocoles et mécanismes de cryptographie[16] et des solutions contre les virus (Amavis pour le serveur de messagerie).

Figure (1) *exemple d'architecture: © 2002 – Ouvrage collectif Cours SIARS Sécurité informatique pour les Administrateurs Réseaux et Systèmes / CNRS/UREC (les chiffres dans les bulles renvoient aux différents chapitres de l'ouvrage)*



2.3 - Sécuriser vos systèmes

De très nombreux systèmes sont encore par défaut accessibles à tout le monde, voire pour certains sans possibilité de mettre en œuvre de la sécurité, ou les mécanismes d'authentifications sont peu robustes par rapport aux critères harmonisés pour l'évaluation de la sécurité des systèmes et produits comme ITSEC[17]. Y insérer un mécanisme d'Imputabilité (Accountability), c'est à dire une fonction destinée à enregistrer l'exercice du droit à effectuer des actions engageant la sécurité pour pouvoir remonter à leur auteur seraient un peut plus dissuasif pour éviter la plupart des problèmes. Pour commencer, il faut choisir un système de fichier qui permette de prendre en compte la sécurité (ntfs, ext2fs, …), ensuite vous partagez votre disque en différentes partitions (systèmes, données). Après avoir fait le choix de votre système qui doit permettre une authentification Vous porterez une attention particulière à l'utilisation de l'administrateur (root) qui donne beaucoup de privilèges. Pour l'ensemble des systèmes d'exploitation, il faut y apporter des restrictions supplémentaires sur la propriété et les droits (écritures, lectures, exécution) de certains fichiers et comme précédemment vous vérifiez vos actions avec des outils comme Cops, System Scanner, ou autres logiciels. Pour terminer vous pourrez filtrer l'ensemble des services et ports qui ne sont pas

[8] Démarche d'analyse des risques informatiques en 8 étapes: Source : http://memoireonline.free.fr/securiteinfo_ibm.htm

[9] Méthode MEHARI (MEthode Harmonisée d'Analyse de Risques): Source https://www.clusif.asso.fr/fr/production/mehari

[10] MARION: (Méthode d'Analyse de Risques Informatiques Optimisée par Niveau) méthode mise au point par le clusif dans les années 1993 http://www.clusif.asso.fr

[11] EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode publiée par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) en version 1.02 de février 1997

[12] ACL: fonction de filtrage des paquets. Ces filtres sont définis pour chaque interface en entrée et/ou en sortie exemple: www.dr15.cnrs.fr/Cours/ACL-Cisco/ex-config.html

[13] CBAC (Context-Based Access Control) page de test sur les CBAC du LORIA : Source http://www.loria.fr/services/moyens-info/securite/CBAC.html

[14] Nessus: Outils de sécurité nessus Marie Claude QUIDOZ présentation dans le cadre des opérations de sécurité CNRS 14 Mai 2002

[15] ISS: Internet Scanner Sécurity: Evaluation. Internet Scanner v5.1. www.loria.fr/services/moyens-info/securite/ISS.html

[16] SCHNEIER Bruce, Cryptographie appliquée, 2e édition, Vuibert Informatique, 2001

[17] l'ITSEC «Information Technology Security Evaluation Criteria» a été publié par une Commission Européenne. Cette commission regroupait les services de sécurité de quatre pays européens (France, Grande Bretagne, Allemagne, Pays Bas). Les critères du TCSEC sont inclus dans l'ITSEC sous forme de couples {mécanismes, assurance}. Pour l'ITSEC la sécurité porte sur 8 thèmes : identification, authentification, contrôle d'accès, imputabilité, audit, fidélité, continuité de service, échange de données

