H A D O P I

HAUTE AUTORITE POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES DROITS SUR INTERNET

SPECIFICATIONS FONCTIONNELLES DES MOYENS DE SECURISATION ET CONSIDERATIONS ORGANISATIONNELLES

VERSION APRES LA CONSULTATION OUVERTE JUSQU'AU 30 OCTOBRE 2010

4 RUE DU TEXEL
75014 PARIS

SPECIFICATIONS FONCTIONNELLES DES MOYENS DE SECURISATION ET CONSIDERATIONS ORGANISATIONNELLES

VERSION APRES LA CONSULTATION

Les spécifications fonctionnelles pertinentes rendues publiques par l'Hadopi permettront d'évaluer la conformité des moyens de sécurisation et leur efficacité, dans le cadre de la procédure de labellisation prévue à l'article L. 331-26 du code de la propriété intellectuelle (CPI).

Le présent document contient un nouveau projet de spécifications fonctionnelles ainsi des considérations organisationnelles en termes de sécurité, selon une approche définie en page 18 (« organisation du document »).

TABLE DES MATIÈRES

INTRODUCTION

L'HADOPI ET LES MOYENS DE SÉCURISATION

Dans le cadre de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, l'Hadopi s'est vue confier une mission de protection des œuvres et des objets auxquels est attaché un droit d'auteur ou un droit voisin à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne (article L331-13 2° CPI).

Deux axes de cette mission concernent les moyens de sécurisation :

- la mise en œuvre d'une procédure dite de « réponse graduée » incitant les titulaires d'un abonnement internet à l'utilisation de moyens de sécurisation ; et

- la labellisation par l'Hadopi des moyens de sécurisation conformes à des spécifications fonctionnelles publiées par elle.

LA REPONSE GRADUEE

La réponse graduée repose sur l'obligation du titulaire d'un accès à internet de veiller à ce que cet accès ne soit pas utilisé à des fins de contrefaçon (article L336-3 CPI).

Elle a pour objectif d'inciter les abonnés à changer de comportement afin que leur accès internet ne soit plus utilisé en violation des droits d'auteur.

À cet effet, il est prévu que sur saisine des ayants droit, la commission de protection des droits de l'Hadopi puisse adresser aux abonnés dont l'accès aura été utilisé pour mettre à disposition ou reproduire sans autorisation des œuvres protégées par le droit d'auteur, des recommandations rappelant les dispositions du code de la propriété intellectuelle. Ces recommandations sont adressées par courrier (électronique et postal) et:

- attirent l'attention des abonnés sur l'existence d'actes de contrefaçon commis à partir de leur accès ;

- invitent les abonnés à installer et à mettre en œuvre des moyens de sécurisation de leur accès à internet.

Dans le cas où l'accès à internet de l'abonné serait de nouveau utilisé à des fins de contrefaçon après deux recommandations dont la seconde est envoyée par lettre remise contre signature, la commission de protection des droits peut prendre la décision de transmettre le dossier au parquet.

L'abonné s'expose alors à un risque de condamnation pour négligence caractérisée dans la sécurisation de son accès internet.

Cette infraction est une contravention de 5ème classe, prévue à l'article R 335-5 du Code de propriété intellectuelle. Celle-ci peut être constituée lorsque, malgré la deuxième recommandation envoyée par l'Hadopi par lettre remise contre signature, un nouveau fait de contrefaçon est constaté alors que le titulaire de l'accès soit s'est abstenu de mettre en place un moyen de sécurisation de son accès internet, soit a manqué de diligence dans la mise en œuvre de ce moyen de sécurisation.

DÉFINITION DES TERMES

Mesures de sécurisation (MS)

Les mesures de sécurisation (dans la suite du document, désignés par MS) sont l'ensemble (technique et organisationnel) des méthodes et procédés, mis en œuvre pour sécuriser l'accès aux réseaux publics (internet, Réseaux de télécoms, etc.) sur les matériels de connexion (terminaux des utilisateurs, point d'accès, liens de communication, etc.) et leurs logiciels (système d'exploitation, protocoles, services, etc.) dans la chaîne de connexion.

Ces MS comprennent habituellement les dispositifs matériels de sécurité, les fonctions de sécurité des systèmes d'exploitation et des logiciels de base des équipements, les protocoles cryptographiques communément utilisés entre les équipements informatiques, les solutions de sécurité du marché pour sécuriser les postes de travail (identification, authentification, pare-feu, antivirus, contrôle parental, antispam, etc.). Ces MS sont imparfaits[1], ne garantissent pas une sécurité absolue, mais l'état de l'art en la matière toujours en évolution assure un niveau d'assurance de sécurité qui fait que ces boîtes à outils sont devenues indispensables. Ne pas les utiliser met l'utilisateur dans une situation périlleuse.

Ces MS comprennent également, dans les organismes collectifs, une charte informatique, des recommandations sur le comportement numérique et des mesures organisationnelles de sécurité dans le règlement intérieur de l'établissement.

Les MS concernent tous les abonnés pour la protection de leur réseau local privé connecté à l'internet, de leurs appareils de communication connectés aux réseaux sans fils et de leurs ustensiles informatiques connectés à un réseau public, afin d'empêcher l'intrusion par un tiers non autorisé dans un système électronique pour le vol ou la falsification de données personnelles ou l'utilisation des ressources informatiques à des fins malveillantes (indisponibilité, usurpation d'identité, etc.).

Ces MS traditionnels et nécessaires de sécurité informatique sont de plus en plus complexes et souvent difficiles à exploiter et à configurer par les utilisateurs non spécialistes. Ils sont en outre insuffisants pour gérer et préserver le patrimoine numérique des différents acteurs (utilisateurs, titulaires de droits, fournisseurs de services, fournisseurs de contenus, etc.) sur le réseau, notamment pour prévenir les utilisations non autorisées d'œuvres ou de documents.

Il est donc souhaitable, voire indispensable, pour compléter la panoplie des outils de sécurisation actuels, d'y adjoindre une Application supplémentaire (objet essentiel de ce document) qui n'est pas une application de sécurité proprement dite, mais qui vise à améliorer le niveau d'assurance de sécurité de son réseau local privé et une meilleure gestion d'usage des contenus dans ce réseau local. Cette Application vise le moyen de sécurisation mentionné à l'article L331-26 du CPI. Les spécifications fonctionnelles de l'Application comprises dans le présent document désignent ainsi les spécifications fonctionnelles des moyens de sécurisation mentionnés à l'article L331-26.

Cette Application comporte des modules :

[1] Force est de constater que les virus, les vers, les botnets et les spams se répandent toujours autant.

- pour faciliter la gestion de ces MS et aider à configurer ces MS afin de fournir davantage de sécurité au titulaire d'accès, et de l'aider à protéger davantage les machines des utilisateurs sous sa responsabilité,

- pour aider le titulaire de l'abonnement et les utilisateurs dans la gestion et l'exploitation des services, des logiciels et des protocoles applicatifs, qui risquent d'entraîner une utilisation à des fins de contrefaçon,

- pour observer et traiter (laisser-faire, ralentir ou bloquer) les flux entrants et sortants des interfaces de réseau des postes terminaux des usagers, et signaler (optionnellement) au titulaire de l'accès à internet (et éventuellement à l'utilisateur) les commandes des utilisateurs susceptibles de soulever des difficultés, et

- pour administrer cette Application, notamment pour enregistrer optionnellement les événements significatifs relatifs à cette Application dans des journaux.

Les MS sont donc composés à la fois des mesures techniques (notamment cette Application supplémentaire et les outils de sécurité informatiques classiques, en support) et des mesures organisationnelles (politique de sécurité, charte, règlement, information, sensibilisation, identification des machines, éventuellement des utilisateurs) nécessaires pour la mise en vigueur d'une attitude vigilante et responsable à l'égard de l'utilisation d'un réseau local informatique connecté sur des réseaux extérieurs. Les mesures élémentaires d'éteindre son ordinateur, de posséder des comptes informatiques personnels avec des mots de passe sophistiqués pour chaque utilisateur autorisé font partie des mesures organisationnelles des MS.

Les MS avec cette Application supplémentaire sont définis par leur objectif[2] de faire en sorte qu'il n'y ait pas (dans la mesure du possible) de téléchargement illicite via l'accès au réseau public (internet, téléphonie mobile).

Le but de cette Application est essentiellement de d'éduquer à une fin d'utilisation des ressources numériques plus respectueuse de la propriété intellectuelle et à cette fin, fournir de l'aide pour élever le niveau de sécurisation de l'environnement informatique, de la responsabilisation des abonnés dans leur connexion aux réseaux extérieurs, de l'encouragement, si nécessaire, à une modification de la conduite numérique, quand un utilisateur persiste à réaliser des « téléchargements ludiques » voire des téléchargements illégaux massifs ou un délit de contrefaçon.

[2] Il est difficile de définir le caractère illicite d'un téléchargement, puisque le clonage est constitutif du numérique. Tel fichier peut avoir été téléchargé légalement, sa copie (son clone) pouvant être selon le cas, légale (copie privée) ou illégale.

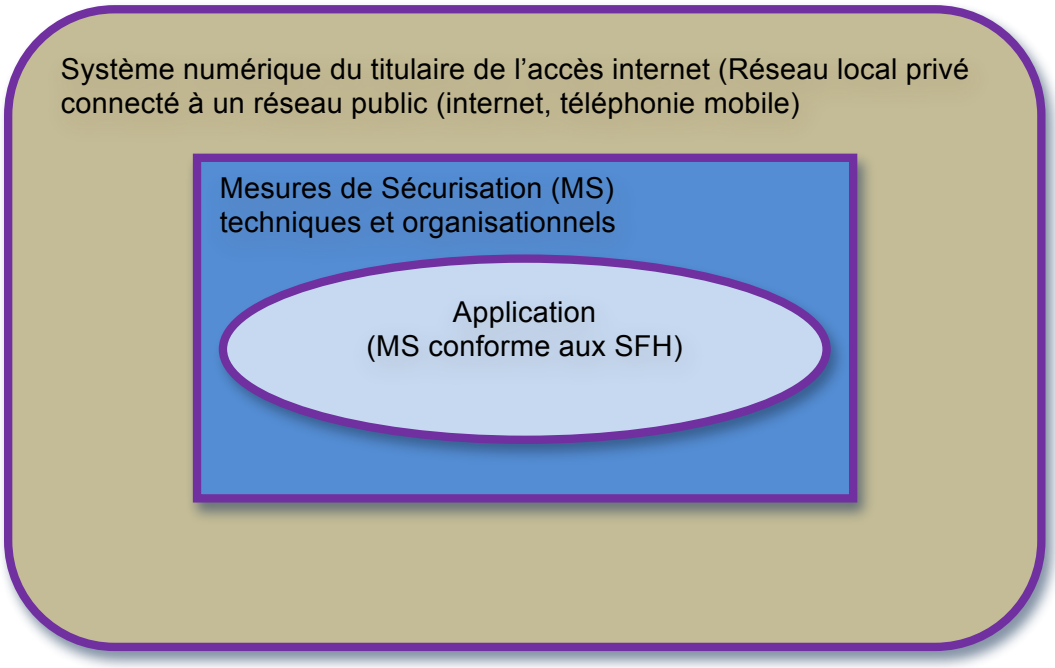

Figure 1: Mesures de sécurisation et l'Application supplémentaire conforme à SFH

Application conforme à SFH

Une application conforme à SFH (dans la suite du document, désignée Application) est un dispositif matériel et/ou logiciel qui s'appuie sur les outils de sécurité éprouvés du marché ou de la communauté du logiciel libre des Systèmes d'Information et des réseaux, afin de répondre aux spécifications fonctionnelles SFH, objet de ce document. Cette Application (matérielle et/ou logicielle, centralisée ou décentralisée) est hébergée en totalité dans les postes des utilisateurs, ou avec une partie seulement sur les postes et une partie dans le point d'accès, ou complètement en dehors des terminaux des utilisateurs sur une station de supervision spécifique du réseau local ou bien encore dans le point d'accès (boîtier ADSL).

Cette Application comprend des modules, décrits dans la suite de ce document, pour assurer la partie supplémentaire des mesures techniques des MS, en complétant les outils de sécurisation traditionnels, en support.

L'Application, à l'instar d'autres logiciels de sécurisation dédiés, a pour objectif de permettre à l'abonné soumis à une obligation légale de surveiller son accès Internet, de sécuriser cet accès afin que celui ne soit pas utilisé pour permettre des actes de contrefaçon. Les actes de téléchargement illégal de tout ou partie d'une œuvre (film, musique, livre, etc.) peuvent être le fait d'un tiers qui aurait utilisé de manière malveillante l'environnement informatique du réseau local ou bien par un utilisateur autorisé qui utiliserait tout moyen technique (des procédés de type pair-à-pair, de streaming, de téléchargement direct, de VPN…) pour se procurer une œuvre de manière illégale. L'Application vise à conseiller le titulaire de l'accès à internet dans la configuration et l'exploitation de ses MS pour sécuriser son accès aux Réseaux Publics (internet, téléphonie mobile, etc.) dans les deux sens montant et descendant. Elle a pour but de responsabiliser les internautes dans le sens d'une meilleure sécurisation de leur accès à internet.

C'est cette Application des MS qui doit être labellisée par Hadopi.

La composante technique originale de SFH s'appuie sur des moyens fournis par l'environnement. Par exemple :

- si l'Application est installée à domicile dans un ordinateur personnel, le protocole WPA2, la sécurité du boîtier, la sécurité du système d'exploitation font partie des MS ;

- si l'Application est installée dans une entreprise sur une station de supervision de réseau reliée à des sondes protocolaires, la sécurité du réseau local et les mesures organisationnelles prises pour les ingénieurs en charge du réseau font partie des MS.

Solution

Une Solution répondant aux MS (implémentation des MS) est un ensemble de mesures techniques et de mesures organisationnelles. Les mesures techniques comprennent une Application qui s'appuie sur les outils de sécurité traditionnels, exploitée et administrée directement par le titulaire de l'abonnement, ou indirectement sous sa responsabilité via des fournisseurs de services (FAI, Opérateurs de télécoms, Opérateurs de sécurité, etc.) et/ou des vendeurs d'équipements (vendeurs d'ordinateurs et/ou de logiciels, etc.) et/ou des éditeurs de solution de sécurité.

Une Solution répondant aux MS comporte nécessairement une Application qui est un produit ou un service.

Cette Application peut être un logiciel libre, développée et maintenue par la communauté du logiciel libre. Dans une organisation, elle est alors gérée par les ingénieurs du réseau qui assurent la bonne exploitation de l'Application. Chez un particulier, elle est sous la responsabilité du titulaire de l'abonnement.

La Solution s'applique au Grand Public (les particuliers et les TPE – très petites entreprises) et aux Professionnels (organismes collectifs), notamment les établissements publics et les entreprises[3].

Le titulaire de l'accès internet

Le titulaire de l'accès internet est la personne physique et/ou morale qui est le titulaire de l'abonnement à un réseau public (internet, Réseaux mobiles, etc.). Dans un foyer, c'est en règle générale une personne majeure (parent, membre de la colocation, etc.). Dans une organisation, il s'agit du signataire du contrat (le chef d'entreprise, le responsable de l'établissement). Dans la pratique, ce dernier peut confier la responsabilité informatique à une personne nommément désignée (un RSSI, un DSI, un DRH ou un informaticien qui gère le Système d'Information et les réseaux locaux et de télécommunication), laquelle est du fait de cette délégation l'Administrateur.

Dans la suite du document, on parle de titulaire de l'accès ou de l'abonnement.

Administrateur

L'Administrateur est le rôle de sécurité qui définit et met en œuvre la politique de sécurité, relative à l'obligation de surveillance prévue par la loi Création et Internet, dite loi

[3] Le renforcement du contrôle de l'employeur se traduira par des dispositions particulières dans la charte informatique de l'entreprise sans remise en cause des dispositions légales relatives à la vie privée sur le lieu de travail (confidentialité des conversations téléphoniques, etc.).

« Hadopi ». Il peut être le titulaire de l'abonnement ou une personne en charge de la politique de sécurité.

- Dans un foyer, l'Administrateur est en général le titulaire de l'abonnement, mais ce dernier peut confier ce rôle à une personne (par exemple, un membre de l'entourage, exercé en informatique) digne de sa confiance.

- Dans une organisation, l'Administrateur peut être le RSSI, le DSI, le DRH, un ingénieur réseau, un ingénieur système.

C'est l'Administrateur qui installe l'Application. Il prévient les utilisateurs de cette installation. Les utilisateurs sont simultanément sensibilisés à la loi Hadopi.

Utilisateur

Un utilisateur est une personne autorisée par l'Administrateur à utiliser les ressources informatiques du réseau local privé.

Dans la pratique, les SFH pour leur partie technique, traitent de machines qui ont des identifications (en général des adresses physiques et logiques) et des programmes logiciels qui sont identifiés (avec des licences ou autres) et des fichiers de données personnelles ou à caractère personnel qui ont des identifications. Il appartient donc à l'Administrateur[4] de s'assurer que les machines, les programmes et les fichiers sous son contrôle sont sécurisés pour être utilisés par des personnes autorisées.

Les utilisateurs sont des personnes sensibilisées au respect du droit d'auteur et à lutte contre la contrefaçon, essentiellement dans les organismes collectifs (institutions, entreprises, etc.), via une charte informatique et le règlement intérieur, mais aussi à domicile via des avertissements fournis par le FAI et par les éditeurs de l'Application. Un menu d'aide de l'Application peut rappeler à tout moment à l'utilisateur ces dispositions.

Éditeur de l'Application

L'éditeur de l'Application est la personne qui met l'Application, produit ou service, à la disposition du public, à titre gratuit ou onéreux.

Politique de sécurité

La Politique de Sécurité dont il est question dans ce document concerne la partie relative au dispositif prévu par les lois Hadopi[5]. Elle est intégrée dans la politique de sécurité globale définie par le titulaire de l'accès internet.

[4] À la maison, le titulaire de l'abonnement n'est pas forcément l'Administrateur car il n'est pas nécessairement la personne la plus mature en informatique. Le Responsable n'a même pas nécessairement de compte informatique sur un poste, encore moins sur tous les postes des proches de son entourage qui se connectent via sa liaison Wi-Fi à internet.

[5] La politique de sécurité des systèmes d'information (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration) en matière de sécurité des systèmes d'information (SSI). Il n'existe pas de PSSI Hadopi, mais les politiques de sécurité des systèmes d'information des organismes collectifs doivent désormais prendre en compte les divers éléments applicables de la loi

LA LABELLISATION DES MOYENS DE SECURISATION

Le législateur a confié à l'Hadopi une mission de labellisation des moyens de sécurisation.

La labellisation des moyens de sécurisation prévue à l'article L. 331-26 CPI s'inscrit dans le cadre de la mission générale de protection des œuvres confiée à l'Hadopi, car elle encourage le développement de moyens de sécurisation de l'accès à internet permettant de lutter contre les usages illégaux de contenu en ligne et identifie facilement ces moyens auprès des internautes souhaitant sécuriser leur accès.

Le label sera attribué au terme d'une procédure d'évaluation certifiée, définie aux articles R. 331-85 et suivants du code de la propriété intellectuelle, permettant de vérifier la conformité d'un moyen de sécurisation – désigné par « l'Application » dans ce document - aux spécifications fonctionnelles rendues publiques par la Haute Autorité ainsi que leur efficacité.

L'objet de ce document est de proposer un projet des spécifications fonctionnelles visées à l'article L331-26 CPI (Spécifications Fonctionnelles Hadopi ou « SFH ») ainsi que d'exposer des considérations d'ordre organisationnel en matière de sécurité (voir l'approche du document exposée en page 18)

Par spécifications fonctionnelles, il est entendu une description de l'ensemble des fonctions informatiques que doit offrir une instanciation de l'Application, qui peut être un produit ou un service, en vue de sa labellisation. La spécification fonctionnelle est indépendante de la façon dont sera réalisé l'Application en question.

Chaque fonction sera décrite, en spécifiant son but, son principe de fonctionnement, les données et les objets manipulés.

Les spécifications SFH relatives à la qualité générale sont aussi abordées dans ce document, c'est-à-dire :

- la performance attendue (contraintes de temps de réponse et de ressources informatiques utilisées, en processeur, en communication et en stockage), l'environnement informatique ;

- la sécurité exigée, en termes de protection de l'Application, et en termes de respect de la vie privée des utilisateurs et de sécurité des données à caractère personnel ;

- le déploiement de l'Application sous forme de produit ou de service tout au long de son cycle de vie (installation, maintenance, évolution, désinstallation).

Le document décrit les exigences attendues d'une instanciation de l'Application répondant aux spécifications SFH.

DIRECTIVES SUIVIES POUR L'ÉLABORATION DE SFH

Dans l'élaboration de ce document, il a été tenu compte des principes suivants :

- le respect du code de la propriété intellectuelle et notamment des lois dites « Hadopi »[6] :

  ⇒ l'Application fournit aux utilisateurs une aide pour respecter les droits des créateurs sur leur œuvres ;
  ⇒ l'Application fait appel à la compréhension des enjeux de la contrefaçon numérique ;
  ⇒ l'explicitation en termes informatiques de la notion de sécurisation dans ces SFH inscrit l'Application dans une logique d'aide à la sécurisation afin que ne soient pas commis d'actes de contrefaçon et non pas dans une logique d'application de sécurité ;

- la liberté des utilisateurs du numérique, le respect de la sphère privée du titulaire de l'accès internet et des utilisateurs :

  ⇒ l'Application des MS et les MS sont essentiellement une « boîte à outils », dans laquelle le titulaire de l'abonnement décide de la gestion et de l'utilisation de son propre écosystème numérique local, sous sa responsabilité ;

- le respect du patrimoine du titulaire de l'accès internet (matériels, logiciels et données associées) :

  ⇒ l'Application donne au titulaire de l'accès internet plus de visibilité sur son patrimoine numérique, à tout moment, qu'il s'agisse d'un particulier ou d'une organisation (entreprise ou autres) ;
  ⇒ l'Application renforce la responsabilité du titulaire de l'abonnement qui est un point clé de sa mise en œuvre ;

- la neutralité du réseau public :

  ⇒ l'Application ne peut pas être installée dans le cœur d'un réseau public ;
  ⇒ L'Application ne peut être gérée que dans un réseau local privé connecté à au moins un réseau public, sous la responsabilité du titulaire de l'accès à ce(s) réseau(x) public(s) ;
  ⇒ Si l'Application est opérée sous forme de service, à l'extérieur du réseau local privé, le titulaire de l'accès internet maîtrise à tout moment les paramètres de sa politique de sécurité et les informations protégées de son Application.
  ⇒ Pour certaines entreprises (avec de nombreuses agences), l'Application peut faire transiter de manière protégée des informations à travers le réseau public, mais à la connaissance et sous la maîtrise du titulaire de l'accès internet.

- La finalité et la proportionnalité de l'Application des MS ;

  ⇒ l'Application ne doit être utilisée que pour sa finalité et mise en œuvre dans le respect d'un principe de proportionnalité : aider le titulaire de l'accès internet à

[6] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet ; loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet.

sécuriser son accès et sa connexion, et aider à la prévention de l'accomplissement d'actes de contrefaçon ;
⇒ l'Application doit être légère et doit préserver la productivité de l'usager : elle doit consommer des ressources en proportion de l'objectif visé et ne doit pas importuner l'utilisateur dans son activité quotidienne ;
⇒ l'écosystème numérique se transforme vite et il convient que l'Application réponde de manière souple et proactive à l'évolution technologique et à l'appropriation souvent variable et parfois inattendue des technologies par les usagers.

Il a été tenu compte des objectifs clés suivants :

- l'établissement d'une politique de sécurité générique, universelle, pour les particuliers et les organisations :

  ⇒ les concepteurs et les opérateurs ont la possibilité de l'instancier pour les différentes cibles (particuliers, entreprises, établissements publics, associations, universités, hôpitaux, hôtels, cybercafé, etc.), et
  ⇒ les concepteurs et les opérateurs ont la capacité d'implanter des solutions évolutives dans la durée, d'ajuster la politique selon la taille de l'écosystème numérique (de 1 personne à des dizaines de milliers d'utilisateurs).
  ⇒ Cette politique de sécurité est adaptée et personnalisée par l'Administrateur de la sécurité (le titulaire de l'abonnement, le responsable de l'établissement – responsable RH ou DSI ou RSSI), afin de répondre de manière plus précise et efficace au contexte local des diverses situations présentées.

- la possibilité de suivi[7] infalsifiable de la politique de sécurité choisie par le titulaire de l'accès internet, ce suivi restant toujours maîtrisé par lui ;

  ⇒ l'Application lui fournit des arguments intrinsèques (examen de l'Application dans son contexte *a posteriori*) ou extrinsèques (examen des journaux de l'historique de l'Application) pour vérifier sa politique de sécurité choisie et suivie ;
  ⇒ à aucun moment le titulaire de l'accès internet n'est dessaisi de ses enregistrements des données d'historique d'utilisation des MS et il n'y a pas, pour la finalité de l'Application[8], d'enregistrement de la navigation d'un internaute (ex : désignation en clair des sites visités[9], noms de fichiers téléchargés…) ; cependant les URL visités et les noms des fichiers téléchargés en outrepassant la politique de sécurité, seront enregistrés dans le journal en clair ou dans le journal chiffré grâce à une fonction de hachage qui masquera les URL et les noms des fichiers téléchargés, afin de respecter la sphère privée des utilisateurs.

[7] Il faut que ce suivi soit lisible par toute personne, avec des explications claires : « adresse physique MAC non autorisée, présence éventuelle d'un tiers non autorisé sur la ligne ».
[8] Dans certains organismes collectifs, la politique de sécurité impose une surveillance de la totalité de l'historique, et ce par utilisateur : les principes de la finalité et proportionnalité de l'Hadopi n'imposent pas une politique aussi sévère.
[9] Il faut toutefois signaler et enregistrer les URL visités qui ont servis à un téléchargement illégal. On n'écrit alors que le haché des URL problématiques. Idem pour le nom du fichier problématique téléchargé : on n'indique que le haché du nom du fichier.

- les exigences de sécurité[10] à la hauteur de l'objectif visé ;

  ⇒ l'Application vise la grande majorité des abonnés pour les aider dans la difficulté de comprendre et d'exploiter leur système numérique local et d'utiliser avec précaution la connexion à des réseaux publics ;
  ⇒ l'Application n'est qu'un élément pour lutter contre le téléchargement illégal et favoriser l'offre légale ;
  ⇒ l'Application n'affronte pas la communauté des pirates informatiques qui souhaiteraient briser sa sécurité ou d'en empêcher son fonctionnement ;
  ⇒ l'Application n'affaiblit pas le niveau de sécurité de l'environnement informatique du titulaire de l'accès internet ; elle ne doit pas constituer un vecteur d'attaque contre un équipement du réseau local, ni la source d'une attaque contre d'autres environnements informatiques ;

- l'intégration possible dans tout environnement (y compris le domaine du logiciel libre) ;

  ⇒ l'Application peut être installée chez un particulier ou dans un organisme collectif ;
  ⇒ l'Application a vocation à être disséminée selon les divers modèles technologiques et économiques, à la pointe du progrès.

- la mise à jour régulière et obligatoire ;

  ⇒ l'Application doit s'adapter aux usages et à l'évolution rapide des procédés, en matière de contrefaçon ; les éditeurs devront faire évoluer leur produit ou leur service car la finalité de l'Application doit demeurer conforme à mesure que les usages et les comportements se modifieront et l'efficacité de l'Application doit rester conforme à son label.

[10] Une difficulté est de spécifier et concevoir la sécurité de ce produit/service. Dans les foyers, précisément, le titulaire souverain possède le produit et ses clés. Il faut donc que le produit s'auto-protège. On sait que les techniques d'assombrissement de code exécutables, d'insertion de code mort, de code chiffré et déchiffrable à la volée ne sont pas sûres à 100% et qu'elles ne font que retarder le déverrouillage.
Ce n'est pas le cas en entreprise, car dans ce cas, l'utilisateur final n'a pas accès au produit en entier puisqu'on sépare radicalement le rôle de l'Administrateur et le rôle de l'utilisateur. L'employé utilise et le responsable (ou l'opérateur) de sécurité (digne de confiance) gère.

TYPOLOGIE DES CONCEPTIONS D'ARCHITECTURES ET DE SOLUTIONS

ARCHITECTURE DES SOLUTIONS

Les présentes spécifications fonctionnelles n'imposent pas d'architecture.

L'Application (produit ou service) conforme aux SFH pourra être composée d'un ou plusieurs dispositifs matériels et/ou logiciels, dans une architecture centralisée et/ou distribuée, selon les solutions définies par les concepteurs.

Ces solutions peuvent être en réseau ou sur poste de travail.

Pour les vendeurs de solutions, le marché des particuliers et le marché des professionnels sont distincts pour de multiples raisons. Les architectures (centralisées ou non) et les modes (produit sous forme de licence ou bien service sous forme de contrat, avec obligation de moyens ou de résultats) des diverses solutions devront être adaptées à ces diverses cibles.

SPECIFICATIONS DES SOLUTIONS DE SECURITE EXISTANTES PERTINENTES

L'Application conforme aux SFH pourra emprunter des éléments aux spécifications des solutions de sécurité existantes mais devra les compléter et les adapter à l'objectif de prévention de l'accomplissement d'actes de contrefaçon.

Les pare-feu applicatifs et les filtres du Web

Les pare-feu sont des matériels (pare-feu pour les organisations avec de multiples connexions de la part de nombreux utilisateurs) et/ou logiciels (pare-feu dans des boîtiers ou pare-feu personnel sur un seul équipement terminal) qui appliquent une politique de contrôle d'accès dans toutes les couches des piles protocolaires. Un pare-feu analyse en temps réel le format des échanges, c'est-à-dire inspecte la syntaxe et la signature comportementale des piles protocolaires (les paquets, les sessions, les ports, etc.). Le pare-feu filtre les trames Ethernet, les paquets IP (en général, filtrage suivant les adresses source et destination), les ports de transport TCP ou UDP, les sessions, les protocoles applicatifs HTTP (pour la restriction des URL accessibles), FTP, SCP (transfert de fichiers), SMTP (pour lutter contre le pourriel), Telnet, SSH, etc. Un pare-feu inspecte le trafic entrant et sortant, et bloque ces flux, selon la politique de sécurité en vigueur sur l'ordinateur. Les pare-feu installés sur les machines personnelles identifient et vérifient le programme qui est à l'origine des données pour lutter contre les virus et les logiciels espions. Ils embarquent en général un serveur mandataire (« *proxy* ») pour analyser en profondeur certains contenus.

L'intégration de SFH dans des ensembles de sécurité élargis

Pour des raisons de réduction des coûts de développement et d'exploitation, de simplicité de gestion et d'usage, il est envisageable que l'Application conforme aux SFH soit intégrée dans les solutions de sécurité.

TYPOLOGIE DES SOLUTIONS SELON LE NOMBRE D'UTILISATEURS

L'Application conforme aux SFH pourra viser des environnements comptant un nombre plus ou moins important d'utilisateurs.

Les cibles d'utilisateurs des dispositifs de sécurité peuvent être classées en 2 grandes classes : les salariés, employés des entreprises, institutions, associations, (avec des clients et des visiteurs) d'une part et le grand public, les particuliers à domicile (avec des amis ou des invités) d'autre part.

Pour les organisations, il y a encore deux sous-catégories : les organisations qui ont du personnel permanent, identifié et les organisations comme les hôtels, les cybercafés, les sites Wi-Fi ouverts (aéroports, etc.) où les utilisateurs sont de passage (et parfois anonymes).

Une approche informatique pertinente est alors de distinguer les conceptions en fonction du nombre d'utilisateurs (de 1 à 10000) et de leur nature (employé ou visiteur), que le titulaire du contrat a sous sa responsabilité.

Il appartient au concepteur de produits (matériel et/ou logiciel) et/ou de service, de définir la typologie de solutions qui lui semble la plus appropriée.

ORGANISATION DU DOCUMENT

En accord avec les définitions de la section « Définition des termes », une Mesure de Sécurisation se compose d'un ensemble de mesures techniques, l'Application conforme aux SFH et d'un ensemble de mesures organisationnelles.

Il n'était pas possible dans ce document, qui spécifie l'Application (mesures techniques) correspondant au moyen de sécurisation prévu à l'article L331-26 CPI, de ne pas non plus aborder les mesures organisationnelles. Ces mesures complètent les mesures techniques d'un MS. Ainsi tout au long de ce document, les spécifications sont accompagnées de mentions et de réflexions concernant des mesures organisationnelles que le titulaire pourra mettre en œuvre.

Les SFH sont présentées tout d'abord, de manière générique, pour l'ensemble des solutions possibles. Ce chapitre décrit l'Application et le cadre dans lequel elle doit évoluer.

A la fin de la présentation générale des SFH, se trouve un chapitre récapitulant les fonctionnalités que l'Application conforme aux SFH doit posséder.

Sont ensuite décrits deux compléments de présentations plus spécifiques, l'une pour les organismes collectifs, l'autre pour le grand public et les TPE. Ces deux présentations déclinent des compléments d'information sur les spécifications en fonction des deux contextes, d'une part l'environnement professionnel (la sécurisation des systèmes d'information et réseaux professionnels) et d'autre part l'environnement personnel grand public (la sécurisation des petits systèmes d'information et le réseau local à domicile) et TPE (Très Petites Entreprises), en fait celles qui possèdent des configurations informatiques analogues aux foyers des particuliers.

Comme pour la présentation générale des SFH, après chacun des compléments se trouve un chapitre récapitulatif des fonctionnalités que l'Application conforme aux SFH doit posséder si celle-ci est destinée à un des deux contextes, organismes collectifs, grand public/TPE, abordés par les compléments.

SYNTHÈSE DES SPÉCIFICATIONS FONCTIONNELLES

L'Application n'est pas obligatoire ; elle peut être installée et/ou désinstallée, être activée et/ou désactivée, à tout moment sur le parc entier des équipements ou sur un sous-ensemble. Il est toutefois recommandé de l'installer et de l'activer pour aider à protéger tout le réseau de l'environnement informatique du titulaire de l'accès internet afin qu'il maîtrise davantage la sécurisation de son accès aux réseaux publics pour prévenir l'accomplissement d'actes de contrefaçon.

La synthèse des fonctionnalités pertinentes de l'Application des MS[11] est la suivante :

I - Mise en mémoire d'une politique de sécurité par l'Administrateur dont la mise en œuvre est décidée par le titulaire de l'accès internet ;

II - Cette politique est définie par le titulaire de l'abonnement en choisissant des règles et des procédures parmi un catalogue d'actions techniques possibles ; l'Application des MS doit offrir une grande souplesse de fonctionnalités et une granularité d'utilisation ;

III - La politique de sécurité s'appuie sur cinq éléments cumulatifs :

Élément 1 : Aide à la sécurisation de la connexion et de l'accès par une analyse statique et/ou dynamique, plus ou moins approfondie, de la gestion de configuration informatique et réseau, et un contrôle de l'utilisation des ressources par le titulaire de l'accès internet.

- ✓ L'examen de la sécurité de l'environnement informatique est obligatoire quand l'Application est activée ; elle sert à guider le titulaire de l'accès internet et/ou les utilisateurs à améliorer la sécurisation de leur environnement.

Élément 2 : Aide à la sécurisation de l'accès par le calcul de diverses statistiques, comme l'existence ou le comptage de paquets (entrant et sortant) transitant entre réseau public et le réseau local privé de l'abonné, à intervalles de temps réguliers (ex : toutes les heures), suivant les diverses adresses des machines physiques autorisées (et non autorisées).

- ✓ Le calcul statistique est optionnel ; si les statistiques ne sont pas calculées, le titulaire de l'accès internet ne recueille pas les informations brutes sur l'activité transitant à travers sa passerelle au réseau public.

Élément 3 : Aide à la prévention des actes de contrefaçon par l'observation en temps réel, sans enregistrement des flux et protocoles qui transitent par l'accès ; sur la base de l'observation et de la politique de sécurité choisie, une ou plusieurs des actions techniques suivantes peuvent s'appliquer :

- ✓ laisser faire ou réduire[12] le débit (montant et/ou descendant) de la connexion correspondant à l'adresse physique de l'équipement, ou bloquer,
- ✓ selon des critères définis dans le présent document ; ces critères incluent notamment le type de flux ou protocoles, le protocole applicatif, des listes[13],

[11] « moyens de sécurisation » sont notés MS, dans la suite du document.

[12] Le ralentissement est optionnel. Il peut être utilisé dans des contextes spécifiques (notamment, pour les organismes collectifs).

[13] Listes :
Les listes peuvent être :
(note de bas de page - suite)

des caractéristiques de formats, de débits, de volumes, des profils d'utilisateurs, des plages horaires.

- ✓ L'observation est optionnelle ; si cette fonction de l'Application est débrayée sur certaines machines de l'environnement, le titulaire de l'accès internet ne pourra détecter des événements à risque, de transferts sur ces machines.

Élément 4 : Compte-rendu des alertes à l'Administrateur et aux Utilisateurs autorisés dans un but d'information mais aussi de pédagogie et de sensibilisation.

- ✓ Le compte-rendu est optionnel ; si cette fonction de l'Application est désactivée sur certaines ou toutes les machines de l'environnement, le titulaire de l'accès internet ne pourra prévenir les utilisateurs des événements à risque transferts sur ces machines. Ce débrayage peut être souhaitable dans certains organismes collectifs dans le souci de ne pas importuner les utilisateurs pour des raisons de productivité, par exemple.

Élément 5 : Journalisation des événements significatifs.

- ✓ La journalisation est optionnelle ; en cas de non journalisation, le titulaire de l'accès internet perd toute référence pour consulter et comprendre[14] l'activité de l'Application ;
- ✓ Il existe deux versions possibles du journal sécurisé par le titulaire de l'accès internet qui possède les clés cryptographiques : une version en clair intègre, signée électroniquement ou bien une version intègre et confidentielle, signée électroniquement et chiffrée ;
- ✓ Le journal en clair est intègre[15] ; son authenticité est attestée par une clé privée que possède le titulaire de l'accès internet ;
- ✓ Le droit de lire le journal signé et chiffré est restreint au titulaire de l'accès internet qui pourra le déchiffrer grâce à une clé secrète qu'il possède[16] ;
- ✓ Le journal trace les éléments de la vie interne de l'Application des MS : démarrage, arrêt, activation, désactivation, modification des profils de sécurité, etc. ;
- ✓ Le journal trace les éléments des sessions à risques (selon la politique de sécurité) de chaque machine : début et fin de connexion, notification et réponse (éventuelle) de l'utilisateur ;
- ✓ Par opposition, le contenu des fichiers, l'historique des pages visitées ne sont pas enregistrés dans le journal ;
- ✓ Le répertoire organisé chronologiquement par machine des journaux sécurisés doit être archivé et conservé sous la maîtrise du titulaire de l'abonnement. L'Application gère l'effacement au-delà des durées de conservation définies par l'abonné. La date des journaux chiffrés est en clair.

- **blanches**, entités autorisées ;
- **noires**, entités interdites par défaut, entités qui peuvent présenter des risques en matière de contrefaçon et qui nécessiteront (si la politique le permet) une action de l'utilisateur pour outrepasser la notification du risque.

[14] Il peut cependant avoir à sa disposition des messages d'alertes avec des informations synthétiques (voir élément 4).

[15] Ce qui ne veut pas dire qu'il est hors d'atteinte de toute tentative de falsification.

[16] Clé privée et clé secrète sont deux clés distinctes (cryptographie asymétrique pour la première, symétrique pour la seconde).

IV - Les éléments 1, 2, 3, 4 et 5 sont à la **discrétion** et dans les termes choisis par le titulaire de l'accès internet. L'élément 1 est actif et non débrayable quand l'Application est activée. Si les éléments 2, 3, 4 et 5 sont inactifs, l'Application ne joue son rôle que de guide dans la sécurisation du réseau local du titulaire de l'accès internet.

V - L'Application et les MS doivent avoir une certaine capacité de sécurisation contre l'usurpation, le contournement ou l'altération. L'Application et les MS sont eux-mêmes sécurisés : les modules et composants, les liens entre les modules et composants, les liaisons avec d'éventuels serveurs, les processus de mises à jour, le cycle de vie des journaux, etc. L'Application n'est pas une source ou un vecteur d'attaque et n'affaiblit pas l'environnement informatique du titulaire de l'accès internet.

- ✓ Dans une organisation, l'Application est sécurisée par les mesures organisationnelles (sécurité informatique, local technique des instruments de gestion, personnel digne de confiance) ;
- ✓ Dans un domicile ou une TPE, l'Application possède un niveau plus faible d'assurance de sécurité.

VI - L'Application doit inclure une possibilité de mise à jour régulière (actions techniques, notifications, alertes, Application)[17].

VII - L'Application peut se présenter sous diverses formes :

- ✓ Elle peut être un produit ou un service.
- ✓ Elle peut être réalisée à partir de bibliothèques de logiciels libres et/ou peut fonctionner en code exécutable fermé, gérée par une licence sur des systèmes d'exploitation libres.
- ✓ Elle peut être intégrée comme une extension dans des dispositifs ou des logiciels, de gestion ou de sécurité.
- ✓ Elle peut être un système autonome, compatible avec des produits et services du marché.
- ✓ Elle s'insère dans un environnement informatique existant. L'Application dépend de l'environnement matériel et logiciel (types de boitier de connexion, types de logiciels d'exploitation installés sur les postes de travail, etc.) qui compose le réseau local du titulaire de l'accès internet. Le titulaire de l'accès internet doit donc s'assurer de la compatibilité d'une Application fournie par un Éditeur avec son propre environnement.

L'Application ne doit pas transmettre d'informations à des tiers, à l'exception d'un ensemble circonscrit d'éléments secrets cryptographiques (numéro de licence, attributs de mises à jour) à l'Éditeur.

- ✓ L'Application des MS n'enregistre pas d'historique de navigation courante (ex : désignation en clair des sites visités, noms en clair de fichiers téléchargés…).
- ✓ Les journaux enregistrent néanmoins une signature des noms de fichiers et des sites lorsque la politique de sécurité a été outrepassée par un utilisateur.

[17] Les listes (noire et blanche) ne sont pas incluses dans la mise à jour régulière, en règle générale. Elles seront incluses si le Responsable fait appel à une prestation extérieure pour leur gestion.

Dans ce cas, les noms sont masqués par une fonction de hachage afin de respecter la sphère privée de l'utilisateur[18].

VIII - L'Application peut être proposée au titulaire de l'accès internet comme un service opéré par un opérateur de télécom, par un FAI ou par un opérateur de sécurité. Dans ce cas, le titulaire de l'accès internet conserve la maîtrise de la politique de sécurité sur toutes ses machines et la maîtrise des journaux. L'Application peut être installée, en partie, à l'extérieur de l'environnement informatique du titulaire de l'accès internet. Le contrat entre le titulaire de l'accès internet et le prestataire garantit à ce dernier la confidentialité, l'intégrité et la disponibilité des données ainsi que le respect des données personnelles et de la sphère privée de l'activité numérique du réseau local concerné. Le contrat garantit que l'Application n'affaiblit pas la sécurité du réseau local de l'abonné.

[18] Ce hachage est réversible ; la fonction est connue du seul Éditeur, qui est à même de procéder au retour en clair à la demande d'un juge.

SPÉCIFICATION GÉNÉRALE

OBJECTIF

La mise en œuvre d'une Application devra permettre au titulaire d'abonnement à un FAI ou de téléphonie mobile de sécuriser sa navigation personnelle et la navigation sur internet des utilisateurs qu'il a sous sa responsabilité, afin de réduire notablement les risques d'utilisation de son accès internet à des fins de contrefaçon.