utiles sur votre machine, en remplacer certains par des plus sûr, exemple: l'utilisation du service Telnet peut être remplacer par SSH [Barrett et Silverman, 2002] et vous veillerez à apporter les différents correctifs systèmes (patch). Il est extrêmement important de choisir des mots de passes digne d'être un mot de passe car peu importe la méthode d'authentification que vous utilisez (Certificats[18], OTP[19], Kerberos[20] …) et le mécanisme (carte, jeton, …).Actuellement les mécanismes utilisant la biométrie (élément physique comme la main, les yeux, ou d'autres moyens issus du comportement de la personne comme la voix, la signature) sont encore peu fréquent, donc en bout de chaîne c'est à 95 % un mot de passe qui est utilisé et il existe beaucoup d'outils pour les découvrir (Crack, Loopcrack, …). Pour construire votre mot de passe le conseil est de concaténer l'initiale de chaque mot d'une phrase en mixant majuscules et minuscules et un utilisant des symboles ou de la ponctuation et en rajoutant des chiffres.

2.4 - Sécuriser vos données

L'ensemble de l'information est numérisé, quelle que soit la nature de cette information, elle doit être sauvegardée. Il est invraisemblable de constater encore aujourd'hui le nombre d'utilisateurs qui ne sauvegardent pas leurs données ! Il existe une multitude se solutions (disquettes, archivage par Cdrom, …) et votre système d'information doit obligatoirement vous proposer des solutions en fonction de la quantité et du type d'informations. Néanmoins vous devez rester vigilent sur le lieu (support, serveur) de stockage de cette information car à l'ère du numérique cette information peut se retrouver sur Internet. Protéger vos documents électroniques contre une lecture non autorisée, contre des modifications intempestives, contre des impressions non désirées... Même ceux que vous destinez à des partenaires extérieurs, éventuellement distribués par Internet. Il est fortement conseillé de mettre un anti-virus sur votre poste de travail avec une mise à jour des signatures. Après quoi, vous pouvez utiliser les applications du chiffrement pour avoir un accès sécurisé aux données[21].

[18] Certificats: Un Système d'authentification avancé basé sur la technique

[19] OTP: One time Password Un Système d'authentification avancé basé sur la technique du mot de passe à usage unique:http://www.ietf.org/html.charters/otp-charter.html 2001-07-31: www.faqs.org/rfcs/rfc2289.html

[20] Kerberos: C'est un protocole d'authentification en réseau conçu par le Massachussetts Institute of Technology. Son but est de permettre l'échange sécurisé de données sur un réseau RFC-1411 RFC-1510 Kerberos: The Network Authentication Protocol

[21] L'accès sécurisé aux données Novembre 1999 Serge Aumont Comité Réseaux des Universités, Rennes Serge.Aumont@cru.fr, Roland Dirlewanger CNRS Délégation Aquitaine www.cru.fr/securite/crypto-jres99.pdf

3 - LA SECURITE DANS VOTRE SYSTEME DE VEILLE

Votre système de veille doit s'intégrer dans votre système d'information, c'est à dire qu'il doit prendre en compte la mise en œuvre et le niveau de sécurité réalisée, même si cela peut paraître paradoxal de solliciter plus particulièrement l'anonymat[22], afin d'éviter à votre concurrent de connaître la teneur stratégique de votre veille ou encore la cybersurveillance qui se trouve au cœur du processus de travail[23] [24] par rapport à des notions telles que la confidentialité, l'intégrité, la disponibilité, l'authentification plus ou moins forte pour autoriser la diffusion de votre veille.

3.1 - Votre anonymat

Au titre de l'enjeu économique qui nécessite des indicateurs et des statistiques. Du bon fonctionnement de votre ordinateur qui peut être client ou serveur d'information. De l'utilisation des différentes applications et services, qui impliquent le suivi de nombreux événements. Au titre de nombreux éléments comme la sécurité, la gestion, la rapidité des débits de l'information avec l'utilisation des mécanismes de caches (Proxies), votre environnement informatique génère et stocke de nombreux événements. Voilà bon nombre d'informations et d'événements qui marquent votre passage tant au travers du réseau que sur votre poste de travail. Ces fichiers dédiés pour journaliser sont appelés fichiers de log. Par conséquent votre anonymat reste éphémère et ceci malgré le droit légitime et légal[24]. La méconnaissance ou la non transparence des traitements de l'information du fonctionnement de votre environnement (systèmes, applications, réseaux) peut se trouver à l'origine de cette conviction fausse que les connexions sont anonymes. Pour votre courrier personnel, envoyez vous que des cartes postales? Qui sont les différents acteurs qui vont pouvoir exploiter, reconstituer votre activité, analyser votre comportement et plus si affinité …