CARACTÉRISTIQUES GÉNÉRALES

L'Application doit être :

- efficace et proportionnée par rapport à l'objectif de lutte contre la contrefaçon de biens culturels numériques.
- pédagogique pour faire la promotion de la protection des œuvres sur internet,
- extensible pour être applicable aux particuliers et aux entreprises / grandes organisations : la souplesse doit permettre un vaste choix et la diversité de granularités doit permettre un ajustement de la politique de sécurité à mettre en vigueur dans les différents contextes, à la maison, au travail ou dans les transports,
- apporter du bénéfice pour l'ensemble de l'écosystème : utilisateurs, ayants-droit, FAI et opérateurs de télécoms et Hadopi.

L'installation de l'Application sous forme de produit (matériel et/ou logiciel) ou l'utilisation sous forme de service est facultative, et la décision dépend du titulaire de l'accès internet.

CADRE TECHNIQUE

La spécification repose sur les outils suivants :

- Les réseaux publics avec leurs piles protocolaires standardisées (Ethernet, IP, TCP, UDP, HTTP, etc.) ;
- Primitives cryptographiques (authentification, chiffrement, cryptographie symétrique et asymétrique, signature électronique, certificat) ;
- Système de base de données (pour l'archivage des répertoires des journaux) ;
- Systèmes de protection informatique : protection architecturale, protection matérielle, protection de logiciels, protection des données, protection de l'intégrité du système, fonctions de sécurité (identification, authentification, contrôle d'accès, protection des données).

INTRODUCTION DES MODULES

Par essence, les spécifications techniques détaillées de ce type de produit et/ou de services sont amenées à évoluer au fil du temps, à mesure que les usages sur les conduites à risques changent et se transforment, et chaque fournisseur de solution devra faire évoluer son produit ou son service pour l'adapter aux nouvelles situations, encore inédites, suite à

l'apparition de nouveaux usages et suite à l'existence de ce genre de produit ou service. Néanmoins, le cadre général est plus stable et évoluera plus lentement.

Les SFH peuvent être regroupées en 4 modules qui idéalement comprennent les quatre familles de fonctions principales.

1. Les fonctions d'**administration** : installation, désinstallation, mise à jour, activation, désactivation. Le module administration comprend des fonctions techniques (interface graphique personne-machine).
2. Les fonctions de **traitement** : d'aide à la gestion de configuration de l'environnement informatique et réseau, de comptage statistique de trafic, et d'observation des flux allant sur le réseau ou provenant du réseau (collecte des entités protocolaires, analyse de signatures protocolaires des informations syntaxiques) et les fonctions de décision prises par l'internaute sur les téléchargements. Ce module comprend des fonctions techniques (gestion des listes, analyse protocolaire, moteur de règles de décision) et des fonctions de notification et d'alertes.
3. Les fonctions de **production de journaux** des événements concernant l'Application (mise en marche, arrêt, activation, désactivation), des commandes d'administration des profils (création de profil, modification) et des événements caractérisant les décisions de l'utilisateur concernant les téléchargements. Ce module comprend des fonctions techniques (base de données, présentation d'écran). Il ne contient pas d'historique de navigation.
4. Les fonctions de **sécurité de l'Application** (sécurité du dispositif et de son contexte d'utilisation, sécurisation des journaux, sécurisation de la liaison entre l'Application et les données produites). Ce module comprend aussi les fonctions de paramétrages de la sécurité (définition de profil, définition de la politique de sécurité par profil). Ce module comprend enfin des fonctions techniques (primitives cryptographiques).

L'Application s'appuie, par ailleurs, sur les fonctions de sécurité du système informatique du titulaire.

Ce découpage fonctionnel de présentation de l'Application ne doit pas nécessairement être projeté tel quel pour la conception de la décomposition du logiciel. Par exemple, l'interface personne-machine de l'installation est de l'ordre du rôle administrateur alors que l'interface personne machine général est du rôle de l'utilisateur.

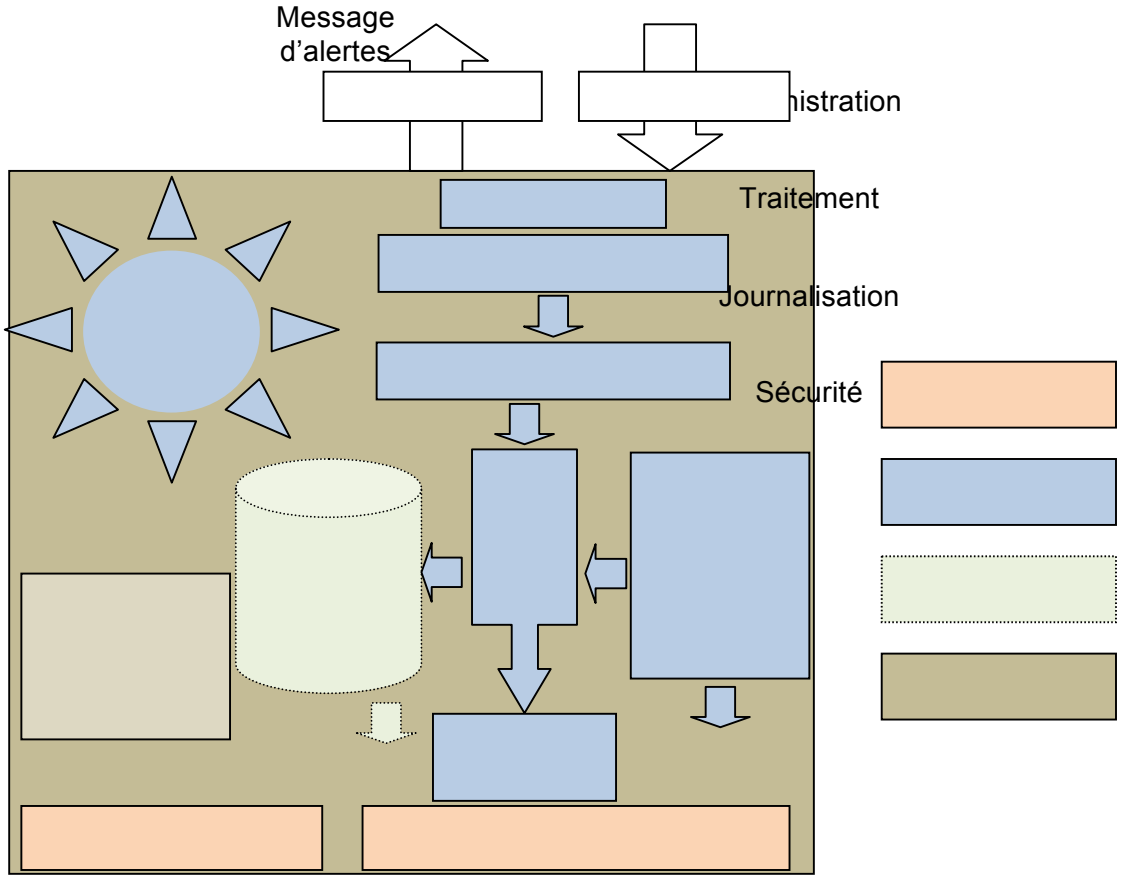

Figure 2 : Schéma fonctionnel de l'Application conforme aux SFH

MODULE 1 : LE MODULE D'ADMINISTRATION

BUT - FONCTIONNEMENT

L'Application comporte un module de gestion du cycle de vie et de gestion de la configuration générale. Le but de ce module est d'administrer le cycle de vie de l'Application (installation, gestion de la licence, mise à jour, maintenance, évolution, désinstallation), de gérer son activité (mise en marche, arrêt, activation, désactivation, gestion des exceptions) et de tracer son cycle de vie et son activité en produisant (optionnellement) des journaux.

ERGONOMIE

L'Application qui est un dispositif (matériel et/ou logiciel) ou un service, est facile à installer (et à désinstaller). Il est facile à activer (et à désactiver) par l'Administrateur.

INTERFACE GRAPHIQUE

L'interface graphique effectue la liaison entre l'Administrateur et l'utilisateur d'une part et l'Application d'autre part. Cette interface doit être aussi discrète que possible lorsque la (ou les) machine(s) a (ont) un comportement normal sur le réseau. Mais lorsqu'une machine a un comportement à risque, l'interface doit le signaler clairement à l'Administrateur (et l'utilisateur). L'Administrateur et/ou l'utilisateur doivent aussi pouvoir apprécier d'un simple coup d'œil le niveau global correspondant au comportement de la (ou des) machine(s).

Lorsque l'analyse de haut niveau aboutit à la détection d'anomalies, c'est-à-dire un comportement à risque de la (ou des) machine(s), l'interface a les caractéristiques suivantes :

- Semi invisibilité en temps normal (mais avec niveau global visible) ;
- Affichage visible des notifications de haut niveau ;

Il existe un mode silencieux de telle façon que l'Administrateur et/ou l'utilisateur ne soient plus importunés par des alertes et/ou notifications. Nonobstant ce mode silencieux, l'Administrateur est toujours responsable des actions susceptibles à risque[19] effectuées par la (ou les) machine(s), y compris dans ce cas.

CYCLE DE VIE DE L'APPLICATION

Installation

Il est nécessaire d'être Administrateur pour installer l'Application, dans le cas d'une installation sur ordinateur.

Si l'Application est un produit ou un service, l'Administrateur devra valider une licence d'utilisation et les termes d'utilisation de l'Éditeur du produit ou du fournisseur de service. L'installation complète ne peut se terminer sans la validation[20] de la licence (logiciel propriétaire ou libre).

[19] Pour éviter tout désagrément à l'Administrateur, on peut envisager par exemple de bloquer les actions problématiques quand l'utilisateur a coché la case de l'interface personne-machine : « ne plus me demander » ou bien quand cette interface est fermée.

[20] On fera un effort dans la procédure d'acceptation pour que la licence soit lue et comprise.

La désinstallation doit être complète sans reste informatique. Toutefois, l'Application ne doit pas être trop facile à désinstaller, afin d'éviter son effacement accidentel ou malveillant. Par conséquent, il est souhaitable de prévoir des mesures de sécurité appropriées pour encadrer cette suppression par l'Administrateur seulement.

Mise à jour

Les mises à jour sont déterminantes. L'Administrateur ne peut pas conserver des versions de l'Application qui possèderaient des erreurs ou failles connues et qui seraient des brèches pour les pirates. Dès que les patches (les rustines) sont disponibles, il doit pouvoir les installer sans tarder.

Afin de garder leurs produits et/ou services opérationnels et efficaces, il est indispensable pour les Éditeurs de recueillir régulièrement, quasiment en temps réel et de façon systématique des informations depuis leurs produits installés.

La transmission de données à l'éditeur est admise dans ce cas précis de contexte d'erreurs à transmettre afin de tenir compte de cet impératif de diligence dans la maintenance curative. Néanmoins pour empêcher la transmission de données personnelles, ce support pour les améliorations ou déclarations de bugs devra être isolé et sous le pilotage de l'Administrateur qui peut le refuser.

L'Application, à la manière du contrôle parental, des systèmes d'exploitation et des logiciels antivirus sera mise à jour en ligne, automatiquement, à partir de sites (FAI, éditeurs de logiciels, éditeurs de sécurité). Ces mises à jour prendront en compte l'émergence de nouveaux protocoles, de nouveaux logiciels de contournements ou de nouvelles pratiques de contrefaçon. Ces mises à jour seront transparentes au titulaire de l'accès internet et aux utilisateurs par une mise à jour en parallèle de la documentation du produit ou du service.

La partie logicielle du dispositif doit pouvoir être mise à jour de manière automatique. Un certain nombre de composants de l'Application doivent régulièrement être mis à jour. Ces composants sont :

- Les définitions des règles de sécurité : Il est nécessaire que les définitions des règles de sécurité suivent les évolutions produites dans le domaine du téléchargement illégal (nouveaux protocoles ou modifications des protocoles existants).

- La définition des notifications et alertes : Les notifications et alertes sont fortement liées aux règles de sécurité. Elles doivent être mises à jour en même temps que celles-ci.

- L'Application : Une mise à jour de l'Application en entier sera nécessaire à chaque nouvelle version de celle-ci.

- Si une version d'une Application labellisée, délivrée par un Éditeur, comporte une erreur qui est découverte par la communauté informatique susceptible d'entraîner un dysfonctionnement voire l'obsolescence de la version de l'Application et/ou qui ouvre une faille de sécurité dans l'Application, cette erreur doit être corrigée avec diligence par l'Éditeur via une mise à jour spécifique.

Les mises à jour doivent être sécurisées (la disponibilité doit être assurée notamment).

CONFORMITÉ DE L'APPLICATION

L'Application doit être conforme aux spécifications et à la documentation.

Elle ne doit pas comporter de fonctionnalités cachées supplémentaires, surtout en termes d'échanges de données (pas de portes dérobées, etc.).

MODULE 2 : LE MODULE DE TRAITEMENT

BUT - FONCTIONNEMENT

Le module de traitement comprend en fait trois sous-modules : un sous-module d'analyse statique de configuration, un sous-module statistique et un sous-module d'analyse dynamique de flux de réseau.

Le premier sous-module est obligatoire. Les 2 autres sous-modules sont à la discrétion et dans les termes choisis par le titulaire de l'accès internet.

Le module de traitement a pour but d'examiner la configuration de l'environnement informatique, par une analyse statique et/ou dynamique, plus ou moins approfondie, de la gestion de configuration informatique et réseau, et de contrôler l'utilisation des ressources par le titulaire de l'accès internet.

Le module de traitement a ensuite pour but de calculer certaines statistiques comme l'existence ou le comptage de paquets (entrant et sortant) transitant entre réseau public et le réseau local privé de l'abonné, à intervalles de temps réguliers (ex : toutes les heures), suivant les diverses identifications (adresses) des machines physiques autorisées (et non autorisées).

Le module de traitement a enfin pour but d'observer en temps réel et sans enregistrement des flux et protocoles qui transitent par l'accès. Sur la base de l'observation et de la politique de sécurité choisie, une ou plusieurs des actions techniques suivantes peuvent s'appliquer :

- laisser faire ou bloquer selon des critères ;
- réduire le débit (montant et/ou descendant) de la connexion correspondant à l'adresse physique de l'équipement. Cette réduction[21] de débit est optionnelle.

Les critères incluent notamment le type de flux ou protocoles, le protocole applicatif, des listes, des caractéristiques de formats[22], de débits, de volumes, des profils d'utilisateurs, des plages horaires[23].

Ces trois sous-modules engendrent des notifications et des alertes, pour l'Administrateur et/ou l'utilisateur. Selon la politique de sécurité, en temps réel ou à intervalles définis, un compte-rendu des alertes est fourni à l'Administrateur pour exploitation et aux utilisateurs autorisés dans un but d'information mais aussi pédagogique de sensibilisation.

[21] La réduction de débit n'a rien à voir avec une sanction. Elle peut être utile dans certains contextes, notamment dans des organismes collectifs avec un grand nombre d'utilisateurs (résidence universitaires, etc.).

[22] Les caractéristiques des formats sont indiquées par les extensions des noms de fichiers, par les métadonnées (comme la taille ou la durée des vidéos). On peut par exemple interdire la vidéo tout en autorisant les vignettes vidéo (de taille faible) ou les bandes annonces de films (de durée limitée).

[23] On peut autoriser ou interdire certaines activités informatiques en fonction des jours ouvrés ou ouvrables et en fonction des heures de la journée.

LES LISTES

Les listes s'appliquent à des entités informatiques : des logiciels, des noms de fichiers[24], des extensions[25] de fichiers (ex : .mpeg, .ogg, .wma, etc.), des sites (URL), des ports de communication, des plages d'adresses, etc.

Le module de traitement utilise des doublets de listes :

- Les listes noires : entités interdites par défaut ou entités qui peuvent présenter des risques en matière de contrefaçon et qui nécessiteront (si la politique de sécurité le permet) une action de l'utilisateur pour outrepasser la notification du risque ;

- Les listes blanches : entités autorisées, par exemple la liste blanche de plages de ports ou d'adresses.

Comme exemple de liste noire, on peut citer :

- les logiciels, la liste des logiciels à risque définis par le titulaire de l'accès internet,

- les fichiers, la liste (ou de leur condensat) de fichiers illicites,

- les protocoles applicatifs, la liste des protocoles à observer,

- les URL, la liste des sites web interdits par décision de justice,

- les ports, la liste des ports TCP ou plages de ports,

- les adresses IP, les plages d'adresses IP interdites qui rentrent en jeu dans certains protocoles ou certains logiciels.

Les éléments du doublet peuvent être un ensemble vide. Il peut, par exemple, ne pas exister de listes noires pour certaines entités informatiques.

Les listes noires et blanches d'une entité sont disjointes. Si les listes ne sont pas disjointes, l'élément est traité de la manière suivante : la liste blanche outrepasse la liste noire. Autrement dit, un élément interdit et autorisé est considéré comme autorisé[26]. Un élément de l'ensemble (des logiciels, des URL, des ports, des adresses, etc.) peut n'appartenir à aucune de ces listes (les listes ne sont pas nécessairement une partition de l'ensemble). Tous les éléments qui peuvent être susceptibles d'être surveillés ne sont pas forcément dans une liste. Les éléments n'appartenant à aucune de ces listes sont traités logiquement et croisés avec d'autres paramètres, conformément aux règles.

L'Administrateur peut modifier ces listes. Ces modifications sont journalisées pour son information.

[24] Les Listes de noms de fichiers ne sont en général pas fiables.
[25] Les extensions de fichiers ne sont en général pas fiables et doivent être traitées avec précaution. Il ne s'agit pas ici d'empêcher tout téléchargement d'image jpeg ou de jeu vidéo qui utilise des fichiers mp3.
[26] Cela peut être le cas, lorsque l'Administrateur génère lui-même ses listes qui doivent écraser des listes standard, par défaut.

LE SOUS-MODULE D'ANALYSE STATIQUE DE CONFIGURATION

Le sous-module statique d'analyse de configuration a pour rôle d'analyser la configuration informatique. Après analyse, l'Application doit conseiller et guider le titulaire dans sa sécurisation.

Le sous-module statique d'analyse des configurations a pour but :

- d'analyser la gestion de configuration informatique (ex : analyse statique de la configuration de postes informatiques ; logiciels installés, base de données, répertoires) ;
  - ✓ Cette analyse est optionnelle (surtout dans le domaine du grand public). Si le titulaire de l'accès internet le décide, cette analyse ne sera pas faite, afin d'éviter toute intrusion dans la sphère privée des utilisateurs.
  - ✓ L'analyse, plus ou moins approfondie, vérifie la bonne configuration du système d'information, des systèmes d'exploitation et des dispositifs de sécurité.
  - ✓ L'analyse peut porter de manière plus fouillée sur l'existence de logiciels ou de comportements à risque.
- de réaliser l'analyse statique de la configuration réseau ;
  - ✓ L'analyse porte sur la vérification de la sécurité du (ou des) point(s) d'accès : pare-feu filtrant dans les organismes collectifs, boîtier/routeur dans l'environnement grand public ou TPE ;
  - ✓ L'analyse porte sur la sécurité du réseau local intranet ;
  - ✓ La vérification porte sur les protocoles de liaisons utilisés (comme WPA2 pour la sécurisation de la connexion Wi-Fi au boîtier) et de vérifier les adresses physiques autorisées (contrôle des adresses MAC).
- d'analyser dynamiquement des logiciels en fonctionnement ;
- de contrôler les utilisations par le titulaire de la connexion.

LE SOUS-MODULE STATISTIQUE

Le sous-module statistique a pour rôle de réaliser un audit constant de comptage statistique de trames montantes et descendantes, transitant à travers le point d'accès, frontière entre internet et le réseau local.

Dans les points d'accès récents[27], il existe dans les routeurs et dans les boîtiers de connexion, des compteurs de trames montantes et descendantes. Il est donc possible (quand on peut y accéder) de fournir au titulaire de l'abonnement, s'il le souhaite, ces statistiques montantes et descendantes, ces statistiques étant décomposées par adresse physique d'équipement.

Avec la connaissance de cette information, l'Application peut donc vérifier si des équipements pirates se sont connectés sur le point d'accès, de manière illicite, peut alerter l'Administrateur si des flux anormaux ont transités sur le point d'accès.

[27] Les routeurs élémentaires ou anciens n'offrent pas cette possibilité.

Ce sous-module, s'il est en activité, peut détecter les machines (autorisées ou non) qui se sont connectées avec les transferts dans les deux sens toutes les tranches de 30 minutes ou toutes les heures. Le titulaire de l'accès internet peut exploiter ces statistiques pour améliorer la sécurité de sa ligne (point d'accès et connexions) et sensibiliser son entourage.

LE SOUS-MODULE D'ANALYSE DYNAMIQUE DE FLUX

Le module d'analyse dynamique de flux est le module de capture, d'observation, de détection, d'analyse du trafic et de décision par la politique de sécurité existante ou par l'utilisateur de la suite à donner à son action, suite à une notification de l'Application.

Le but de ce module est d'inspecter dynamiquement le contenu entrant et sortant du trafic sur les interfaces du réseau de la (des) machine(s) de l' (des) utilisateur(s).

Ce module réalise en temps réel une analyse contextuelle et syntaxique des flux du contenu ; il n'analyse pas le contenu sémantique des fichiers[28] dans la mesure où ne sont pas analysés à ce jour les attributs de mesures techniques de protection (MTP ou *DRM*) ou les empreintes des contenus des fichiers.

- Il observe en temps réel et sans enregistrement les flux et protocoles qui transitent par l'accès.

- Il bloque, ralentit[29], autorise ou prévient l'utilisateur selon des critères qui incluent le type de flux ou protocoles, le protocole applicatif, les listes, les caractéristiques de formats, les débits, les volumes, les profils d'utilisateurs, les plages horaires.