Tout comme dans la vie de tous les jours où la vidéo-surveillance est omniprésente, vos télécommunications qui vous positionnent au mètre près et à la seconde, ou l'utilisation de votre carte bleu en dit long sur vous! Attention! Internet n'échappe pas à la règle. On vous observe à l'insu de votre plein gré.

[22] Anonymat:référence aux différents dossiers sur http://www.anonymat.org

[23] Rapport d'étude et de la consultation publique: La Cybersurveillance des salariés dans l'entreprise Hubert BOUCHET Mars 2001 htpp://www.cnil.fr

[24] légitime et légal http://www.droit-technologie.org

3.1.2 - Principe d'identification et d'échange d'information sur Internet

3.1.2.1 - Principe d'identification

Actuellement, l'ensemble des mécanismes, postes de travail, équipements réseaux, serveurs, et autres, …, utilisés pour l'échange d'informations sur Internet stockent des informations plus ou moins liées à votre identification. Le principe de fonctionnement d'Internet est l'adoption des règles ou protocoles de communication communs à tous tel que: Internet Protocol (IP, RFC[25]: 791) qui qualifie l'unicité d'une ressource via une adresse. Dans notre cas ce numéro IP (votre adresse d'identification) est codé sur 16 bits: exemple 193.49.100.10. Votre poste de travail interconnecté sur le réseau sera qualifié par ce type d'adresse. Dans le cas personnel et plus particulièrement chez vous cela sera via votre numéro de téléphone, par la connexion avec votre modem et votre prestataire attribuera temporairement un identificateur. Dans le cas ou celui-ci sera directement raccordé sur le réseau, par la carte réseau à l'intérieur de votre ordinateur, l'identification de celui-ci se fera par ce numéro IP et une adresse supplémentaire (MAC Adresse) qui, elle aussi, qualifie l'unicité de votre carte réseau. Donc, par association votre anonymat n'est absolument pas préservé. Par exemple, si vous utilisez votre poste de travail à une heure donnée: Votre poste de travail est identifié par une ou plusieurs adresses donc: *Votre Authentification personnelle = login + mot de passe Sur le poste de travail à un instant (t) = adresse du poste (adresse IP, MAC, Tél.)*

Ensuite, il suffit de consulter les bases publiques d'attribution des adresses IP et des noms de domaine comme : *http://www.iana.net, http://www.ripe.net pour l'Europe http://www.arin.net pour les Etats-Unis*.

Une autre possibilité de vous identifier extrêmement facilement est votre adresse de messagerie électronique. Celle-ci, donne votre Prénom et Nom par un mécanisme d'alias dans la plupart des cas. Sans évoquer l'entête de votre message que peu d'utilisateurs regardent et qui contient, là encore, un certains nombres d'informations, tout comme les suffixes (sous domaine, domaine) qui qualifient l'organisation à laquelle vous appartenez et sa situation. Exemple d'adresse de messagerie: Prenom.Nom@sous-domaine.domaine.fr

[25] RFC: The Requests for Comments, ensemble de notes techniques et d'organisation au sujet de l'Internet: http://www.rfc-editor.org/go.html

Tout comme votre poste de travail qui possède bien d'autres identifiants en fonction du système d'exploitation et des applications utilisés (UID, …). Les applications programmées en VbScript ou ActiveX peuvent lire la base de registre de votre système qui contient bon nombre d'informations pouvant vous identifier. C'est la même chose pour les scripts en PHP, PERL (langage de programmation), qui peuvent accéder à bon nombre de documents et d'informations pouvant vous identifier comme avec l'ensemble des fichiers «logs». Nous trouvons d'autres techniques d'identification avec les «espiogiciels» (SpyWare), applications qui envoient des informations à votre insu, par les écoutes des télécommunications (le réseau ECHELON [27], pour ne citer que lui), les «cookies» qui sont des fichiers d'informations déposés par le serveur sur lequel vous naviguez, les «web bugs» images pratiquement invisibles (1 pixel) qui sont téléchargées automatiquement et provoquent la connexion à un site distant. La fonction d'effacement (Delete, rm, …) pour certains systèmes est assez illusoire!