Ce module a pour but d'identifier de manière précise les protocoles applicatifs, par le biais d'analyseurs des interactions entrante et sortante sur les interfaces du réseau par une analyse détaillée des signatures, des formats et de la syntaxe des protocoles de la couche applicative.

Ce module gère dynamiquement les protocoles applicatifs et les couches sous-jacentes du trafic de communication. L'analyse protocolaire reconnaît les signatures applicatives quelque soit le port utilisé pour garantir une identification exhaustive, y compris pour les protocoles dynamiques.

Les actions possibles s'étendent sur toute la palette des protocoles (pair-à-pair, streaming, téléchargement direct, messagerie instantanée…, *cloud computing*) de l'internet. Le module détecte et contrôle les protocoles répertoriés par l'Éditeur de l'Application.

Il existe en 2011, environ 150 piles protocolaires utilisées sur internet : par exemple HTTP/TCP/IP est un exemple de pile protocolaire applicative pour consulter le Web, ed2k/TCP/IP[30] est un exemple de pile protocolaire applicative pour télécharger des fichiers avec une méthode de poste-à-poste.

Chaque protocole analysé dispose de son propre composant. Un composant se comporte comme un objet de configuration qui peut être associé à un service et dont l'Administrateur peut définir les paramètres.

[28] Cf. infra le paragraphe intitulé « Cas particulier du filtrage des contenus dans certains organismes ».
[29] Le ralentissement de certains flux est optionnel. Il peut être utilisé à des fins de gestion de réseaux privés ou de manière préventive.
[30] Pile protocolaire qu'utilisent les clients P2P eMule, eDonkey.

Le paramétrage permet d'appliquer une politique de sécurité en restreignant l'usage du protocole.

Dans une organisation ou chez le particulier, ces actions, portant sur des accès et des contenus permettent de réguler l'utilisation d'internet des utilisateurs autorisés conformément aux règles établies par le responsable de l'établissement ou le titulaire de l'abonnement.

L'analyse dynamique du réseau a pour rôle d'analyser les connexions réseau de l'ordinateur, de détecter toutes connexions et le cas échéant de générer une notification de bas niveau.

L'Application prévoit par défaut une liste non exhaustive des connexions à surveiller.

Il y a deux types de détection et d'analyse des flux suspects[31] :

- Analyse en temps réel : Certains protocoles sont identifiables par la signature de leurs paquets, une détection en temps réel est alors possible. La notification de bas niveau est générée dès les premiers échanges de paquets sur la connexion suspecte.

- Analyse différée : Certains protocoles (notamment les protocoles chiffrés) ne peuvent être détectés qu'à la suite d'une analyse statistique. La notification de bas niveau est, dans ce cas, générée en différé. La période séparant la création de la connexion suspecte et la génération de l'alerte doit être aussi courte que possible (quelques secondes).

La détection des connexions suspectes est basée sur un ensemble de règles de sécurité. Ces règles sont régulièrement mises à jour de façon à prendre en compte de nouveaux protocoles ou de nouveaux comportements délictueux sur le réseau.

LE MOTEUR D'ANALYSE PROTOCOLAIRE

Une Application possède un moteur de règles qui permet d'enchaîner en séquence les conditions qui sont imposées par la politique de sécurité. Le moteur dispose de fonctionnalités multiples de détection et d'identification de piles protocolaires (éventuellement simultanées), de comptage en volume des flux (nombre d'octets d'un fichier, nombre d'octets entrant et sortant, débit en octets par seconde en entrée et en sortie, etc.), de comptage en durée des flux (nombre de secondes ou de minutes de durée de vie d'un protocole, etc.) qui lui permettent de filtrer les fichiers échangés, à bon escient, selon la granularité souhaitée.

Le moteur de règles couplé à l'utilisation de profils autorise une flexibilité dans le paramétrage des politiques de sécurité : gestion selon des quotas en volume, en durée, selon des plages horaires, etc.

Découpage en deux niveaux

Une Application comprend essentiellement un moteur intelligent d'analyse et de détection de piles protocolaires et de contrôle de flux entrant et sortant, en analysant les caractéristiques et les attributs des protocoles aux niveaux des couches OSI (application, présentation, session, transport, réseau, liaison de données), dans un poste terminal (ordinateur ouvert) ou bien dans un réseau en distinguant les diverses machines terminales (ordinateur, téléphone mobile, console de jeu, etc.). L'Application n'examine pas le contenu applicatif des échanges.

[31] Il est nécessaire de répéter que la technologie est neutre.

L'analyse s'effectue de manière passive, c'est-à-dire qu'elle ne modifie pas les contenus et les attributs du réseau que l'Application traite.

Il est toutefois possible, selon la politique de sécurité mise en vigueur par le titulaire de l'abonnement d'adopter une attitude plus active et de mettre fin, par précaution, à certaines connexions pour lesquelles des logiciels, des adresses, des sources, des destinations seraient suspects.

L'Application peut ainsi opérer en deux temps[32] :

Le moteur de bas niveau

Dans un premier temps, un moteur de bas niveau capte à la volée le trafic réseau et décode syntaxiquement les différentes couches protocolaires de manière à en extraire des caractéristiques (motifs distinctifs, signature protocolaire). Cette étape fournit des éléments et des événements qui sont ensuite analysés, en temps réel, selon les règles de la politique de sécurité. Par exemple, l'analyse se fera par la comparaison des URL à des URL définis dans une liste.

Le moteur de haut niveau

Dans un second temps, un moteur de haut niveau, analyse en léger différé (comme un serveur mandataire – un « proxy »), les éléments et les événements générés par le premier moteur, et agit selon des règles de haut niveau d'abstraction de la politique de sécurité, prenant en compte le contexte. Ces règles sont des canevas d'analyse qui prennent en compte le contexte statique (la configuration présente de l'ordinateur) et le contexte dynamique (les flux entrant et sortant).

Ces règles seront, à plus long terme, après le déploiement des solutions, mises à jour au fil du temps.

Langage de règles

Une règle de sécurité se compose de (Conditions => Actions).

Ces règles doivent être écrites dans une norme commune à tous les fournisseurs des Applications. La politique de sécurité peut être écrite en utilisant le langage SAML. Le langage de règles peut être par exemple XrML.

La nature des règles

L'Application prévient l'Administrateur et/ou l'utilisateur que les modes et les outils de communication utilisés (les URL, les piles protocolaires, les ports, les adresses, etc.) sont potentiellement à risque.

Si les protocoles de partage poste-à-poste et les espaces de stockage en ligne "Coffres forts électroniques" sont utilisés pour le transfert illicite de contenus soumis au copyright, ils sont aussi utilisés pour le transfert de contenus tout à fait légaux, par exemple des mises à jours de logiciels libre de droits et pour la circulation autorisée de contenus soumis à copyright dans un cadre commercial. En conséquence même si la complexité importante liée à la limitation de l'accès à certains protocoles particuliers P2P peut être résolue jusqu'à un

[32] Le découpage en deux parties n'est pas une exigence fonctionnelle, mais un choix pour la présentation de la spécification. Dans une réalisation locale sur un ordinateur, on intriquera sans doute ces deux moteurs.

certain point, le résultat d'un blocage pourrait interdire l'accès à des services de livraison des contenus légaux.

Fournir aux Administrateurs et/ou aux utilisateurs une manière de reconnaître, agir, en évitant ou interrompant un téléchargement illégal, doit être une fonctionnalité essentielle de toute initiative de sécurisation d'un accès contre son mauvais usage.

Pour les règles, il existe donc des indices de situation courante, de conduite ordinaire, et des indices de situation remarquable, spécifiques de conduites à risque ou anormales. Cette distinction normale-anormale ne sépare donc pas l'acquisition ou la présentation d'un fichier légal (téléchargement en P2P d'une version de Linux, *streaming* sur France culture, etc.) de l'acquisition ou la présentation d'un fichier illégal. Cette analyse distingue des conduites protocolaires spécifiques, définies sur des bases de critères quantitatifs, qui varient au cours de la session.

Les règles et les critères devront évoluer avec les usages dans le temps, en fonction des pratiques sur internet, et être mis à jour. Il sera nécessaire de mesurer l'impact des règles utilisées dans les mois passés afin d'affiner les règles à venir. L'analyse anonyme statistique, sur les réseaux des opérateurs de télécoms, des éléments et des événements permet en effet :

- De distinguer les piles protocolaires et les attributs spécifiques (apparition de nouveaux protocoles pour télécharger, téléchargement de type P2P, téléchargement en ligne de type *streaming*, messagerie avec un attachement très volumineux, etc.) et

- De décider d'un ensemble de règles (décrites en termes d'événements et de signatures) pour réduire les conduites à risque, les dérives ou les anomalies : VPN chiffré vers des sites à risque , présence de connexions de l'utilisateur vers certains services, tentatives de connexions infructueuses, etc.

Les notifications et les alertes

Il y a deux catégories de notifications, les notifications de bas niveau et les notifications de haut niveau.

- Les notifications de bas niveau sont générées en cas de détection d'une anomalie dans le comportement de la machine (ou dans ses configurations ordinateur et boîtier/routeur). À chaque anomalie doit correspondre une notification précise. Ces notifications sont destinées à l'analyseur haut niveau de l'Application.

- Les notifications de haut niveau sont générées par l'analyseur haut niveau de l'Application.

Chaque notification dans son contexte doit être inscrite dans le journal si celui-ci est activé.

L'analyse de haut niveau consiste à analyser les différentes notifications de bas niveau émises par la partie analyse de configurations et la partie analyse dynamique du réseau, et, en fonction de ces notifications de bas niveau et des règles de sécurité régulièrement mises à jour, de générer une notification de haut niveau.

Les notifications sont destinées à l'Administrateur et/ou à l'utilisateur. Les alertes sont des notifications de haut niveau destinées à l'Administrateur.

En cas d'impossibilité d'inscription dans le journal (absence de journal, par exemple), en substitution, les alertes peuvent être envoyées à l'Administrateur par un moyen approprié (webmail, sms, etc.).

Flexibilité et mise à jour des règles du moteur de haut niveau

L'Application utilise pour décrire ces règles un langage particulier : on prendra un langage standard (par exemple XrML) qui permet d'être flexible pour la mise à jour afin de s'adapter rapidement au contexte à surveiller.

Le moteur de haut niveau devra être relativement standard entre les diverses solutions proposées par les différents acteurs de telle manière qu'un groupe de veille technique sur les pratiques sur le réseau puisse permettre d'échanger rapidement et de diffuser les règles nouvelles à adopter.

MODULE 3 : LE MODULE DE JOURNALISATION

BUT - FONCTIONNEMENT

Une Application engendre optionnellement un journal détaillé, qui sauvegarde les différents événements observés. Les traces doivent enregistrer les événements comme les démarrages, les mises à jour, les actions de l'utilisateur, les arrêts, etc.

Le but de ce module est de produire un journal d'événements qui retrace l'historique de l'activité des différents utilisateurs de la ligne internet.

La journalisation consiste en la sauvegarde, de toute l'activité réseau notable, des notifications et/ou alertes générées et des choix de réponse aux notifications de l'utilisateur et/ou de l'Administrateur dans un journal.

- Le journal trace les éléments de la vie interne de l'Application des MS : démarrage, arrêt, activation, désactivation, modification des profils de sécurité, etc.

- Le journal trace les éléments des sessions à risque (selon la politique de sécurité) de chaque machine : début et fin de connexion, notification et réponse de l'utilisateur.

- Par opposition, le contenu des fichiers, l'historique des pages visitées ne sont pas enregistrées dans le journal.

Cette journalisation est optionnelle pour chaque utilisateur. Il peut donc n'y avoir aucune journalisation pour le réseau local, ce qui n'empêche pas l'Administrateur de recevoir optionnellement des messages d'alerte avec des informations synthétiques sur les anomalies observées, comme indiqué dans le module de traitement.

Si la journalisation est active, il existe une alternative de format de journalisation des événements significatifs : le journal est en clair ou bien le journal est chiffré.

- Si le journal est en clair, il est intègre, signé électroniquement en utilisant la cryptographie asymétrique, la signature étant chiffrée par une clé privée (un mot de passe) que possède l'Administrateur.

- Le journal est chiffré, il est intègre et confidentiel ; le journal est intègre (idem au point précédent) et confidentiel, c'est-à-dire qu'il est chiffré en utilisant la cryptographie symétrique par une clé secrète (un autre mot de passe) que possède l'Administrateur. Le droit de lire ce journal sécurisé est restreint au titulaire de l'accès internet qui pourra le déchiffrer en utilisant la clé secrète qu'il détient. L'Application permet le déchiffrement de ce journal, lorsqu'on est Administrateur et qu'on possède cette clé secrète.

Le journal en clair sera rédigé en langue française, avec des explications comme « Vendredi 3 septembre 2010, 19h23 mn – Alerte significative - Un nouvel ordinateur inconnu se connecte au boîtier <adresse> : veuillez vérifier les adresses physiques des équipements informatiques qui sont autorisés à se connecter ». Un appel à une aide éventuelle fournit les mesures possibles à mettre en œuvre pour remédier à la notification.

Ce journal (on parle de *logs* ou de traces, en informatique) pour chaque ordinateur est engendré selon un format standard (heure locale, on utilise les standards de logs), éventuellement en utilisant le système de gestion du système d'exploitation. Les logs

utilisent de préférence le standard « syslog » ou IDMEF[33], qui est une RFC expérimentale de l'IETF. Les événements seront enregistrés par exemple selon le format suivant :

> Date et Heure : (degré d'importance - optionnel), type d'événement (description de l'événement, optionnelle).

Ci-dessous se trouvent des exemples d'événements tels qu'ils seront enregistrés dans le journal :

> Jeudi 20 mai 2010 18 :12 :59 : Notification connexion Protocole ABC lancée
> Jeudi 20 mai 2010 20 :32 :10 : Notification site interdit lancée

- Le premier exemple indique qu'une notification de haut niveau concernant la connexion à un protocole sur liste noire a été générée et signalée à l'utilisateur le jeudi 20 mai 2010 à 18h12.

- Le second exemple indique qu'une notification de haut niveau concernant une connexion à un site interdit a été générée et signalée à l'utilisateur le jeudi 20 mai 2010 à 20h32. Un exemple de journal plus détaillé se trouve dans la Figure 3 : Exemple de journal.

Les événements inscrits à mettre dans le journal sont les suivants :

- Mise en route/Arrêt de l'Application : Lorsque l'Administrateur décide d'arrêter l'Application, la date et l'heure de l'arrêt sont inscrites dans le journal. Il en va de même pour la mise en marche de l'Application (voir Figure 3 : Exemple de journal, <1>) ;

- Mise en route/Fermeture de la connexion réseau : La connexion réseau peut démarrer en différé par rapport à la mise en marche de l'Application. Une interface réseau peut aussi être ajoutée dynamiquement, ces événements seront inscrits dans le journal (voir Figure 3 : Exemple de journal, <2>) ;

- Mise/Sortie de pause de l'Application : L'Administrateur peut temporairement désactiver l'Application, et la réactiver ensuite. Ces événements sont inscrits dans le journal (voir Figure 3 : Exemple de journal, <3>) ;

- Changement de profils : Le profil utilisateur courant est modifié en fonction de l'utilisateur qui utilise la connexion internet. Ces modifications sont enregistrées dans le journal (voir Figure 3 : Exemple de journal, <4>) ;

- Notifications générées (bas et haut niveau) : Les notifications générées par les modules d'analyse ou la gestion des profils sont enregistrés dans le journal (voir Figure 3 : Exemple de journal, <5>) ;

- Réponses aux notifications ou alertes par l'utilisateur : à la suite d'une notification, l'utilisateur doit prendre une décision, suivre les conseils proposés avec la notification ou les ignorer. Ce choix et les actions qui découlent de ce choix (blocage ou non d'une connexion, etc.) sont enregistrés dans le journal, (voir Figure 3 : Exemple de journal, <6>).

[33] IDMEF : Intrusion Detection Message Exchange Format, RFC 4765 de l'IETF.

OPTIONS DE JOURNALISATION

Pour chaque utilisateur (ou profil d'utilisateurs), il existe un menu à la carte qui offre trois options :

1. Pas de journalisation ;

2. Un journal en clair que chaque utilisateur pourra consulter ainsi que l'Administrateur. Ce journal est signé électroniquement par une clé privée que détient l'Administrateur ; l'utilisateur pourra aussi vérifier l'intégrité de son journal (il a connaissance de la clé publique).

3. Un journal chiffré que seul l'Administrateur pourra déchiffrer puisqu'il détient seul la clé secrète. Ce journal est intègre et confidentiel. Cette version du journal est en mode binaire, compressée, signée électroniquement, chiffrée et archivée. Ce journal sera donc accessible en clair au titulaire de l'abonnement. Il permettra de vérifier, après déchiffrement avec la clé correspondant à l'Application, la mise en œuvre du l'Application à une date et heure donnée, et l'activité informatique de l'internaute concerné. Ce journal permet de refléter, sans interférence possible de l'utilisateur, les événements de l'accès internet considéré.

Il est conseillé de ne pas écrire en temps réel les informations dans les journaux .log, mais avec un léger temps différé pour contrecarrer les quelques menaces provoquées par la synchronisation d'événements.

CONSERVATION DU JOURNAL

L'organisation des journaux et la date en clair des journaux chiffrés permettent à l'Administrateur de gérer les journaux et d'adapter la durée de conservation des différents journaux aux différentes exigences légales.

Il est conseillé à l'Administrateur d'effacer après exploitation et dès que possible le journal en clair.

Exemple de Journal engendré	Signification des étapes
Jeudi mai 20 12 :30 :48 2010 : Mise en marche de l'Application<1>	
Jeudi mai 20 12 :30 :49 2010 : Lance l'Écoute de l'interface : \Device\NPF_{A0160E28-0054-4824-BB02-3658DA127EAB} 0 :c :29 :f8 :21 <2>	
Jeudi mai 20 12 :30 :50 2010 : Rapport (Signale programme sur liste noire: Programme ABC) <5> Jeudi mai 20 12 :30 :50 2010 : Notification programme sur liste noire Programme ABC lancée <5> Jeudi mai 20 12 :30 :50 2010 : Rapport (Signale programme sur liste noire : Programme DEF) <5> Jeudi mai 20 12 :30 :50 2010 : Notification programme sur liste noire Programme DEF lancée <5> Jeudi mai 20 12 : 30 :52 2010 : Continue malgré Notification : programme sur liste noire : Programme DEF <6> Jeudi mai 20 12 :30 :53 2010 : Continue malgré Notification : programme sur liste noire : Programme ABC <6>	Détection des programmes sur Liste noire
Jeudi mai 20 12 :42 :50 2010 : Changement de profil : Admin + 19h00-22h00 <4> Jeudi mai 20 12 :44 :09 2010 : Rapport (Signale hors de la plage horaire : 19h00-22h00) <5> Jeudi mai 20 12 :44 :09 2010 : Notification heure hors plage horaire lancée <5> Jeudi mai 20 12 :44 :57 2010 : Arrête après Notification : heure : hors plage horaire <6> Jeudi mai 20 12 :44 :58 2010 : Bloque les connexions <6> Jeudi mai 20 12 :49 :02 2010 : Changement de profil : Admin + 12h00-17h00 <4> Jeudi mai 20 12 :49 :03 2010 : Débloque les connexions <6>	Plage horaire non respectée
Jeudi mai 20 13 :29 :28 2010 : Rapport (Signale site sur liste noire) <5> Jeudi mai 20 13 :29 :28 2010 : Notification site sur liste noire lancée <5> Jeudi mai 20 13 :29 :28 2010 : Rapport (Signale site sur liste noire) <5> Jeudi mai 20 13 :29 :29 2010 : Rapport (Signale site sur liste noire) <5> Jeudi mai 20 13 :29 30 2010 : Rapport (Signale site sur liste noire) <5>	Sites sur Liste noire
Jeudi mai 20 14 :12 56 2010 : Rapport (Signale connexion ed2k) <5> Jeudi mai 20 14 :12 59 2010 : Notification connexion ed2k lancée <5> Jeudi mai 20 14 :13 03 2010 : Arrête après Notification : connexion ed2k <6> Jeudi mai 20 14 :13 03 2010 : Connexion bloquée : ed2k <6> Jeudi mai 20 14 :32 :27 2010 : Rapport (Signale connexion ed2k) <5> Jeudi mai 20 14 :32 :28 2010 : Notification connexion ed2k lancée <5> Jeudi mai 20 14 :13 :03 2010 : Continue après Notification : connexion ed2k <6> Jeudi mai 20 14 :22 :27 2010 : Rapport (Signale connexion ed2k) <5> Jeudi mai 20 14 :22 :57 2010 : Rapport (Signale connexion ed2k<5> Jeudi mai 20 14 :23 :27 2010 : Rapport (Signale connexion ed2k) <5> Jeudi mai 20 14 :23 :57 2010 : Rapport (Signale connexion ed2k) <5> Jeudi mai 20 14 :24 :27 2010 : Rapport (Signale connexion ed2k) <5> Jeudi mai 20 14 :24 :57 2010 : Rapport (Signale connexion ed2k) <5> Jeudi mai 20 14 :25 :27 2010 : Rapport (Signale connexion ed2k) <5>	Connexion P2P
Jeudi mai 20 14 :25 :32 2010 : Désactivation de l'Application<3> Jeudi mai 20 18 :41 :28 2010 : Réactivation de l'Application<3>	Pause
Jeudi mai 20 18 :41 :28 2010 : Rapport (Signale hors de la plage horaire : 12h00-17h00) <5> Jeudi mai 20 18 :41 :29 2010 : Notification heure hors plage horaire lancée <5> Jeudi mai 20 18 :41 :29 2010 : Continue après Notification : heure : hors plage horaire <6> Jeudi mai 20 18 :41 :19 2010 : Rapport (Signale hors de la plage horaire : 12h00-17h00) <5> Jeudi mai 20 18 :41 :49 2010 : Rapport (Signale hors de la plage horaire : 12h00-17h00) <5> Jeudi mai 20 18 :42 :19 2010 : Rapport (Signale hors de la plage horaire : 12h00-17h00) <5> Jeudi mai 20 18 :42 :49 2010 : Rapport (Signale hors de la plage horaire : 12h00-17h00) <5> Jeudi mai 20 18 :43 :19 2010 : Rapport (Signale hors de la plage horaire : 12h00-17h00) <5> Jeudi mai 20 18 :43 :49 2010 : Rapport (Signale hors de la plage horaire : 12h00-17h00) <5> Jeudi mai 20 18 :44 :12 2010 : Changement de profil : Admin + 12h00-22h00 <4>	Plage horaire, après Pause
Jeudi mai 20 18 :46 :36 2010 : Rapport (Signale streaming vidéo) <5> Jeudi mai 20 18 :46 :37 2010 : Notification streaming vidéo lancée <5> Jeudi mai 20 18 :46 :40 2010 : Continue après Notification : streaming vidéo <6> Jeudi mai 20 18 :47 :40 2010 : Rapport (Signale streaming vidéo) <5> Jeudi mai 20 18 :48 :40 2010 : Rapport (Signale streaming vidéo) <5> Jeudi mai 20 18 :49 :40 2010 : Rapport (Signale streaming vidéo) <5> Jeudi mai 20 18 :50 :40 2010 : Rapport (Signale streaming vidéo) <5> Jeudi mai 20 18 :51 :40 2010 : Rapport (Signale streaming vidéo) <5> Jeudi mai 20 18 :52 :40 2010 : Rapport (Signale streaming vidéo) <5> Jeudi mai 20 18 :53 :40 2010 : Rapport (Signale streaming vidéo) <5>	Streaming
Jeudi mai 20 18 :54 :48 2010 : Mise en veille de l'Application <1>	

Figure 3 : Exemple de Journal

MODULE 4 : LE MODULE DE SÉCURITÉ

BUT - FONCTIONNEMENT

Le but du module de sécurité est double. Il permet de protéger l'Application, les entrées et les sorties issues de l'Application, et il permet de construire et mettre en œuvre des politiques de sécurité par utilisateur ou par groupe d'utilisateurs.