3.1.2.2 - Principe d'échange d'information sur Internet

Dans la forme la plus simple, prenons une application comme par exemple votre navigateur Netscape ou IE, client qui émet une requête sur un serveur d'information. Ce processus entre votre client et votre serveur est identifié par un port qui dans notre cas est assigné par défaut. Donc ce flux de données entre votre navigateur et un serveur d'information est qualifié par le port 80. Tout comme le port 443 sera assigné au même type de flux mais sécurisé. Ce procédé de réception et d'émission peut être exécuté simultanément. Autrement dit, plusieurs applications peuvent fonctionner simultanément (messagerie, navigateur, …). Donc, ce duo information: l'adresse Ip et le port du service utilisé, constitue une «socket», indispensable pour arriver à joindre le bon service sur le bon serveur et traduit:
L'unicité du numéro IP qui qualifie l'émetteur d'un coté et le récepteur de l'autre coté.
L'unicité de l'association d'un port et d'un numéro IP (Socket) qui permet de distinguer les différentes sources de données.

3.1.2.2.1 - Méthodes pour véhiculer l'information : le push et le pull

La Technologie «Pull» (tirer en Anglais) consiste à aller chercher les informations. C'est ce que nous faisons lorsque nous utilisons les moteurs de recherche et que l'on navigue sur le Web ou lorsqu'on télécharge des fichiers. Dans ce cas, nous faisons l'effort de recherche et nous décidons qu'elle

est l'information que l'on va simplement consulter ou bien que l'on va sauvegarder sur notre disque. Pour les serveurs, cette méthode consiste à être passif et à servir l'information lorsqu'elle est sollicitée. Attention! le Spam[26], c'est à dire les messages publicitaires dans les boîtes de messagerie, ainsi que les bandeaux publicitaires sur les pages Web ne correspondent pas à une attitude passive de la part des serveurs.
La Technologie «Push» (pousser en Anglais) permet à l'utilisateur de recevoir automatiquement l'information. Pour ce faire, il suffit de s'abonner, c'est à dire donner ses références (information personnelle). Par exemple, votre adresse de messagerie qui peut être revendu au plus offrant?

3.2 Méthodes et solutions pour conserver l'anonymat de votre système de veille.

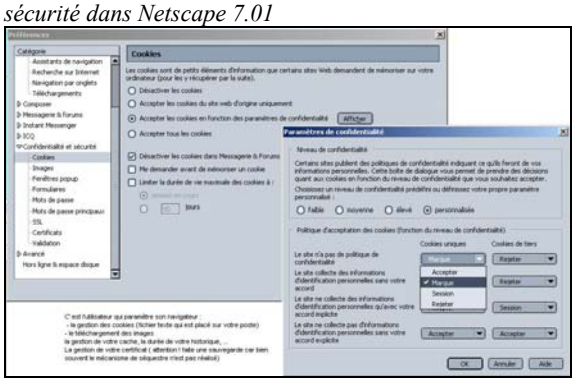
L'ensemble des méthodes utilisées et les différents outils, nécessitent de votre part une compréhension du mécanisme ou des mécanismes pour les utiliser correctement. A titre d'exemple, prenons l'utilisation de vos navigateurs (figure 2) qui par défaut ne filtre rien et que pratiquement personne ne paramètre. Donc il ne paraît pas opportun de citer des listes exhaustives d'outils spécialisés. Néanmoins, au travers de ces solutions, il vous sera aisé de les trouver avec des moteurs de recherche.