Il a premièrement pour finalité d'aider à sécuriser la ligne qui relie le poste de l'internaute à internet (ou l'usager mobile au réseau de l'opérateur mobile) et de protéger l'Application et les résultats de cette Application. L'Application doit être disponible (éviter les menaces de déni de service) et intègre (éviter les menaces d'altération ou de falsification de l'Application).

Il a deuxièmement pour but de définir les deux rôles d'Administrateur (l'Administrateur est le titulaire de l'accès ou son représentant) et d'utilisateur de l'Application (ex : les employés d'une entreprise, les membres du foyer d'un domicile).

Le contrôle de la ligne permet au titulaire de l'abonnement internet ou de téléphonie mobile, grâce à un dispositif dédié (matériel et/ou logiciel), de surveiller, de restreindre l'accès aux utilisateurs sous sa responsabilité, à internet ou aux services réseaux, en le limitant à certaines catégories d'accès et en bloquant l'accès à certains sites ou services applicatifs de l'internet ou de la téléphonie mobile.

Ce module permet de paramétrer l'accès par des plages horaires (surveillance pendant les plages horaires, blocages en dehors de plages horaires), par des durées de type connexion[34] (limites de 15 minutes de streaming), par limitation dans le débit ou le volume de flux (entrant ou sortant) des ordinateurs ou de la ligne.

OBJECTIFS DE SÉCURITÉ

L'Application doit viser les objectifs de sécurité suivants :

Auditabilité

« Ces événements se sont passés ici et dans ce contexte-là ».

L'objectif visé est d'assurer l'intégrité du contexte du poste terminal et du contexte de la ligne réseau qui relie le poste terminal (l'ordinateur, téléphone 3G) à internet ou au réseau mobile.

Il faut être capable de reconstituer la situation telle qu'elle était, au moment du téléchargement illégal : est-on sûr qu'il y avait téléchargement à ce moment-là et à cet endroit-ci ? Est-ce qu'un pirate téléchargeait ou est-ce qu'un faux pirate (un utilisateur qui veut se faire passer pour un pirate) était connecté en même temps ?

Il faut, pour atteindre cet objectif, utiliser des fonctions d'identification et d'authentification pour identifier les sujets (login de l'utilisateur, logiciel en exécution, etc.) et les objets en situation (matériels, logiciels, données). Il faut mettre en œuvre plusieurs fonctions de

[34] Le but de ces courtes durées est par exemple de rendre possible la visualisation des bandes annonces de films nouveaux.

sécurité, notamment l'identification[35] de l'Application qui fonctionne dans son environnement identifié.

Ces fonctions d'identification et d'authentification seront elles-mêmes sécurisées.

Un tableau de bord de la configuration du réseau avec les connexions, les adresses physiques et logiques des équipements, avec les caractéristiques des liaisons sécurisées doit, sur demande, conseiller et guider le titulaire pour assurer le confort de sa sécurité.

Intégrité et disponibilité de l'Application

« L'Application fonctionne correctement, elle n'est pas contournée, ni détournée, ni empêchée ».

On peut atteindre cet objectif notamment en identifiant chaque Application.

Une clé permet de vérifier la signature électronique du contenu exécutable du logiciel.

Une clé est utilisée pour chiffrer les journaux.

Une autre clé est utilisée pour signer les journaux.

Les listes sont sécurisées, en particulier, en termes d'intégrité et d'authenticité.

Le module dispose de fonctions avancées journalisant, notifiant et alertant les contournements de l'Application, opérés par des serveurs mandataires (« proxys ») anonymes ou autres accès médiateurs sophistiqués.

L'Application ne doit pas affaiblir le niveau de sécurité des systèmes d'exploitation, lorsqu'une partie de l'Application est construite dans le noyau des systèmes d'exploitation.

Les mises à jour de l'Application sont sécurisées[36], en particulier la mise à jour des règles.

La sécurité des biens sensibles de l'Application repose aussi sur les meilleures pratiques en termes de sécurisation du système d'exploitation sous-jacent à l'Application et sur l'absence de vulnérabilités dans l'Application et dans le système d'exploitation sous-jacent.

Protection du journal

L'objectif visé est l'authenticité, l'intégrité et la disponibilité du journal des événements. Si l'on ajoute l'objectif de confidentialité du journal, il est alors chiffré.

L'horodatage est envisageable pour des cas relativement rares. Il n'est pas forcément souhaitable, et donc pas du tout obligatoire.

« Ces journaux sont (optionnellement) confidentiels37, authentiques, intègres, disponibles38 ont été engendrés par l'Application identifiée dans ce contexte-ci, et les événements se sont passés à cette date-là ».

[35] Il ne faut pas prendre trop de paramètres pour identifier le lieu, sinon les modifications de l'identification seront trop fréquentes.
[36] On vérifie la provenance de la mise à jour, l'intégrité de la mise à jour.
[37] Pour les personnes autres que le titulaire.

On utilise un ensemble de primitives cryptographiques afin de garantir la confidentialité (optionnel), l'authenticité, l'intégrité, la justesse du journal, la non répudiation du journal de l'Application et leur disponibilité lorsqu'un titulaire les demande, et de garantir la conformité et la disponibilité de l'Application qui aura engendré ce journal.

Les journaux sont intègres, signés électroniquement, enregistrent la chronologie des événements avec des dates et heures, éventuellement dignes de confiance (horodatage optionnel sécurisé des événements) et enregistrent le lieu et le contexte des événements (lieu informatique de l'événement, identification et authentification du contexte informatique - la machine, le logiciel et le journal engendré associé).

La datation éventuelle des traces s'opère à partir d'une date et heure récupérée sur un serveur NTP (*Network Time Protocol*). Ce serveur NTP est alors sécurisé en redondance avec une bascule, afin d'assurer une continuité de service, suite à un dysfonctionnement. La connexion au serveur est sécurisée, par exemple, par SSL.

Il existe une procédure automatique à disposition du titulaire afin de récupérer des journaux en clair et de vérifier leur intégrité ou bien de récupérer des journaux chiffrés et de les déchiffrer à partir des codes secrets correspondant à l'Application, afin de pouvoir les lire et les exploiter.

RISQUES

L'Application des MS doit être protégée notamment contre les risques suivants :

- L'Application ne fonctionne pas correctement (erreur dans la spécification, dans la conception, dans l'implantation, problème dans l'exploitation) et le journal n'est pas écrit et archivé de manière régulière.

- Une personne exploite une défaillance de l'Application.

- L'Application est contournée ou détournée ou empêchée dans son fonctionnement normal par un utilisateur.

- Une personne détruit des journaux ou fabrique des leurres de journaux, à l'insu du titulaire de l'accès internet pour le tromper ou le gêner.

- Une personne provoque un déni de service sur les serveurs de mise à jour et/ou les serveurs de temps.

- L'Application ne prend pas en compte la prévention de tous les risques relatifs à la vie privée de l'utilisateur : par exemple, l'accès non autorisé au journal en clair.

Les MS techniques doivent être protégées notamment contre les risques suivants :

- Une personne exploite des failles dans la mise en vigueur de la politique de sécurité, usurpe l'identité de l'utilisateur autorisé et télécharge à son insu.

- Une personne exploite un défaut de sécurité dans l'environnement. L'environnement informatique n'est pas sécurisé : par exemple le lien de réseau sans fil entre les ordinateurs du domicile et le boîtier ADSL est vulnérable à une intrusion ou bien un pirate s'est glissé dans la communication autorisée du titulaire,

[38] Uniquement pour le Responsable (le titulaire de l'abonnement), s'il est chiffré, ou les utilisateurs s'il est en clair.

en brisant la sécurité WEP du Wi-Fi quand l'abonné utilise une sécurité WEP sans pouvoir migrer vers une sécurité WPA.

- Un utilisateur utilise normalement l'Application sur un premier poste en téléchargeant légalement des fichiers, et télécharge simultanément et illégalement des fichiers sur un second poste sans l'Application, simulant ainsi la présence d'une machine pirate.

- Les MS ne prennent pas en compte la prévention de tous les risques relatifs à la vie privée de l'utilisateur : par exemple, l'accès non autorisé au journal en clair de l'Application.

L'Application doit contrecarrer les risques, grâce à la politique de sécurité mise en vigueur qui comprend des mesures techniques et organisationnelles. Les journaux doivent consigner le strict nécessaire des éléments pertinents et des événements saillants de la mise en vigueur de la politique de sécurité, lesquels témoignent de la situation informatique *hic et nunc*.

POLITIQUE DE SÉCURITÉ

Politique de sécurité discrétionnaire

Le titulaire est souverain numériquement ; il est responsable de son patrimoine numérique et du comportement numérique des machines des internautes et des appareils mobiles qui dépendent de sa politique de sécurité.

La politique de sécurité est à la discrétion de l'utilisateur, c'est-à-dire non obligatoire. Même installée, le titulaire de l'abonnement peut désactiver l'Application quand bon lui semble. Toutefois, le journal enregistrera le fait que l'Application a été désactivée.

L'Application doit être sécurisée et digne de confiance : elle doit fonctionner correctement (intégrité et disponibilité). Le titulaire de l'accès (ou l'Administrateur) est souverain de son patrimoine numérique et responsable de son comportement. Il doit donc connaître les conséquences de ses choix en matière de politique de sécurité.

- Il peut installer l'Application ou pas ; l'installation sera basée sur le volontariat. Il peut la désinstaller.

- Il peut l'activer ou la désactiver sur l'un des ordinateurs ou sur tous les ordinateurs, s'il le souhaite.

L'Application s'installera, sous le contrôle du titulaire de l'abonnement, par un téléchargement de manière automatique, par exemple via les FAI ou les éditeurs de solutions de sécurité. Et il sera mis à jour automatiquement, également sous son contrôle.

L'Application doit être identifiée dans son environnement informatique, elle doit être disponible, intègre, infalsifiable.

L'Application produit des journaux d'événements. Les journaux sont optionnels. Le journal est sécurisé (intègre dans sa version claire ou bien intègre et confidentiel dans sa version chiffrée). L'Application et les journaux associés sont liés de manière sécurisée.

Rôles de chacun dans la politique de sécurité

Il existe deux rôles principaux :

- L'Administrateur : c'est la personne qui a accès aux fonctionnalités d'administration du produit ou du service. Il est chargé de la politique de la sécurité et responsable de l'Application.

- L'utilisateur : il s'agit d'un ou plusieurs utilisateurs autorisés à utiliser l'accès sécurisé au FAI via la ligne du titulaire de l'abonnement ou utiliser l'accès au réseau mobile. Si ce sont les employés d'une entreprise ou d'une institution, les clients d'un hôtel ou d'un cybercafé. Si ce sont les proches ou les membres du foyer du titulaire qui utilisent son accès internet, sous sa responsabilité ou si ce sont des membres du foyer qui utilisent des appareils nomades pour se connecter aux réseaux sans fils via une ligne du titulaire d'accès, ces personnes ont été instruites sur les conséquences du téléchargement illégal et sur la contrefaçon sur les réseaux.

Profil d'utilisateurs dans le cadre de la politique de sécurité

L'Administrateur peut créer ses propres profils selon son contexte particulier d'utilisation.

Un ensemble de profils de base doit être proposé avec l'Application.

CRYPTOLOGIE

On utilisera, pour toute la partie cryptographique (chiffrement symétrique, chiffrement asymétrique, signature électronique, authentification, horodatage, etc.), les algorithmes et les protocoles cryptographiques standards en vigueur.

FONCTIONNALITÉS CLÉS DE L'APPLICATION CONFORME AUX SFH

Sont regroupées dans ce chapitre les fonctionnalités qu'une Application conforme aux Spécifications Fonctionnelles Hadopi doit posséder.

Ces fonctionnalités sont classées en 5 catégories, les fonctionnalités générales, les fonctionnalités du module d'Administration, les fonctionnalités du module de Traitement, les fonctionnalités du module de Journalisation, les fonctionnalités du module de Sécurité.

FONCTIONNALITÉS GÉNÉRALES

- Il existe des listes noires composées d'entités informatiques (logiciels, fichiers, signature de fichiers, protocoles, URL, ports , IP, etc.) interdites et présentant un risque en matière de contrefaçon
- Il existe des listes blanches composées d'entités informatiques autorisées
- Il existe un ensemble de règles de sécurité (conditions ==> actions)
- Il existe un ensemble de définitions des notifications
- Il existe une interface graphique
- Il existe un module Administration (module 1)
- Il existe un module Traitement (module 2)
- Il existe un module Journalisation (module 3)
- Il existe un module Sécurité (module 4)

FONCTIONNALITÉS DU MODULE D'ADMINISTRATION (MODULE 1)

- Les rôles (Utilisateur, Administrateur, titulaire de l'accès) et droits de chacun sont définis par des profils
- Installation/désinstallation facile
- Activation/désactivation facile
- L'interface graphique doit être discrète en l'absence de notification de haut niveau
- L'interface graphique permet à tout moment à l'Administrateur ou à l'Utilisateur d'apprécier le niveau de risque en matière de contrefaçon
- L'interface graphique rend visible à l'Administrateur ou à l'Utilisateur les notifications de haut niveau remontées par le module de traitement (module 2)
- L'interface graphique permet de répondre aux notifications de haut niveau
- Un mode silencieux permet de ne pas rendre visible les notifications de haut niveau remontées par le module de traitement (module 2)
- Le mode silencieux est activable par l'Administrateur
- Les règles de sécurité doivent régulièrement être mises à jour
- Les listes doivent régulièrement être mises à jour
- Les définitions des notifications doivent régulièrement être mises à jour
- Les erreurs et bugs, susceptibles d'entrainer un dysfonctionnement, connus par l'Éditeur doivent être corrigés
- Les failles de sécurité connues par l'Éditeur doivent être corrigées
- L'Administrateur peut autoriser la transmission de données à l'Éditeur en vue d'une amélioration de l'implémentation (rapport de crash, correction de bugs, de failles, etc.)
- Aucune fonctionnalité cachée supplémentaire ne doit exister

FONCTIONNALITÉS DU MODULE DE TRAITEMENT (MODULE 2)

- Analyse de la configuration informatique (postes informatiques, logiciels installés, base de données, répertoire, etc.)
- Analyse de la configuration réseau (règles pare-feu, sécurité des liaisons entre le point d'accès Wifi et les postes de travail, etc.)
- Analyse du comportement des logiciels en fonctionnement
- Analyse statistique (comptage des trames montante et descendant par adresse physique d'équipement, etc.)
- Analyse dynamique des flux réseau (analyse et reconnaissance des flux et protocoles qui transitent par l'accès à Internet)
- Des notifications de bas niveau sont générées lorsque les analyses mises en correspondance avec un profil et les listes révèlent un risque potentiel en matière de contrefaçon
- Des notifications de haut niveau sont générées lorsque la mise en correspondance des notifications de bas niveau avec un profil et les règles de sécurité révèlent un risque avéré en matière de contrefaçon
- Les notifications de haut niveau sont portées à connaissance de l'Administrateur ou de l'Utilisateur via l'interface graphique (module 1)
- Les Utilisateurs peuvent répondre (ignorer, appliquer la mesure proposée, etc.) aux notifications de haut niveau via l'interface graphique (module 1)
- Les notifications et leurs contextes (date, heure, etc.) doivent être journalisées (module 3)
- L'Analyse statistique peut être désactivée par le titulaire de l'accès internet
- L'Analyse dynamique peut être désactivée par le titulaire de l'accès internet
- Les règles de sécurité doivent être écrites dans une norme commune à tous les Éditeurs

FONCTIONNALITÉS DU MODULE DE JOURNALISATION (MODULE 3)

- Il existe par Utilisateur trois options de journalisation :
  - Pas de journal
  - Journal intègre en clair (module 4)
  - Journal intègre et chiffré (module 4)
- Les journaux utiliseront le standard Syslog ou IDMEF
- Les évènements à journaliser sont les suivants :
  - Mise en route/Arrêt de l'Application
  - Mise en route/Fermeture de la connexion réseau
  - Activation/Désactivation de l'Application ou d'une de ses fonctionnalités
  - Changement de profils
  - Notifications générées
  - Réponses aux notifications
- Les journaux doivent pouvoir être conservés.

FONCTIONNALITÉS DU MODULE DE SÉCURITÉ (MODULE 4)

- Il existe trois rôles Utilisateur, Administrateur et titulaire de l'accès internet
- Le titulaire de l'abonnement endosse le rôle d'Administrateur et de titulaire de l'accès internet
- Le titulaire de l'abonnement peut confier le rôle d'Administrateur à un Utilisateur
- L'Application est sécurisée (disponibilité, intégrité, confidentialité, traçabilité)

- L'Application ne doit pas faire baisser le niveau de sécurité global sur lequel elle est déployée
- Les sujets (Utilisateur, logiciel en exécution, etc.) sont identifiés
- Les objets (matériels, logiciels, données) sont identifiés
- Les mises à jour (listes, règles, définitions notifications, etc.) sont sécurisées (disponibilité, intégrité, confidentialité, traçabilité)
- Les listes, règles de sécurité, définition des notifications sont sécurisées (disponibilité, intégrité, confidentialité, traçabilité)
- Les journaux sont sécurisés (disponibilité, intégrité, confidentialité, traçabilité) en accord avec les options de journalisation (module 3)
- L'horodatage des journaux est sécurisé (disponibilité, intégrité, confidentialité, traçabilité)
- Seul l'Administrateur peut installer et désinstaller l'Application
- Seul l'Administrateur peut activer et désactiver l'Application
- Un ensemble de profils de base (Utilisateur, Administrateur, titulaire de l'accès internet) sont proposés par défaut
- Seul l'Administrateur peut gérer (créer, modifier, supprimer) les profils
- Seul le titulaire de l'accès internet et l'Utilisateur peuvent vérifier l'intégrité du Journal dudit Utilisateur
- Seul le titulaire de l'accès internet peut déchiffrer un journal chiffré
- Les listes sont modifiables par le titulaire de l'accès internet

COMPLÉMENTS DES SPÉCIFICATIONS FONCTIONNELLES À DESTINATION DES PROFESSIONNELS (ORGANISMES COLLECTIFS)

Ces compléments de spécifications s'adressent aux organismes collectifs : entreprises de toute taille (Grands Groupes, Entreprises avec agences, PME/PMI), administrations collectivités locales, ministères, universités, établissements scolaires, associations, hôpitaux, hôtels, cybercafés, aérogares, *hotspots* publics, restaurants, etc.

Dans ces organismes, le titulaire de l'accès internet est le chef d'entreprise ou le chef d'établissement qui peut confier cette responsabilité à sa direction informatique (DSI) ou à un service (interne ou externe) équivalent. Cette Direction désigne en général un Administrateur de la sécurité, quand il n'existe pas de RSSI. Pour les PME/PMI, un employé, avec une expertise informatique, joue en général ce rôle. Parfois la mission est confiée à un prestataire de service qui assure sous forme contractuelle les diverses missions.

Ces compléments expliquent l'adaptation envisageable et l'intégration possible de l'Application au contexte d'un organisme collectif, avec les produits et/ou services de sécurité réseau déjà déployés dans ces entreprises ou ces établissements.

LA SECURITE NUMERIQUE DES ORGANISMES COLLECTIFS

Dans une organisation, il existe en général un système d'information en réseau intranet qui est protégé par des mesures techniques et organisationnelles.

- La sécurité des réseaux locaux et l'interconnexion avec les réseaux publics est assurée par des filtrages (pare-feu, système de détection d'intrusion, de virus, de spam, de liens vers des sites de torrents, filtrage du Web, etc.) qui assurent la protection et le contrôle des réseaux haut débit contre les menaces diverses et variées. La sécurité du point d'accès, surtout pour les utilisateurs autorisés nomades, est en général assurée de manière centralisée (prévention des intrusions, contrôle des accès réseaux Wi-Fi, contrôle des applications). Les dispositifs de filtrage se situent soit sur un serveur mandataire ou derrière le pare-feu installé à la frontière du réseau de l'organisation. En général, aucun logiciel n'est installé sur les ordinateurs ou tablettes ou téléphones portables.