3.2.1 - Votre poste de travail

Une des solutions extrêmement simple consiste à utiliser la fonction de verrouillage de votre système d'exploitation dés lors que vous interrompez votre travail. Vous pouvez utiliser ensuite des outils d'effacement si votre système n'assure pas correctement cette fonction. Après quoi, vous mettez l'accent sur les différents fichiers d'événements. Pour augmenter ce niveau, il vous reste à utiliser des mécanismes de cryptographie, mais attention! Cela nécessite l'utilisation d'un mot de passe avec la problématique des mots de passes (oubli, et autres,…). On rencontre de plus en plus d'outils de rapport d'erreur ``Error Reporting Tool'' qui transmettent, via Internet, des informations en cas d'erreur non récupérable. Cette fonctionnalité est justifiée par l'accélération du cycle de correction des problèmes. L'ennui, c'est que ce dispositif communiquerait parfois trop d'informations concernant votre machine et bien d'autres encore[27].

Concernant l'utilisation de votre messagerie[28], la première chose est de paramétrer celle-ci en tenant compte de la sécurité. Si possible d'utiliser des protocoles sécurisé comme pops, imaps. Il existe différents outils pour esquiver le problème en dissimulant son adresse, mais cela n'est pas satisfaisant pour un contexte professionnel. Actuellement le processus de messagerie permettant de diffuser de l'information en toute sécurité passe par l'utilisation d'un certificat numérique avec les mécanismes de signature et chiffrement.
La configuration de votre navigateur, par exemple, nécessite de paramétrer la confidentialité et la sécurité que vous souhaitez, tant dans la gestion de vos mots de passes, des cookies, de votre cache, que la durée de votre historique, que l'utilisation de certains scripts ou encore en effectuant une sauvegarde de votre certificat.

Figure (2) *Exemple: Paramètres de confidentialité et sécurité dans Netscape 7.01*



3.2.2 - Utilisation des mécanismes d'adressage dynamique et de translation d'adresse

Le protocole DHCP (Dynamic Host Configuration Protocol, et les incontournables RFC: 951, 1497, 1541, 1542, 2131, 2132.) permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Ce qui est intéressant dans ce mécanisme c'est l'envoi d'une configuration donnée pour une durée donnée à un client donné. Donc, si vous sollicitez une nouvelle demande, votre configuration peut être changée.
La fonction de translation d'adresses (Network Adresse Translation, RFC:1631) est très utile pour rendre invisibles de l'extérieur les machines d'un réseau local ayant un plan d'adressage privé. Cette fonction est généralement implémentée sur un routeur ou éventuellement un firewall. Si ce mécanisme cache l'identité réelle des machines, et rend la traçabilité de bout en bout extrêmement

[26] Le Spam: Envoi massif, et parfois répété, de courriers électroniques non sollicités,http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm

[27] Article 8 de la Convention Européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit http://www.justice.gouv.fr/textfond/europ1.htm

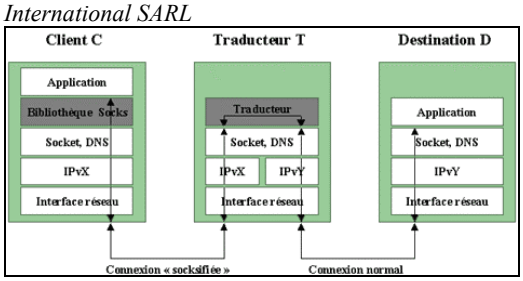
[28] Des solutions et outils: http://websec.arcady.fr/, Protection de la vie privée http://www.anonymat.org/ , http://security.tao.ca/francais/index.html

difficile, par contre elle réduit les possibilités de communications sécurisées au sens cryptées.
Il est conseillé d'analyser ces mécanismes avec l'administrateur de votre système, pour leur mise en œuvre.