- La sécurité de l'information est assurée par des dispositifs de sécurité et des mécanismes de cryptologie (protocole cryptographique, chiffrement, signature électronique) pour protéger l'échange et le partage des données entre les postes de travail, les téléphones et les serveurs.

- La sécurité numérique dans une organisation est en général sévère, stricte et rigoureuse. Elle prend en compte les utilisateurs du réseau fixe et la nomadicité des utilisateurs.

LES DISPOSITIFS DE SECURITE EXISTANTS PERTINENTS

Les filtres du Web

Les filtres Web répondent pour les organismes collectifs aux problématiques suivantes :

- Filtrer les accès Wi-Fi publics et privés ;
- Filtrer les groupes d'utilisateurs selon une politique de sécurité ;
- Vérifier a posteriori dans les logs, les sites Web visités ou les services utilisés par les usagers autorisés (Skype, BitTorrent, P2P, etc.).

Le filtrage peut être passif (aucun impact sur l'utilisateur avec la seule journalisation des accès) ou actif (blocage éventuel des flux des utilisateurs).

Le blocage est déterminé sur des plages horaires, des extensions ou des types de fichiers. Le filtre peut bloquer les VPN de tout type. En entreprise, en général, on bloque le trafic VPN en sortie afin que les utilisateurs ne puissent pas contourner les systèmes de protection.

Le responsable de sécurité peut détecter statistiquement si un employé fait un usage intempestif de l'internet, s'il utilise de manière abusive les ressources informatiques pour son propre compte, s'il fait du téléchargement, dans les limites des lois applicables (respect des doits de l'employé, information des comités, etc.).

Ces filtres Web sont mis à jour régulièrement, souvent en temps réel via des tunnels sécurisés. La configuration du filtre est sécurisée (et enregistrée à intervalles réguliers).

En cas d'alertes, le responsable de sécurité est directement alerté par messagerie électronique.

Le filtrage des contenus

Dans certaines organisations, il existe des dispositifs de filtrage de contenus. Installée comme une passerelle de filtrage de contenus, cet outil agit directement sur les flux de communication et constitue ainsi une barrière complémentaire de l'analyse locale (antivirus et antispyware sur poste de travail). Pour assurer un niveau complet de sécurité, on effectue l'analyse intégrée des contenus de communication. Les contenus hostiles (virus, spywares, scripts, codes malveillants) et les non sollicités (spam, divers Web) sont bloqués avant d'atteindre les systèmes d'information.

Ce sont des technologies en temps réel qui combinent les techniques de filtrage avec état (utilisées pour le filtrage IP) et l'analyse des couches Applicatives. Les filtres bloquent les attaques contre le réseau et les attaques qui exploitent les vulnérabilités des applications. L'analyse effectuée repose sur l'analyse des flux échangés par les protocoles de communication des applications. Les filtres analysent les protocoles suivants : IP, ICMP, TCP, UDP, HTTP, SMTP, FTP, DNS, SNMP, H323, RTP, SIP, SSL, etc.

Le niveau de contrôle est configuré par l'Administrateur à l'aide de l'interface d'administration.

SITES AVEC UN NOMBRE ÉLEVÉ D'UTILISATEURS

Dans une organisation avec un grand nombre d'utilisateurs, l'Application n'est en général pas installée sur les postes des utilisateurs. Les fonctions s'opèrent en général par une observation (passive ou active) sur le réseau, en amont des postes de travail. Dans ce cas, l'Application se rapproche des N-IDS (*Net-Intrusion Detection System*) dans le réseau local ou des pare-feu applicatifs à la frontière du réseau.

Pour les organisations et entreprises, l'Application peut se présenter sous la forme d'un pare-feu applicatif puissant à la frontière du réseau local de l'organisation ou bien l'Application peut se présenter sous la forme de sondes (analyseur de protocoles) sur le réseau de l'organisation, gérées sur une station de supervision de réseau, opérée par le responsable de sécurité de l'établissement. C'est un réseau de capteurs où les postes des utilisateurs ne sont pas concernés. Le responsable de sécurité, ou l'ingénieur réseau, supervise le trafic et les flux en examinant les indicateurs des sondes branchées sur le réseau.

Une solution centralisée sous forme de station de supervision branchée à des sondes en réseau (et non pas sur les postes de travail des utilisateurs) permet une gestion simple et efficace :

- l'installation est unique et ne nécessite pas d'intervenir sur l'ensemble des postes de travail. La charge de travail des services internes en est limitée ;
- la mise à jour est efficace car concentrée sur un équipement ;
- elle n'est pas contournable sur le poste de travail (en entreprise, certains utilisateurs possèdent les droits administrateurs), car elle est présente sur le réseau ;
- elle peut être aisément dupliquée sur l'ensemble des sites des entreprises, la DSI pouvant avoir une politique unique de sécurité.

Pour ces sites, l'Application doit savoir gérer les serveurs qui traitent des multiutilisateurs et des multisessions.

MODE DE LA SOLUTION : PRODUIT OU SERVICE

Lorsque la solution est un produit, ce produit est installé, opéré et maintenu en conditions opérationnelles par le personnel compétent et dûment habilité.

Lorsque la solution est un service, ce service peut être assuré en interne par une société de service qui maintient en conditions opérationnelles les ressources informatiques du service. Ce service peut être externalisé, tant au niveau des ressources informatiques (tout ou partie à l'extérieur du périmètre de l'organisation) que de la gestion de la solution.

Lorsque l'Application est un service, il existe un contrat qui stipule entre autres choses que le prestataire :

- distribue les listes de contrôle (listes noires et blanches, signatures, etc.) conforme à la réglementation ;
- conserve les journaux dans un centre de données sécurisé, afin d'assurer la traçabilité et fournisse un service de stockage et d'archivage.

L'APPLICATION CONFORME AUX SFH

Le responsable de l'organisme collectif cherche à protéger son accès vers internet avec des objectifs parfois contradictoires :

- avoir la meilleure protection contre les attaquants,
- respecter le cadre légal d'usage des ressources télécoms et informatiques,

- ne pas ennuyer l'utilisateur pour augmenter sa productivité,
- bénéficier du meilleur coût.

Sur les systèmes d'information de plus de 20 personnes, les dispositifs de type SFH existent déjà, de plusieurs natures et de plusieurs origines (français, européens et autres). Pour les Grands Groupes, ce sont souvent des systèmes propriétaires ad hoc intégrés à leur système de sécurité.

Une Application conforme aux SFH pourra emprunter des éléments aux spécifications des dispositifs de sécurité existants mais devra les compléter et les adapter à l'objectif de lutte contre les contrefaçons en ligne.

L'Application peut être intégrée comme une extension dans un dispositif de sécurité.

MESURES ORGANISATIONNELLES

Pour compléter l'action de l'Application conforme aux SFH, il est important que les organisations mettent en place des mesures organisationnelles.

Dans les organisations, il est recommandé qu'une charte informatique explicitement mentionne la contrefaçon comme interdite et qu'une session de sensibilisation soit introduite dans le calendrier de l'établissement de façon que les utilisateurs des ressources informatiques soient effectivement prévenus des risques encourus respectivement par le responsable de l'établissement, par le responsable de sécurité et par l'utilisateur, si les ressources informatiques sont utilisées pour capturer illégalement des œuvres. Les utilisateurs de chaque organisme collectif sont informés (et signent une charte) lorsqu'ils accèdent pour la première fois à ces ressources.

SPÉCIFICATION GÉNÉRALE : COMPLÉMENT PROFESSIONNEL

CARACTERISTIQUES GENERALES

L'Application doit être :

- non-intrusive dans le fonctionnement courant et légal de l'accès aux réseaux (internet, téléphone) pour ne pas impacter la performance des systèmes de l'utilisateur.

L'Application et les MS doivent être :

- sécurisés, administrables, pour vérifier leur bon fonctionnement et éviter leur piratage,
- auditables pour vérification de leur bonne utilisation.

Les divers éléments (1, 2, 3, 4 et 5) de la synthèse des spécifications générales sont à la discrétion et dans les termes choisis par le titulaire de l'accès internet. Il est clair que dans le domaine professionnel, il est recommandé de rendre tous ces éléments actifs sur l'ensemble des machines concernées.

L'élément 4 concernant l'affichage des notifications et des alertes pédagogiques doit être tempéré par l'exigence de productivité d'un organisme collectif. La spécification se limitera à des comptes-rendus différés (via par exemple des *emails*) aux utilisateurs (à des intervalles

de temps à définir) des alertes remontées à l'Administrateur par l'Application de façon à sensibiliser les utilisateurs au respect de la politique de sécurité.

MODULE 1 : LE MODULE D'ADMINISTRATION (VERSION PROFESSIONNELLE)

BUT – FONCTIONNEMENT

Lorsque l'Application est un système autonome ou un service externalisé, elle est gérée par le l'Administrateur qui assure les mises à jour, la conformité, l'efficacité et l'innocuité du système ou du service.

ERGONOMIE

L'Application est quasi-transparente aux utilisateurs. Pour les architectures des MS dans les organisations, l'Application est transparente pour les terminaux des utilisateurs (quasiment rien n'est installé sur le poste des utilisateurs).

La présence et le fonctionnement de l'Application ne demande pas de connaissances techniques aux utilisateurs (internautes, téléphonie mobile).

INTERFACE GRAPHIQUE

L'interface de l'Administrateur a les caractéristiques suivantes :

- Possibilité d'activer et de désactiver l'Application (en quelques clics) ;
- Gestion des profils avec envoi d'un message électronique aux utilisateurs.

MODULE 2 : LE MODULE DE TRAITEMENT (VERSION PROFESSIONNELLE)

Dans les entreprises où la simplicité et la facilité de mise en œuvre de la politique de sécurité est primordiale, les listes sont noires (entités interdites) ou blanches (entités autorisées). La politique de sécurité est alors stricte. L'utilisateur n'a pas la possibilité d'outrepasser les règles sans violer cette politique de sécurité, et le filtrage (autorisation ou blocage) s'opère selon la définition de la politique de sécurité.

La politique de sécurité s'appuie sur les éléments cumulatifs :

- Élément 1 : Aide à la sécurisation de la connexion et de l'accès par une analyse statique et/ou dynamique, approfondie, de la gestion de configuration informatique et réseau, et un contrôle de l'utilisation des ressources par le titulaire de l'accès internet.

  ⇒ Il existe déjà de nombreux outils sur étagère pour contrôler la gestion de configuration de l'environnement informatique et réseau d'un intranet afin d'aider à sécuriser une connexion à un réseau public.
  ⇒ Il existe déjà de nombreux outils sur étagère pour contrôler les ressources informatique dans un établissement tout en respectant la sphère privée des utilisateurs.

  ✓ Analyse de la gestion de configuration informatique (ex : analyse statique de la configuration de postes informatiques ; logiciels installés) ;

- ✓ Analyse statique de la configuration réseau (ex : analyse de la configuration du pare-feu et de la DMZ, analyse des répertoires des listes blanches des adresses physiques MAC des machines autorisées à dialoguer à travers le point d'accès et des listes noires des adresses interdites).
- ✓ Analyse dynamique des logiciels en fonctionnement, et contrôle des utilisations par le titulaire de l'accès internet.

- Élément 2 : Aide à la sécurisation de l'accès par le calcul de diverses statistiques.

  ⇒ Les pare-feu du marché produisent des statistiques qui permettent de discerner si des intrusions pénètrent ou sortent du réseau local ou bien si un utilisateur autorisé utilise de manière intempestive le réseau externe.

- Élément 3 : Aide à la prévention de téléchargement illégal et de contrefaçon par l'observation en temps réel, sans enregistrement des flux et protocoles qui transitent par l'accès ; sur la base de l'observation et de la politique de sécurité choisie, une ou plusieurs des actions techniques suivantes peuvent s'appliquer :

  ⇒ si cette fonction de l'Application est débrayée sur certaines machines de l'environnement, l'Administrateur ne pourra détecter des événements susceptibles de poser des problèmes de transferts sur ces machines.

- Élément 4 : Compte-rendu des alertes aux utilisateurs autorisés dans un but d'information mais aussi pédagogique de sensibilisation.

  ⇒ Le compte-rendu ne se réalise pas nécessairement en temps réel. Il peut être différé et adressé aux utilisateurs par messagerie, après exploitation par l'Administrateur. Le débrayage de ces comptes-rendus peut être souhaitable dans le souci de ne pas importuner les utilisateurs pour des raisons de productivité, par exemple.
  ⇒ Il est souhaitable de mettre en option un mode silencieux.

LE SOUS-MODULE D'ANALYSE DYNAMIQUE DE FLUX

Le but de ce module est d'inspecter dynamiquement le contenu entrant et sortant du trafic sur les interfaces du réseau des machines des utilisateurs.

LE MOTEUR D'ANALYSE PROTOCOLAIRE

Le moteur de bas niveau

Dans un premier temps, un moteur de bas niveau dans des sondes branchées sur le réseau quand il s'agit d'une architecture distribuée à l'extérieur des postes des utilisateurs, capte à la volée le trafic réseau et décode syntaxiquement les différentes couches protocolaires de manière à en extraire des caractéristiques (motifs distinctifs, signature protocolaire).

Le moteur de haut niveau

L'identification des protocoles utilisés, des logiciels en cours de fonctionnement ou des URL utilisés, est intéressante, mais n'est pas nécessairement liée à la pile protocolaire. Les volumes des flux entrant et sortant sont des indicateurs précieux qui permettent de détecter la sémantique de la pile protocolaire réelle, en cours d'exécution.

Les notifications et alertes

Dans les organisations, il est plus courant de devoir appliquer de façon stricte une politique de sécurité plutôt que de détecter dynamiquement une application et ensuite demander l'accord. L'utilisateur n'a pas le choix et n'intervient pas dans la décision : les actions sont autorisées ou interdites, selon la politique de sécurité, connue de chaque utilisateur, grâce à la charte informatique et aux séances de sensibilisation. Dans ce cas précis, les notifications et les alertes seront remontées à l'Administrateur.

Il n'est donc pas impératif de posséder un système de notification de l'utilisateur. Il est de coutume de ne pas ennuyer l'utilisateur et de rendre la solution la plus transparente possible.

MODULE 3 : LE MODULE DE JOURNALISATION (VERSION PROFESSIONNELLE)

Dans une organisation, les journaux sont collectés de manière automatique par les Administrateurs sur une station de supervision et conservés (voire intégrés) dans un système de sauvegarde sécurisé.

Si l'Application est un service externalisé par un prestataire, les journaux peuvent être transportés de manière sécurisée, en dehors de l'organisme, à travers le réseau.

Ce peut être le cas pour des organismes avec de nombreuses agences qui ont pour des raisons économiques un service d'Application centralisée.

Afin d'assurer la pérennité du journal, une sauvegarde est envisageable sur un serveur externe dans un coffre électronique. Le serveur est alors hébergé dans un lieu sécurisé.

MODULE 4 : LE MODULE DE SÉCURITÉ (VERSION PROFESSIONNELLE)

Dans un contexte où il existe de nombreux utilisateurs (dans les institutions, dans les entreprises), l'Application est sécurisée par des mesures organisationnelles.

RISQUES

Hypothèses sur l'environnement

L'Application doit être installée sur un système sain, correctement mis à jour, en particulier concernant les correctifs liés à la sécurité. Le système d'exploitation supportant l'Application, est correctement administré et configuré. En particulier, les accès aux différents composants de l'Application ne sont accessibles qu'aux seules personnes autorisées (ayant le rôle d'administrateur).

Il convient également de sécuriser le système, par désactivation des services et partages inutiles.

Les Administrateurs de l'Application sont considérés comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

L'Administrateur consulte régulièrement les événements d'audit générés par l'Application, analyse et traite les alertes engendrées et remontées par l'Application.

Les équipements contenant les services de l'Application, ainsi que tous supports contenant les biens sensibles de l'Application (papier, sauvegardes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux Administrateurs.

L'Administrateur dispose des moyens de contrôler la configuration matérielle et logicielle de l'Application par rapport à un état de référence, ou de la régénérer dans un état sûr.

L'heure est de confiance (la sécurité de l'horodatage n'est pas nécessaire).

POLITIQUE DE SECURITE

Rôles de chacun dans la politique de sécurité

Le rôle de l'Administrateur

Le rôle de l'Administrateur, personnel de la DSI, est très important, car c'est lui qui gère (en temps réel ou en différé) la sécurité des flux entrant et sortant, par exemple au moyen d'une station de supervision, avec des outils pour exploiter les journaux de tous les utilisateurs. L'Administrateur obéit à une déontologie claire et précise pour respecter la sphère privée des individus dans le cadre de ces organisations. On peut définir dans ce cas des politiques de sécurité silencieuses, où l'utilisateur n'est pas alerté en permanence, et/ou n'a pas à outrepasser la politique de sécurité définie par le responsable de l'établissement.

Des mesures organisationnelles (politique de sécurité, charte informatique, règlement intérieur, contrat de travail, définition de poste, séance de sensibilisation, plan de formation) permettent de compléter les mesures techniques afin d'informer le personnel et de respecter la confidentialité et l'intégrité des activités des membres du personnel.

Le rôle de l'utilisateur

En entreprise, la mise en vigueur d'une politique de sécurité doit être simple et efficace, car elle s'adresse à une population plus grande d'individus. Il n'est donc pas souhaitable dans cette situation de laisser chaque employé décider en temps réel s'il bloque ou s'il laisse passer certains flux. La décision doit être prise en amont par le dispositif de sécurité du système d'information de l'entreprise. Le filtrage peut dans ce cas, se faire par des instruments sur le réseau de l'entreprise, géré par l'Administrateur.

Ces dispositifs sont sous le contrôle de la personne qui a le rôle de l'Administrateur. Ce peut être un responsable de sécurité. Ce rôle peut être délégué à un prestataire de service, digne de confiance. Dans ce cas, l'analyse protocolaire en temps réel filtre les flux des utilisateurs et applique une politique de sécurité donnée, sans possibilité de l'outrepasser en temps réel par un quelconque utilisateur.

L'Administrateur veille à ce que les utilisateurs soient informés (politique de sécurité, charte, sensibilisation, formation) sur l'existence de ce dispositif en conformité avec la législation sur les données à caractère personnel.

Profil d'utilisateurs dans le cadre de la politique de sécurité

Pour les administrateurs, l'Application permet de créer des listes personnelles, additionnelles, des profils différents par utilisateur, selon des plages horaires, des volumes et débits de trafic entrant et sortant, etc. Ces ajouts et modifications sont enregistrés dans le journal de l'Application.

Ces profils peuvent être associés à un couple identifiant / mot de passe dont le niveau de sécurité doit être satisfaisant, et sont automatiquement sélectionnés lorsqu'un utilisateur ouvre une session.

Les caractéristiques d'un profil permettent d'établir des règles dépendantes de plusieurs paramètres :

- L'utilisateur (ou le groupe d'utilisateurs) identifié et authentifié ;
- La plage horaire ;
- L'adresse ou la plage d'adresses du réseau.

Les Administrateurs peuvent définir leurs propres catégories de sites :

- *Black-lists* / listes noires (sites interdits) ;
- *White-lists* / listes blanches (sites autorisés).

FONCTIONNALITÉS COMPLÉMENTAIRES DE L'APPLICATION CONFORME AUX SFH À DESTINATION DES PROFESSIONNELS (ORGANISMES COLLECTIFS)

Sont regroupées dans ce chapitre les fonctionnalités qu'une Application conforme aux Spécifications Fonctionnelles Hadopi destinée aux professionnels (organisation collectives) doit posséder en plus des fonctionnalités clés précédemment définies. Dans le cadre de l'élaboration d'une Application destinée aux professionnels (organismes collectifs) et en cas de conflit avec une fonctionnalité clé listée précédemment la priorité doit être accordée aux fonctionnalités présentées ci-dessous.

Ces fonctionnalités sont regroupées en 5 catégories, les fonctionnalités générales, les fonctionnalités du module d'Administration, les fonctionnalités du module de Traitement, les fonctionnalités du module de Journalisation, les fonctionnalités du module de Sécurité.

FONCTIONNALITÉS GÉNÉRALES

- Ne doit pas entraver le fonctionnement courant (accès au réseau, performances des systèmes, etc.)

FONCTIONNALITÉS DU MODULE D'ADMINISTRATION (MODULE 1)

- Les notifications de haut niveau ne seront pas rendues visibles à l'Administrateur ni aux Utilisateurs
- Les notifications de haut niveau seront envoyées en différé par mail à l'Administrateur
- L'interface graphique permet à l'Administrateur d'envoyer des messages électroniques aux Utilisateurs

FONCTIONNALITÉS DU MODULE DE TRAITEMENT (MODULE 2)

- Les Utilisateurs ne peuvent répondre (ignorer, appliquer la mesure proposée, etc.) aux notifications de haut niveau

FONCTIONNALITÉS DU MODULE DE JOURNALISATION (MODULE 3)

- Les journaux sont collectés automatiquement et conservés dans un système de sauvegarde

FONCTIONNALITÉS DU MODULE DE SÉCURITÉ (MODULE 4)

- L'horodatage des journaux n'est pas à sécuriser
- L'Administrateur peut modifier (ajout, création, suppression) l'ensemble des définitions des notifications
- L'Administrateur peut modifier (ajout, création, suppression) l'ensemble des définitions des règles de sécurité
- Le système de sauvegarde des journaux est sécurisé (disponibilité, intégrité, confidentialité, traçabilité)
- L'Administrateur peut contrôler la configuration matérielle et logicielle de l'Application

- L'Administrateur peut rétablir la configuration matérielle et logicielle de l'Application à un état de référence

COMPLÉMENTS DES SPÉCIFICATIONS FONCTIONNELLES À DESTINATION DU GRAND PUBLIC (PARTICULIERS ET TPE)

Ces compléments des spécifications s'adressent au grand public et aux TPE (Très Petites Entreprises). Ils sont orientés vers une solution logicielle installée sur le poste de travail, ou bien dans les boîtiers de point d'accès internet, que cette solution soit un produit géré par le titulaire de l'abonnement ou bien soit un service délivré par un prestataire.

LA SECURITE NUMERIQUE DES PARTICULIERS ET TPE

À ce jour, les logiciels de sécurisation pour l'accès à internet, qui existent sur le marché, destinés à des particuliers, sont essentiellement des suites de sécurité internet vendues sous forme de *packs* de sécurité ou bien des logiciels autonomes (payants ou gratuits), indépendamment des solutions de sécurisation du boîtier de connexion et de sa liaison avec l'ordinateur personnel.

Ces ensembles de logiciels comportent en général un logiciel de contrôle parental, un antispam (contre le pourriel), un pare-feu, un antivirus et anti-espio-logiciels pour contrôler l'utilisation du poste de l'utilisateur connecté à internet.

Ces produits sont mis à jour en permanence, parfois quotidiennement, pour contrecarrer les attaques nouvelles qui apparaissent sur le réseau (nouveaux virus, nouvelles formes de *spam*, mises à jour des listes noires de sites contenant des fichiers illicites ou inappropriés, mises à jour de listes blanches de sites autorisés, etc.). Ils sont un bouclier indispensable pour l'internaute qui veut préserver son patrimoine numérique personnel et éviter les désagréments d'une navigation sans précaution sur le Web.

LES DISPOSITIFS DE SECURITE EXISTANTS PERTINENTS

Les suites de sécurité

Les solutions de contrôle parental

Les produits de type « contrôle parental » permettent de restreindre le champ d'utilisation du poste pour les utilisateurs légitimes. Un contrôle parental comporte des profils d'utilisateurs (enfants, adolescent, etc.) pour réguler son utilisation et/ou vérifier sa navigation, par ses parents.

Les logiciels installés sur les ordinateurs des utilisateurs appliquent une politique de contrôle d'accès des flux entrant et sortant, paramétrée selon des critères et des paramètres qui tiennent compte :

- Des plages horaires de navigation et du volume d'heures maximum de navigation et utilisation des logiciels applicatifs (*Chat, P2P*, etc.), de protocoles (par jour et/ou par semaine).

- Des profils de navigation, selon les âges ou la maturité.

- Des listes noires : dans ce cas, il est possible de se connecter à l'ensemble des sites URL d'internet et pages du Web, excepté ceux qui sont inscrits dans cette liste. Dans le cadre du contrôle parental ces listes (centaines de milliers d'éléments, en général) sont définies et mises à jour par diverses organisations ou groupes d'ordre éthique.

- Des listes blanches : dans ce cas, il n'est possible de se connecter qu'à un site appartenant à une liste définie (pour les enfants, utilisé dans les établissements scolaires).

- Des types de fichiers pour empêcher le téléchargement de fichiers internet sur l'ordinateur : vidéo, musique, exécutables, images, fichiers compressés, etc.

- De tentatives multiples de connexions à une page censurée : le compte est alors bloqué et ré-activable par le titulaire de l'abonnement.

L'Administrateur du logiciel peut activer et désactiver les filtres, peut modifier la configuration des paramètres. Une personnalisation permet d'autoriser des accès interdits dans une catégorie.

Une journalisation (fichiers *.log) des événements (blocage, désactivation, etc.) permet de conserver un historique des navigations, des protocoles utilisés, et même de visualiser les pages visitées.

Le contrôle de l'accès internet des particuliers se limite aujourd'hui au contrôle parental. Celui-ci est opéré sur les postes clients au travers de logiciels fournis par les fournisseurs d'accès internet[39]. Malgré une plus grande maturité des outils utilisés, ces solutions de filtrage sont peu adoptées par les clients des principaux opérateurs (quelques pourcents seulement des clients). Une des raisons pouvant expliquer cette situation tient dans la complexité d'installation et de paramétrage des logiciels, mais aussi des problèmes de compatibilité des systèmes d'exploitation avec les versions téléchargées.

Les pare-feu

Les produits de type pare-feu personnel permettent de prévenir et réduire la prise de contrôle illégitime du poste par un tiers extérieur. Le pare-feu personnel permet de contrôler l'accès au réseau des logiciels installés sur la machine, et notamment empêcher les attaques par des chevaux de Troie, programme intrusif pour une prise en main à distance de la machine par un pirate. Cela dit, la prise de contrôle des ordinateurs existe malgré les pare-feu parce que les utilisateurs téléchargent et installent (souvent à leur insu) des logiciels malveillants.

Les antivirus

Un antivirus détecte les virus, les vers, les logiciels espions, qui s'immiscent subrepticement parmi les fichiers légitimes des utilisateurs ou dans la mémoire en tant que programme exécutable ou partie de code. Certains vers ne s'écrivent même pas sur le disque (comme SQL Slammer).

Les antivirus sont des logiciels d'analyse de contenu pour identifier des programmes malveillants (appelés virus, vers, chevaux de Troie, etc.) et les neutraliser en supprimant les fichiers contaminés ou en transportant dans une zone de quarantaine les fichiers supports, ou en éradiquant ces virus et réparant les fichiers infectés. Ces virus proviennent de l'extérieur (du Web, d'une clé USB, etc.), et circulent sur le réseau avec des propriétés de duplication.

Les antivirus scrutent les programmes au moment de leur lancement et protègent le système en observant certains appels (remplacement des fonctions du système d'exploitation par leurs méthodes de contrôle : par exemple à chaque accès aux fichiers une politique est vérifiée, chaque écriture est vérifiée en rapport avec la base des virus, etc.).

[39] Les applications de contrôle parental commencent à être intégrées dans certains systèmes d'exploitation : Mac OS X, Windows.

Les antivirus examinent les flux montants et descendants, les fichiers entrants, les courriers, etc., en temps réel ou bien analysent l'ensemble des dispositifs de stockage de l'ordinateur (disque fixe et amovible, mémoire, etc.) sur demande de l'utilisateur. Les algorithmes des antivirus sont variables en efficacité : comparaison avec des virus connus (analyse de signature virale), heuristique d'analyse de comportement, analyse morphologique (filtrage suivant des règles).

Les antispams

Les produits de type « antispam » réduisent la réception de pourriel et de messages non sollicités. Un antispam regarde le contenu des mails, des échanges selon des heuristiques plus ou moins sophistiquées : analyse par mot clés, analyse linguistique statistique. Mais ces techniques sont plutôt dépassées. Elles sont remplacées de nos jours par les heuristiques d'intelligence artificielles capables d'apprentissage basés sur les réseaux bayésiens. Cela ne concerne pas seulement la linguistique, mais aussi les formes, les formatages, la sémantique. Les FAI ont une bonne vision des spams car un spam est un message qui se distribue énormément : de ce fait les corrélations sont bien visibles.

La sécurité des systèmes d'exploitation et des protocoles

Il existe dans les MS des réseaux locaux des fonctions de sécurité indispensables pour le bon fonctionnement de l'environnement informatique.

Des fonctions de contrôle d'accès existent dans les systèmes d'exploitation des différents équipements, notamment grâce à une identification et une authentification de l'utilisateur à l'ouverture et à la reprise de session, avec les systèmes d'exploitation, locale ou distante.

Le contrôle d'accès plus fin dans les systèmes d'exploitation modernes permet notamment de restreindre certains programmes. Ce sont des mécanismes spécifiques de la protection de l'intégrité du système. Ce sont aussi la vérification des signatures pour tous les pilotes et tous les logiciels à installer, la protection d'exécution des données, la protection des piles, etc.

Des fonctions d'audit existent par la création de journaux des systèmes d'exploitation pour l'imputabilité (permettant de savoir qui a fait quoi).

Des fonctions d'identification existent, notamment les systèmes de gestion de fichiers qui identifient les fichiers pour chaque propriétaire.

Il existe des mécanismes de protection des données avec les systèmes de chiffrement de fichiers sur les disques durs utilisant un mot de passe lié au nom du compte de l'utilisateur (un ordinateur portable volé peut en effet servir à extraire des mots de passe d'accès pour utiliser la ligne du titulaire de l'accès).

Il existe enfin les systèmes de contrôle d'accès aux réseaux menant à la ligne du titulaire de l'accès internet, surtout dans le cadre des réseaux sans fil :

- Wi-Fi : WPA/WPA2 pour les particuliers mais aussi les portails captifs avec des logs pour les TPE de type hotspots/café internet ;

- 3G/UMTS : AKA par USIM, avec des logs dans l'USIM. Ces systèmes sont souvent complémentaires des pare-feu et des règles d'accès dans les équipements des FAI, que cela soit le SGSN/GGSN dans 3G ou le boîtier 3Play dans ADSL.

Boîtier ADSL

Ces fonctions de sécurité permettent de définir des règles d'accès, des zones de quarantaine, des serveurs bastions, des ports à utiliser sur certains équipements dans le réseau, etc.

La gestion des boîtiers varie selon le FAI. Certains boitiers ne se configurent qu'en local (Orange, SFR, etc.), certains autres ne se configurent que par le réseau (Free) ce qui laisse une trace d'une configuration chez un tiers (le FAI, en l'occurrence).

SITES AVEC UN NOMBRE RESTREINT D'UTILISATEURS

Pour les particuliers ou les TPE, l'Application peut être, par exemple, des dispositifs sous la responsabilité du titulaire de l'abonnement, soit dans les boîtiers ADSL, soit sur chacun des ordinateurs, soit répartis sur ces appareils informatiques. Ils peuvent être entièrement ou en partie dans les serveurs hébergés chez le FAI (mais sous la maitrise du titulaire) ou bien virtualisés sur plusieurs machines (de l'ordinateur du client au serveur, en utilisant le boîtier de connexion comme relais).

L'Application conforme aux SFH pourra emprunter des éléments aux spécifications des suites de sécurité existantes (qui n'ont pas été conçues à l'origine pour lutter contre la contrefaçon en ligne) mais devra les compléter et les adapter à l'objectif SFH.

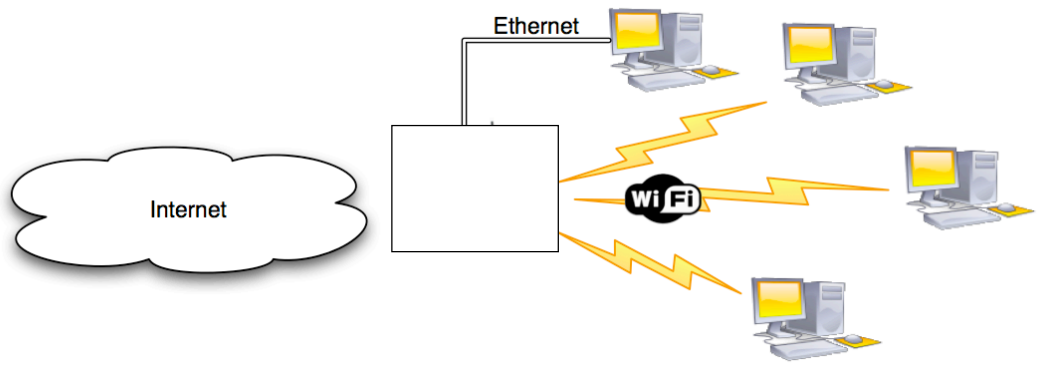

Figure 4: Architecture informatique chez un particulier : entre internet et les ordinateurs du particulier, le boîtier de connexion (« box ») fourni par le FAI. La liaison s'effectue par Wi-Fi ou par câble Ethernet.

MODE DE LA SOLUTION : PRODUIT OU SERVICE

Lorsque la solution est un produit géré par le titulaire de l'accès internet :

- La solution, déployée sur les postes terminaux (ordinateurs), peut être identifiée comme un module des suites de sécurité classiques actuelles dont font partie les antivirus, les pare-feu, le contrôle parental, les antispams, les antimalware…

- La solution, déployée sur les boîtiers, peut-être identifiée comme un filtre en amont de toutes les machines du titulaire, permettant à la fois, une granularité de politique de sécurité selon les utilisateurs et une identification physique et logique des machines pouvant être connectées, sécurisant ainsi la liaison entre ces machines et le point d'accès internet.

Lorsque la solution est un service géré par un opérateur de service, ce service d'option d'adhésion (*opt-in*) peut être proposé aux internautes et/ou aux utilisateurs de la téléphonie

mobile. La solution peut être installée dans les boîtiers ADSL ou bien peut être une solution sécurisée en réseau déployée via le réseau du FAI.

Il existe alors un contrat clair qui fixe les responsabilités entre le FAI d'une part et l'opérateur de sécurité d'autre part, ainsi qu'un contrat clair entre l'opérateur de sécurité et le client, titulaire de l'abonnement, notamment pour le respect de la sphère privée numérique et la confidentialité des données à caractère personnel (l'opérateur de sécurité devra pouvoir exhiber au client les traitements avec une certaine transparence de façon à éviter les portes dérobées, les captures de flux).

La sécurité des MS repose sur l'Application conforme aux SFH et s'appuie, par ailleurs, sur les fonctions de sécurité du système informatique du titulaire : par exemple, les MS utilisent la sécurisation classique de la connexion, c'est-à-dire le protocole cryptographique WPA entre les ordinateurs et le boîtier ADSL.

DIFFICULTES DE LA CONCEPTION DE L'APPLICATION DES MS

L'hétérogénéité des terminaux

La mise en place de moyens de sécurisation se heurte à la multiplication toujours croissante et diverse des terminaux connectés à internet au sein du foyer à travers la connexion Wi-Fi des boîtiers ADSL : tablettes, ordiphones, téléviseurs, consoles de jeux et autres tablettes électroniques. En effet, aucun éditeur de logiciel ne propose à ce jour de solution technique de sécurisation pour ces terminaux.

L'hétérogénéité des boîtiers

Le parc des boitiers est très hétérogène en France : modem, routeur, boîtiers « triple Play ». Certains boîtiers datent de 2003.

Cependant il existe une évolution de plus en plus rapide de ce parc pour réduire la maintenance de ces appareils chez l'habitant.

Par ailleurs, à l'avenir, le marché des *SetTopBox* de télévision risque de se transformer (les *SetTopBox* peuvent être davantage intégrée aux téléviseurs pour coder et déchiffrer les flux), si bien que les boîtiers ADSL risquent de devenir de véritables tours de contrôle géré par l'Administrateur, des passerelles ouvertes sécurisées indispensables à domicile pour administrer le réseau local.

Le parc de ces passerelles risque de converger à l'avenir vers des passerelles sécurisées avec des systèmes d'exploitation standard (de type Linux ou Unix BSD). Il est probable que le titulaire de l'abonnement devra dans le futur piloter la sécurité et surveiller son accès à partir de cette passerelle, plutôt que de surveiller les actions et les commandes informatiques à partir de la kyrielle de terminaux autorisés.

La sécurité de l'Application

Une Application propriétaire d'un Éditeur risque, comme tout autre logiciel de sécurité, d'être attaquée.

L'APPLICATION CONFORME AUX SFH

Une Application conforme à SFH doit emprunter des fonctionnalités aux différentes catégories de produits existants, décrits ci-dessus. En effet, une Application est :

- Construite fonctionnellement comme un pare-feu mais avec une reconnaissance plus fine des protocoles applicatifs observés, y compris les encapsulations de protocoles en poupées russes.

- Construite fonctionnellement comme l'architecture d'un contrôle parental, sauf que ce n'est pas un parent mais un titulaire de l'abonnement qui est responsable et qui peut définir des profils pour réguler l'utilisation de l'internet dans son foyer. Une Application ne journalisera pas d'historique de navigation. La notion de profil d'utilisateur implique qu'il existe dans le réseau local et dans l'environnement informatique des fonctions d'identification et de contrôle d'accès de ces utilisateurs.

- Construite comme une structure d'antivirus car l'Application devra se protéger contre les différentes attaques qui pourraient surgir contre elle-même. Elle devra détecter des procédures et les logiciels de contournement, etc. L'Application aura besoin de l'antivirus car certains vers, virus ou bots pourraient réaliser des actions illicites via la ligne du titulaire de l'accès internet sans qu'il puisse s'en apercevoir.

- Un antispam : tant qu'il n'y a pas de DRM standard, ou de technologie d'identification de signature standard et largement développée, cette Application n'appartient pas à cette catégorie.

En termes de culture informatique, une Application se rapproche des pare-feu personnels (culture protocolaire) et des antivirus (culture de sécurité et de cryptographie). En termes de présentation et de gestion informatique, une Application se rapproche du contrôle parental. Une Application sur l'ordinateur de l'internaute doit être compatible avec l'existant, et doit cohabiter avec les logiciels des suites de sécurité, c'est-à-dire les pare-feu, les antispams, le contrôle parental et les antivirus, ainsi qu'avec les fonctions de sécurité (identification et contrôle d'accès) aux systèmes et réseaux.

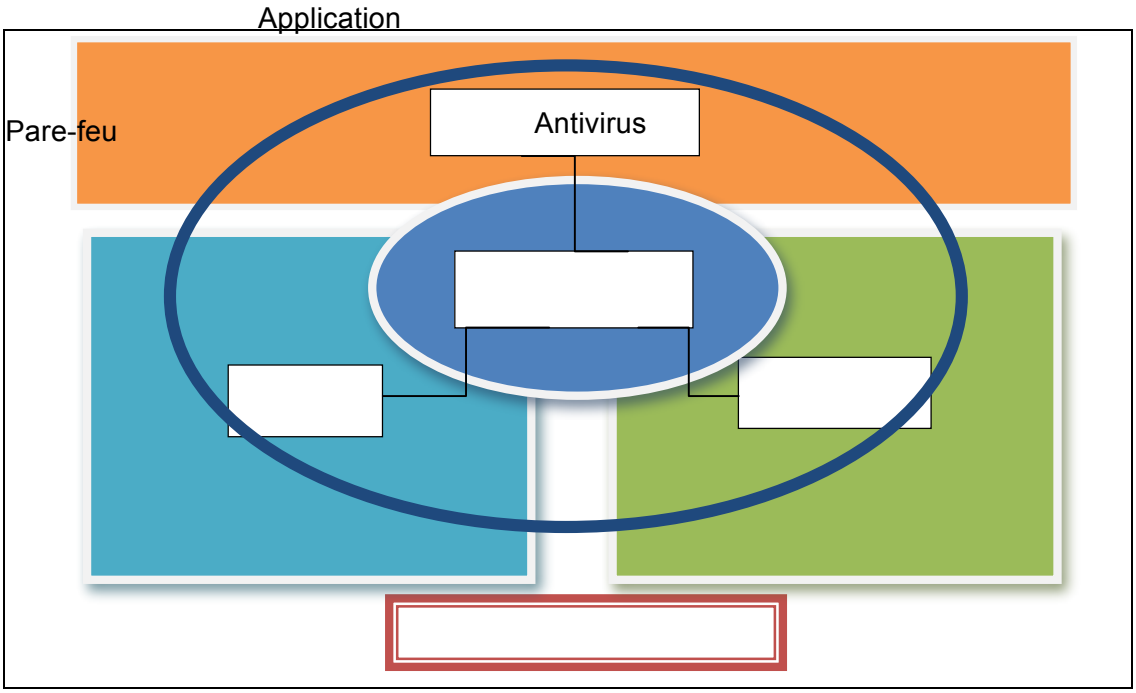

Figure 5 : Positionnement de l'Application par rapport aux fonctions du contrôle parental, du pare-feu, et de l'antivirus.

L'Application est destinée à surveiller les événements et leur contexte, à notifier, prendre ou proposer certaines actions à l'utilisateur dans les cas où un événement et/ou un contexte sont jugés comme porteurs de risque au sens de la politique de sécurité définie par l'Administrateur, et à journaliser (optionnellement) lesdits événements, contextes, notifications et actions de l'Administrateur, du titulaire et du (des) utilisateur(s).

L'Application n'examine pas le contenu des échanges, n'identifie pas le contenu en transit comme étant – ou n'étant pas – protégé par un droit d'auteur, n'enregistre pas de noms de fichier ou d'historique de navigation, et ne transmet pas de données à des tiers.

MESURES ORGANISATIONNELLES

Pour compléter l'action de l'Application conforme aux SFH, il est important que le titulaire de l'abonnement mette en place des mesures organisationnelles. Par exemple, le titulaire de l'abonnement devra informer les utilisateurs des dangers du téléchargement illégal.

SPÉCIFICATION GÉNÉRALE : COMPLÉMENT GRAND PUBLIC

CARACTERISTIQUES GENERALES

L'Application conforme aux SFH doit être :

- simple pour tous les utilisateurs pour faciliter sa diffusion rapide ;
- non-intrusive dans le fonctionnement courant et légal de l'accès aux réseaux (internet, téléphone) pour ne pas impacter la performance des systèmes de l'utilisateur ;

- engageante pour contribuer à la responsabilisation de l'utilisateur ;
- administrable par l'Administrateur, pour vérifier son bon fonctionnement et éviter son piratage.

Les moyens de sécurisation doivent être :

- simples d'accès pour tous les utilisateurs (internautes, téléphonie mobiles) pour faciliter leur diffusion rapide ;
- faciles à mettre en œuvre pour tous les utilisateurs, y compris les personnes non-techniques,
- sécurisés, administrables, pour vérifier leur bon fonctionnement et éviter leur piratage.

Lorsque c'est un produit, l'installation doit être simple pour l'Administrateur et pouvoir être faite en quelques clics pour sa composante logicielle. Il en va de même pour la désinstallation qui doit être effective à 100% (aucun « reste » informatique après désinstallation).

L'utilisation pour l'Administrateur et l'usager de l'Application sont simples : activation, désactivation, administration notamment les mises à jour, ergonomie, interface personne-machine.