3.2.3 - Les services Proxies et Gardes-barrière

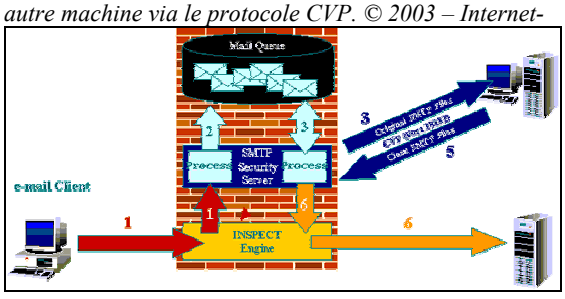
Dans notre cas le principe consiste à passer par un ordinateur relais dit «proxy», intermédiaire entre vous et le site qui adressera son adresse IP et non la votre. Ils existent un certain nombre de logiciels gestionnaires de proxies (les plus sollicités sont de type: «Proxysock», proxy qui utilise le protocole Sock[29]).

Figure (3) *Utilisation d'un proxy Socks v5 comme traducteur d'adresses © 2002 - Hermitage Technologies International SARL*



Dans ce principe vous pourrez utiliser plusieurs proxies en cascade. Exemple: http://proxy1/http://proxy2:80/proxy3:80/http://www.votremoteur de recherche.fr. Il existe différents sites qui proposent ces services à titre gratuit ou payant.
Les Gardes-barrière (Firewall ou pare feux) doivent répondre à une combinaison de filtrage (statique ou dynamique). C'est à dire qu'il vont examiner les données jusqu'au niveau applicatif. Il doive associer de l'authentification et avoir une fonction de relais applicatif. On les trouve sous différentes formes: comme un ensemble de boîtes à outils (TIS), des produits logiciels (Firewall-1, ZoneAlarm,) et des produits matériel (PIX).

Figure (4) *Cet exemple montre comment le Firewall-1 de CheckPoint délègue le contrôle de contenu sur une autre machine via le protocole CVP. © 2003 – Internet-*

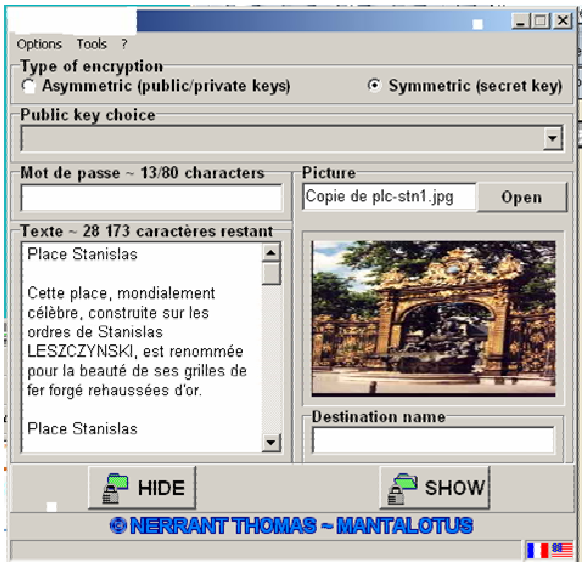


[29] SOCKS: (RFC: 1928,1929) présentation du protocole Sockc: http://www.socks-proxy.com/socks5/index.html

3.2.4 - Les services de cryptographie sur votre poste

PGP[30] [Barett et Silverman (2002)] est le logiciel le plus connu dans le domaine de la protection des données sur Internet. Il est souvent utilisé pour protéger le courrier électronique.
La stéganographie [Barett et Silverman (2002)] qui permet de cacher ou dissimuler des informations dans une image, ou plus généralement dans un flot de données redondantes. Une information qui n'a pas l'air d'être cryptée n'a aucune raison d'être décryptée. Cela pourrait être utilisé pour réaliser un Filigrane ('watermarking') ou un Canal de communication secrète ('cover channel')

Figure (5) *exemple de dissimulation d'un message dans une image avec l'outil Stéganozorus*