Lorsque c'est un service, l'utilisation doit être simple : le titulaire peut se désabonner du service facilement (et récupérer ses données personnelles – aucun « reste » informatique après désabonnement chez le fournisseur de service).

Chaque copie de l'Application est personnalisée (par un identifiant ou un numéro de licence sécurisé) et tout ou partie de l'Application peut être installée sur chacun des ordinateurs utilisant la connexion du titulaire de l'abonnement internet, sauf en cas de mise en place de MS au niveau du boîtier ADSL / Routeur sans aucun logiciel à installer sur les terminaux.

L'Application peut être intégrée comme une extension dans une suite de sécurité (contrôle parental, antispam, antivirus, pare-feu, etc.).

L'Application ne doit pas transmettre d'informations à des tiers. L'Application conforme aux SFH n'enregistre pas d'historique de navigation (ex : désignation en clair des sites visités, noms de fichiers téléchargés[40]…). Le journal enregistre (quand il est activé) néanmoins une signature des noms de fichiers et des sites lorsque la politique de sécurité a été outrepassée par un utilisateur. On indique ces noms via une fonction de hachage de manière à masquer ces noms et respecter la sphère privée des utilisateurs.

Cadre technique

La spécification repose sur les outils suivants :

- Système d'exploitation (Windows, MacOS, Unix, Linux, Android, iOS, etc.) pour les postes terminaux, Linux ou autre pour les routeurs ou boîtiers ;

[40] On n'enregistre pas le nom des fichiers de P2P, de streaming et les URL des sites qui ont participé au téléchargement, mais on peut enregistrer ces identifiants sous forme de fonctions de hachage pour être en mesure de vérifier les actions « suspectes » autorisées par l'utilisateur.

- Serveur de temps pour l'horodatage ;

- Systèmes de protection informatique : protection architecturale, protection de logiciels (assombrissement - « *obfuscation* » - de code exécutable, insertion de code mort, compression et chiffrement de code exécutable avec déchiffrement à la volée, stéganographie), protection des données, protection de l'intégrité du système, fonctions de sécurité (identification, authentification, contrôle d'accès, protection des données, signature).

MODULE 1 : LE MODULE D'ADMINISTRATION (VERSION GRAND PUBLIC)

ERGONOMIE

L'utilisation par les usagers (internautes, téléphonie mobile) ne demande pas de connaissances techniques. L'Application est soit transparente, soit préparée de telle manière qu'aucune configuration compliquée ne soit nécessaire pour les options par défaut.

INTERFACE GRAPHIQUE

L'interface a les caractéristiques suivantes :

- Possibilité de désactiver l'Application (en quelques clics) ;

- Gestion des profils (en quelques clics).

L'Application doit fonctionner avec discrétion, afin de ne pas importuner l'utilisateur dans son activité numérique principale. L'Application est visible uniquement dans la barre des tâches, par une icône. L'interface devient visible à l'utilisateur lors des paramétrages, des affichages interactifs de notification (aussi modérés que possible) lors des détections d'une utilisation non conventionnelle demandant une validation, ou d'une information furtive au niveau de la barre des tâches (mise à jour, contrôle de validité, informations diverses, etc.).

CYCLE DE VIE DE L'APPLICATION

Installation

L'installation sera automatique pour une configuration standard. L'intervention manuelle sera minimale pour utiliser des profils.

Certains composants du logiciel peuvent être signés électroniquement.

Aucune donnée ne reste sur l'ordinateur suite à sa désinstallation.

L'installation et le paramétrage lors de la première installation doit tenir compte des configurations les plus courantes des principaux équipements du FAI de la ligne concernée.

Pendant cette installation, l'Application peut présenter à l'Administrateur les différents conseils de sécurisation connus des équipements du Fournisseur d'accès en question.

L'Administrateur doit être identifié et authentifié (par un mot de passe sophistiqué).

Mise à jour

La mise à jour de l'Application nécessite un transfert d'information (version des logiciels utilisés, réception des mises à jour).

Quand une Application demande à l'utilisateur de permettre la mise à jour et qu'il répond par l'affirmative, il est impératif d'enregistrer tous les éléments ayant amené à la question ; sinon le journal pourrait ne pas enregistrer la réalisation effective de cet événement. Les mises à jour sont automatiques, en temps réel, via le réseau, sous la responsabilité du titulaire.

Lorsque les MS, en tout ou partie, sont dans les terminaux des utilisateurs, la partie logicielle doit pouvoir être mise à jour automatiquement, via le réseau, au démarrage de l'Application et par la suite à intervalles réguliers.

Pour certaines architectures de MS, l'Application est embarquée dans les systèmes de communication (modem, routeur, boîtier ADSL, …). Dans ce cas, les prestataires autorisés effectuent les mises à jour automatiquement.

Efficacité et performances de l'application

Les MS doivent avoir un faible impact sur les performances des machines des utilisateurs sur lesquelles se fait l'exploitation.

Les processus d'analyse et de mise à jour se déroulent de manière transparente en tâches de fond, sans diminution perceptible des performances de l'ordinateur.

L'Application engendre des fichiers journaux dont le volume ne doit pas être excessif.

Une Application est légère, capable de surveiller le trafic de plusieurs connexions internet ; elle est en mesure d'atteindre les performances nécessaires à un trafic important.

MODULE 2 : LE MODULE DE TRAITEMENT (VERSION GRAND PUBLIC)

Le module de traitement relatif au contrôle est automatiquement démarré lors du démarrage du système d'exploitation du poste lorsque l'Application est installée sur l'ordinateur ou lors du démarrage de l'interface réseau lorsque l'Application est installée en dehors du poste.

Les fonctions de paramétrage du module de traitement ne sont exécutées qu'à la demande de l'Administrateur, en interactif.

LES LISTES

L'utilisateur peut modifier ces listes, si la politique de sécurité l'y autorise. Ces modifications sont journalisées. Le titulaire est alerté.

LE SOUS-MODULE D'ANALYSE STATIQUE DE CONFIGURATION

Ce sous-module a pour but d'une part la prévention d'intrusion extérieure et d'autre part la prévention d'une utilisation à risque du poste. Il prévient et guide l'utilisateur afin de proposer une meilleure configuration de protection et de sécurisation.

Le sous-module statique d'analyse de configuration a pour rôle d'analyser la configuration de l'ordinateur sur lequel est installée l'Application, d'en déduire si cette

configuration est à risque ou non pour l'utilisateur et le cas échéant de générer une notification de bas niveau et de lui proposer des solutions pour rendre la configuration de son ordinateur compatible avec un usage responsable.

Le sous-module effectue un contrôle de la structure de l'environnement informatique dans lequel l'Application s'exécute de façon à vérifier la sécurisation de la connexion : vérification du protocole cryptographique du réseau Wi-Fi (WPA2 plutôt que WPA, WPA plutôt que WEP, avec prévention de faille en cas de configuration de WEP, ou bien encore alerte sérieuse en cas de non utilisation de protocole cryptographique).

Cette analyse doit, dans la mesure du techniquement possible, prendre en considération (entre autres) :

- Les logiciels applicatifs installés sur l'ordinateur. Ces logiciels doivent être comparés avec ceux des listes (noires, blanches) des logiciels susceptibles d'entrée en interfaçage avec internet (téléchargement de fichiers, échange de données, etc.). En cas de découverte d'un logiciel suspect, une notification de bas niveau est générée au titulaire de l'abonnement. Cette analyse statique des logiciels est optionnelle. Elle peut être réalisée, au moins une fois, à l'installation de l'Application.

- La configuration réseau de l'ordinateur. L'analyse doit signaler toutes configurations réseau atypique (utilisation d'un serveur mandataire - *proxy* - douteux, connexion à un réseau Wi-Fi non sécurisé, amorce - *boot* - à partir d'un CD, etc.). En cas de découverte d'une configuration atypique, une notification de bas niveau est générée.

- La configuration du boitier ADSL/Routeur. Si l'utilisateur se connecte à internet par le biais d'un boitier ADSL ou d'un routeur (et si ceux-ci permettent une introspection), l'analyse doit vérifier que la configuration du boîtier ou du routeur ne facilite pas une éventuelle usurpation de ligne/identité sur internet (pas de sécurisation WPA, SSID en clair, routeur avec aucun contrôle sur les adresses MAC des appareils se connectant à lui, etc.). En cas de découverte d'une configuration fragile, une notification de bas niveau est générée. Excepté certains boîtiers à code ouvert, la plupart des boîtiers sont des boîtes noires opaques dont le sous-ensemble de gestion de configuration permise au détenteur du boîtier est souvent mal documenté.

Après analyse, l'Application doit conseiller et guider le titulaire dans sa sécurisation si celui-ci le souhaite (ex : choisir une clé WPA plus longue et plus aléatoire, compléter le contrôle d'accès par adresse physique), grâce à un tableau de bord de configuration de réseau, en tenant compte des architectures et des solutions possibles des divers FAI. L'Application doit aussi conseiller et guider l'usager pour les divers appareils qui ne sont pas des ordinateurs (lecteur DVD, boîtier multimédia, etc.) mais qui sont susceptibles de posséder des fonctions de téléchargement avec une problématique de contrefaçon.

L'Application peut par ailleurs demander au FAI de vérifier que les clés (WPA) du boîtier ne sont pas des clés faibles (ex : 12345) et de vérifier les adresses MAC des équipements physiques connectés. Cette fonction de diagnostic donne une bonne assurance de sécurité pour l'amélioration de la sécurisation de l'écosystème du titulaire de l'accès internet, bien que les adresses MAC soient réinscriptibles par une personne malveillante.

LE SOUS-MODULE STATISTIQUE

L'Application peut se connecter de manière sécurisée à ces points d'accès à des intervalles de temps réguliers (par exemple, toutes les 30 minutes ou toutes les heures). Ces

statistiques pourront être recueillies (éventuellement via le FAI et uniquement si le FAI le propose par ailleurs sans que ce soit une conformité avec SFH) de façon que l'Application puisse exploiter ces comptages.

Avec la connaissance de cette information, l'Application peut alerter si des flux anormaux ont transité sur le boîtier, en particulier pour les terminaux (console de jeux, etc.) où l'Application ne peut être installée.

On pourrait envisager que le FAI puisse transmettre une alerte (par mail ou par SMS) à l'abonné, si ce dernier le désire. Une telle fonctionnalité, si elle est retenue par l'abonné, devra prévoir une conservation a minima des informations. L'abonné devra avoir été clairement informé par le FAI de la politique de conservation mise en œuvre par ce dernier.

LE SOUS-MODULE D'ANALYSE DYNAMIQUE DE FLUX

Il réduit le débit, bloque, autorise ou prévient l'utilisateur selon des critères qui incluent le type de flux ou protocoles, le protocole applicatif, les listes, les caractéristiques de formats, les débits, les volumes, les profils d'utilisateurs, les plages horaires.

Selon la politique de sécurité, déterminée par le titulaire de l'accès internet, l'utilisateur détermine librement les risques et décide de la suite à poursuivre (passer outre ou arrêt) à moins que le titulaire de l'accès internet ait décidé d'arrêter la connexion.

Des algorithmes de détection performants garantissent une qualité de service auprès des utilisateurs finaux.

LE MOTEUR D'ANALYSE PROTOCOLAIRE

Le moteur de bas niveau

Le moteur de bas niveau peut être situé dans une sonde branchée sur le réseau local quand il s'agit d'une architecture à l'extérieur des postes des utilisateurs, ou bien éventuellement à l'intérieur du système d'exploitation lorsqu'il s'agit de postes terminaux des utilisateurs.

Le moteur de haut niveau

L'identification des protocoles utilisés, des logiciels en cours de fonctionnement ou des URLs utilisés, est intéressante, mais n'est pas nécessairement liée à la pile protocolaire. Les volumes des flux entrant et sortant sont des indicateurs précieux qui permettent de détecter la sémantique de la pile protocolaire réelle, en cours d'exécution.

Langage de règles

Une règle de sécurité (Conditions => Actions) se compose de :

- Une combinaison de notifications (bas et haut niveau) couplées au contexte dans lequel ces notifications ont été générées ;
- Une ou plusieurs actions qui permettent de réagir ou de corriger l'anomalie pointée du doigt par la règle ;
- Une description pédagogique permettant à tout utilisateur de comprendre l'anomalie pointée du doigt par la règle (et ce, peu importe son niveau).

Les notifications et alertes

Le but de cette notification de haut niveau est d'avertir l'utilisateur de l'anomalie, de lui proposer de modifier tel ou tel aspect du comportement de la machine ou de la configuration.

Une fois averti, l'utilisateur conserve le choix, de suivre le conseil proposé par l'analyse de haut niveau ou de l'ignorer. Dans les deux cas, le choix de l'utilisateur est inscrit dans le journal.

Les actions proposées à l'utilisateur par l'Application peuvent être de :

- bloquer certaines connexions, certaines destinations, la communication locale réseau de certains programmes, toute une plage de ports, toute une plage d'adresses IP ;
- bloquer toutes les connexions ;
- proposer des solutions de remplacement.

Cette énumération n'est pas exhaustive. Dans tous les cas, les actions doivent pouvoir être appliquées en quelques clics. L'Application doit automatiser toutes les procédures qu'elle propose à l'utilisateur.

Les actions proposées à l'utilisateur de modifier la configuration de l'ordinateur, de modifier la configuration du boîtier/routeur ou de désinstaller certains programmes, sont réalisées en dehors de l'Application.

Les notifications de haut niveau sont destinées à être vues en temps réel ou en temps légèrement différé par les utilisateurs. Elles indiquent aux utilisateurs une anomalie importante et une méthode afin de corriger cette anomalie.

L'affichage de notifications et d'alertes sont pédagogiques[41], par exemple : « Vous allez téléchargez un fichier en utilisant le protocole <nom du protocole> : voulez-vous continuer ? ».

MODULE 3 : LE MODULE DE JOURNALISATION (VERSION GRAND PUBLIC)

Ce module comporte des modalités pour exploiter les journaux.

- Le titulaire de l'accès internet peut déchiffrer les journaux chiffrés.
- Le titulaire de l'accès internet peut vérifier l'intégrité des journaux en clair.

[41] Les notifications verbeuses risquent d'être néfastes si elles sont trop répétitives. Il convient, après quelques itérations, de présenter alors des messages concis.

MODULE 4 : LE MODULE DE SÉCURITÉ (VERSION GRAND PUBLIC)

RISQUES

Hypothèses sur l'environnement

L'Administrateur dispose des moyens de contrôler la configuration matérielle et logicielle de l'Application par rapport à un état de référence, ou de la régénérer dans un état sûr.

L'assurance de sécurité est plus faible lorsque l'Application est installée en autonome sur les postes terminaux des utilisateurs.

POLITIQUE DE SECURITE

Rôles de chacun dans la politique de sécurité

Lorsque l'Application est installée sur les ordinateurs personnels qui sont reconnus par le boîtier ADSL, le titulaire de l'abonnement, Administrateur de la politique de sécurité, peut configurer la politique de sécurité selon des profils d'utilisateurs.

Dans un foyer ou dans une TPE, le rôle de l'Administrateur doit être clairement identifié, car la personne qui est le titulaire de l'accès internet n'est pas forcément une personne familière avec l'informatique.

Les utilisateurs autorisés doivent dans ce cas être fortement sensibilisés aux risques qu'ils font encourir au titulaire de l'accès internet en cas de mauvaise configuration de l'environnement informatique ou de mauvais usage de l'informatique.

Profil d'utilisateurs dans le cadre de la politique de sécurité

L'Administrateur de l'Application peut définir différents profils utilisateurs.

Ces profils peuvent être associés à un couple identifiant / mot de passe dont le niveau de sécurité doit être satisfaisant, et sont automatiquement sélectionnés lorsqu'un utilisateur ouvre une session sur l'ordinateur de l'Administrateur. Dans le cas d'une solution au niveau du boîtier ADSL / routeur, les profils concernent l'ensemble des équipements connectés. La gestion des profils, s'opérant au niveau du boîtier, on peut utiliser un système de cookies pour que le boîtier reconnaisse l'utilisateur après une première connexion d'identification.

Les caractéristiques d'un profil sont, par exemple, les suivantes :

- Plage horaire de fonctionnement pour les utilisateurs autres que l'Administrateur : en dehors de cette plage de fonctionnement les connexions internet sont automatiquement bloquées et une notification est générée. Pour l'Administrateur, en dehors de cette plage de fonctionnement, une notification est générée, mais contrairement aux utilisateurs sans droit, il lui est alors proposé de débloquer les connexions malgré tout.
- IP : pour chaque profil, il existe une liste noire d'adresses IP à notifier, une liste blanche d'adresses IP autorisées. Toutes tentatives de connexions à ces IP sur liste noire sont notifiées à l'utilisateur et la réponse de l'utilisateur est enregistrée.
- Ports : pour chaque profil, il existe une liste noire de ports. Toutes tentatives de connexions via ces ports sont notifiées à l'utilisateur et la réponse de l'utilisateur est enregistrée.

- Type de connexions : pour chaque profil, il existe une liste noire de protocoles ou de type de connexions. Toutes tentatives de connexions sont notifiées et la réponse de l'utilisateur est enregistrée.
- Logiciels : pour chaque profil, il existe une liste noire de logiciels. Les tentatives pour lancer un logiciel sont, ou bien avortées et une notification est enregistrée, ou bien une notification est signalée à l'utilisateur qui peut outrepasser l'avertissement et la réponse est enregistrée.

L'interface de gestion des profils doit être particulièrement soignée et simple, de façon que l'Administrateur puisse parvenir à configurer un ensemble de profils et ce quel que soit son niveau de connaissances en informatique.

Ce catalogue de profils, est défini selon l'âge (de type contrôle parental), selon le degré de connaissance informatique des utilisateurs (expérimenté, novice) et selon le degré de risques accepté par le responsable de l'abonnement : aucune prise de risque par filtrage de toutes les situations à risque, prise de risque maximale sans notification, et enregistrement silencieux du journal si cette fonctionnalité est activée.

Ces profils peuvent être par exemple :

- L'Application détecte les catégories protocolaires et journalise les catégories à risque, selon le contexte donné.

- L'Application détecte les catégories protocolaires, notifie l'utilisateur et/ou alerte l'Administrateur, et journalise les éléments et les événements à risque.

- L'Application détecte les catégories protocolaires, notifie l'utilisateur et alerte l'Administrateur, exécute une commande définie par l'Administrateur, qui peut réduire le débit, qui peut mettre fin à une connexion, qui peut bloquer un ordinateur hôte à la volée, bloquer les trafics correspondants, et journalise l'arrêt. Dans ce cas, l'Application se comporte, non pas passivement, mais activement comme un filtre.

FONCTIONNALITÉS COMPLÉMENTAIRES DE L'APPLICATION CONFORME AUX SFH À DESTINATION DU GRAND PUBLIC

Sont regroupées dans ce chapitre les fonctionnalités qu'une Application conforme aux Spécifications Fonctionnelles Hadopi destinée au grand public et aux TPE doit posséder en plus des fonctionnalités clés précédemment définies. Dans le cadre de l'élaboration d'une Application destinée au grand public et aux TPE et en cas de conflit avec une fonctionnalité clé listée précédemment la priorité doit être accordée aux fonctionnalités présentées ci-dessous.

Ces fonctionnalités sont regroupées en 5 catégories, les fonctionnalités générales, les fonctionnalités du module d'Administration, les fonctionnalités du module de Traitement, les fonctionnalités du module de Journalisation, les fonctionnalités du module de Sécurité.

FONCTIONNALITÉS GÉNÉRALES

- Simplicité d'utilisation

FONCTIONNALITÉS DU MODULE D'ADMINISTRATION (MODULE 1)

- Les mises à jour sont automatisées et soumises à l'acceptation de l'Administrateur

FONCTIONNALITÉS DU MODULE DE TRAITEMENT (MODULE 2)

- Le module de traitement est démarré automatiquement
- Analyse de la configuration du boitier ADSL/Routeur
- Après et en accord avec les analyses, l'Application conseille l'Administrateur sur la sécurisation de son réseau local
- Les notifications de haut niveau doivent être pédagogiques
- Les notifications de haut niveau doivent proposer à l'Utilisateur les actions (s'il en existe) pour réduire ce risque
- Les actions proposées à l'Utilisateur doivent être automatisée quand cela est techniquement possible

FONCTIONNALITÉS DU MODULE DE JOURNALISATION (MODULE 3)

- Les mises à jour sont journalisées

FONCTIONNALITÉS DU MODULE DE SÉCURITÉ (MODULE 4)

- L'Administrateur peut donner l'autorisation à un Utilisateur de modifier les listes
- L'Utilisateur peut modifier les listes s'il a l'autorisation nécessaire
- L'Administrateur peut activer/désactiver des règles de sécurité
- L'Administrateur peut contrôler la configuration matérielle et logicielle de l'Application
- L'Administrateur peut rétablir la configuration matérielle et logicielle de l'Application à un état de référence

CONTRAINTES OBLIGATOIRES DE SFH

Après avoir spécifié ce que doit réaliser l'Application, ce que peut réaliser l'Application, il est indispensable de pointer les obligations que doit respecter l'Application, en termes de conception et/ou de propriétés non fonctionnelles.

- L'Application ne doit pas fonctionner au cœur d'un réseau public ;
- L'Application est sous la responsabilité totale du titulaire de l'abonnement (pas d'activation par défaut, pas d'activité par des tiers à l'insu de l'abonné).
- L'Application ne doit pas porter atteinte à la sphère privée des utilisateurs ;
- La journalisation est optionnelle par profil d'utilisateur ; le journal s'il existe, est en clair ou bien chiffré, par profil d'utilisateur ;
- L'Application ne doit pas inspecter le contenu des fichiers téléchargés ;
- L'Application ne doit pas réaliser de DPI (*Deep Packet Inspection*) dans les réseaux publics ;
- Le traitement est optionnel (sauf l'aide à la bonne gestion de configuration du réseau local).

TABLE DES FIGURES