Méthodes et solutions pour assurer : la confidentialité, l'intégrité et l'authentification.
Bon nombre de services et de protocoles vont ou sont remplacés par d'autres qui offrent en plus de la cryptographie, de façon à renforcer la sécurité ou en apporter (par exemple pour le réseau: Ipsec[31], IPv6, pour le transport : TLS/SSL[32], application: SSH)
Pour des échanges de confiance au sein d'une communauté dite "ouverte", par exemple Internet, on peut utiliser un autre type de modèle de confiance reposant sur l'existence d'une "autorité centrale" nommée autorité de certification[33],

[30] PGP: OpenPGP est un standard de chiffrement dont le nom vient du logiciel "Pretty Good Privacy"® ou PGP®, un outil de cryptographie forte créé en 1992 sous l'impulsion de Philip Zimmermann, et qui était à l'époque gratuit, d'une grande robustesse cryptographique, et particulièrement bien adapté à l'utilisation sur Internet http://www.openpgp.fr.st/

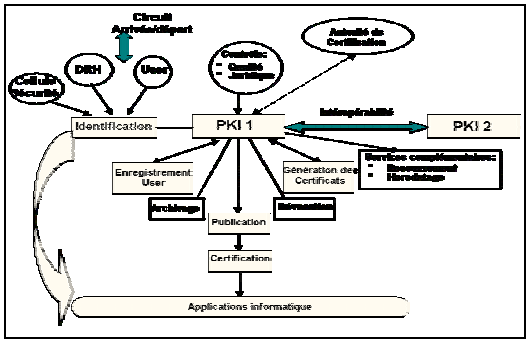
[31] IPSec : Utilisateurs nomades et IPSec François Morris https//:www-ext.lmcp.jussieux.fr/informatique/IPSec/IPSec.htm 29/10/2002

[32] OPENSSL Network security with OpenSSL O'REILLY

[33] IGC: Infrastructure de Gestion de Clefs du CNRS http://igc.services.cnrs.fr/doc/html/doc-certif.html Décembre 2002, version 1.5.1 http://www.urec.cnrs.fr/igc/CNRS-IGC/

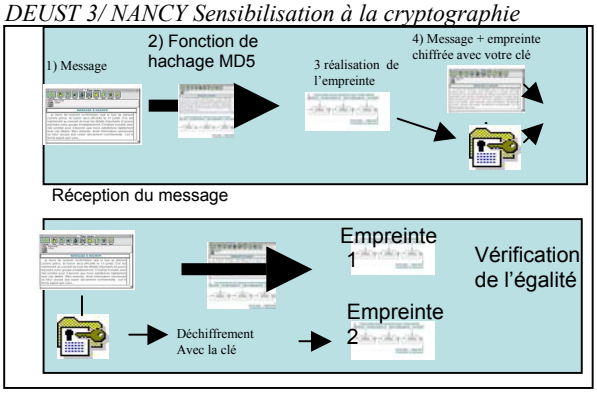
laquelle émet des certificats et est supposée digne de la confiance des utilisateurs. Ce modèle présente une analogie par rapport à notre société (obtention d'une carte d'identité, …).

Figure (6) *Infrastructure de Gestion de clé © 2003 – Internet-*



La signature numérique est un procédé de cryptologie très largement utilisé pour authentifier des documents et générer des signatures électroniques. Prenez votre message, réalisez un condensé avec une fonction de hachage (empreinte) que vous cryptez avec la clé publique de la personne et vous envoyez l'ensemble à cette personne. Cette personne recommence la même opération avec le message (réalise une empreinte) et vérifie l'égalité des 2 empreintes en décryptant l'empreinte envoyée avec sa clé privée. Ce mécanisme assure l'intégrité du message. Avec l'ajout de votre certificat vous assurez l'authentification, donc, l'équivalent d'un acte authentifié dont le contenu n'a pas été changé. Pour ajouter la confidentialité, vous pourrez générer un message chiffré [16].

Figure (7) *Mécanisme d'intégrité © 2003 – Cours DEUST 3/ NANCY Sensibilisation à la cryptographie*



4 - LES DIFFERENTS ACTEURS

Les éditeur de logiciels, firmes commerciales, hackers, pirates, régulateurs, activistes du Web indépendant, cyberpoliciers, dirigeants, administrateurs, utilisateurs, tels sont les noms par lesquels on peut désigner les différents acteurs qui aujourd'hui construisent, s'affrontent, s'enrichissent, à l'intérieur d'Internet.

Tous ces acteurs ont le seul point commun d'utiliser ou de s'exprimer par ce média qu'est «Internet»

Les acteurs économiques - Les acteurs économiques ont réussi à impulser la logique marchande à l'intérieur d'Internet et du Web. Il a surtout été question de «start-up», de valorisation boursière gigantesque et d'enrichissement ultra rapide des fondateurs et dirigeants. Cette approche est aujourd'hui prédominante et pourrait laisser penser qu'il n'y a qu'un seul modèle. Cependant ils tendent à augmenter le niveau de sécurité dans le contexte transactionnelle.

Les hackers - Il existe différents types de personnes derrière cette désignation : les bons, les moins bons, mais le point commun c'est qu'ils n'hésitent pas à recourir à des actions illégales pour essayer de prendre les droits de l'administrateur. Eux aussi connaissent très bien les mécanismes, les outils, et les failles existantes.

Les activistes et régulateurs - Les activistes du Web indépendant dénoncent les stratégies des régulateurs qui veulent imposer la censure sur le Web. Ce qui implique du bruit ou de la bande passante consommée.

L'administrateur - Docteur pour certains, pompier pour d'autres, dont l'émergence d'un techno pouvoir au travers de la connaissance de cette technologie gêne un peu les décideurs car elle ne cesse de croître à tel point que si eux-mêmes n'effectuent pas une veille régulière ils sont très vite dépassés par les événements. Notons l'évolution croissante de la demande en matière de sécurité vers l'évolution de métiers comme celui de responsable sécurité du système d'information (RSSI). Encore faut il clarifier quelques notions de droit et responsabilité.

Les utilisateurs ou internautes qui réclament leur part, doivent comprendre ou apprendre, pour utiliser cet espace de «liberté», mais en respectant les règles et une certaine déontologie qu'il faut de temps en temps rappeler.

5 - CONCLUSION

Votre système de veille, au même titre que tout système doit garantir un minimum de sécurité et le niveau de sécurité souhaité doit être pensé dès son origine. Il ne doit en aucun cas altérer l'environnement dans lequel il se trouve. Pour cela, il n'existe pas une solution mais des solutions, en fonction du niveau de sécurité que l'on veut atteindre, des risques et du coût. La mise en œuvre et l'optimisation de ces solutions passent par des compétences et ressources humaines que l'on a toujours tendance à minimiser. La gestion de l'information événementielle du système se doit d'être transparente. Il n'est pas concevable de faire

de la cybersurveillance[34] au titre du fonctionnement. Ce qui est extrêmement important c'est de connaître quel type de traitement va subir cette information et son but avoué ou inavoué.
Actuellement, on sollicite beaucoup de mécanismes utilisant la cryptographie qui repose sur le partage d'un secret (clé) se traduisant le plus souvent par l'utilisation d'un mot de passe qui ne possède pas la même robustesse. La tendance actuelle est la mise en œuvre des certificats électroniques (cartes d'identités) qui sont des composants très utiles, voire indispensables, de la confiance sur Internet. Mais, en fin de compte, nous devons toujours nous demander sur quoi repose la confiance que nous attribuons. Les solutions techniques n'apportent pas forcément toutes les réponses à tous les problèmes et il faut quelquefois utilisé le cadre Juridique.

BIBLIOGRAPHIE

Barrett D. J., Silverman R. E., *SSH le Shell sécurisé*, O'REILLY, février 2002

Schneider B., *Cryptographie appliquée*, 2ème édition, Vuibert Informatique, 2001

[34] Rapport d'étude et de la consultation publique: La Cybersurveillance des salariés dans l'entreprise Hubert BOUCHET Mars 2001 htpp://www.cnil.fr