Consultation publique de la
Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet

Projet de spécifications fonctionnelles des moyens de sécurisation

Hadopi
Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet

Objet : Dossier de consultation publique de la Haute Autorité sur les spécifications fonctionnelles des moyens de sécurisation

Chère Madame, cher Monsieur,

La Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (« Hadopi ») soumet à consultation publique un projet de spécifications fonctionnelles pour des moyens de sécurisation destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne.

Comme suite à votre demande, vous trouverez ci-joint le projet de spécifications fonctionnelles soumis à consultation.

Ce projet a été établi par M. Riguidel, professeur émérite à Télécom ParisTech.

La présente consultation s'inscrit dans le cadre de l'article L 331-26 du code de la propriété intellectuelle (« CPI »), prévoyant qu'*« après consultation des concepteurs de moyens de sécurisation destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne, des personnes dont l'activité est d'offrir l'accès à un tel service, ainsi que des sociétés régies par le titre II du présent livre* [les sociétés de perception et de répartition des droits] *et des organismes de défense professionnelle régulièrement constitués, la Haute autorité rend publiques les spécifications fonctionnelles pertinentes que ces moyens doivent présenter* ».

Les spécifications fonctionnelles pertinentes rendues publiques par l'Hadopi permettront d'évaluer la conformité des moyens de sécurisation dans le cadre de la procédure de labellisation prévue à l'article L. 331-26 CPI.

La présente consultation publique est ouverte jusqu'au 10 septembre 2010.

Si vous souhaitez apporter votre contribution, vous devez avant cette date adresser vos observations, à l'Hadopi :

- soit par voie électronique, à l'adresse suivante : consultation-sfh@hadopi.net
- soit par voie postale, à l'adresse suivante (mentionner sur l'enveloppe :

« Réponse à la consultation publique sur les spécifications fonctionnelles ») :

Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet - Hadopi

4, rue du Texel

75014 Paris

Tout contributeur doit préciser la catégorie de personne consultée prévue à l'article L 331-26 CPI à laquelle il appartient, et en justifier par tout moyen approprié.

Dans un objectif de transparence, la Haute Autorité publiera les contributions reçues. Si vous ne désirez pas que votre contribution soit publiée, vous devez l'indiquer clairement en remarque préalable dans votre contribution.

Dans l'attente de votre retour, je vous prie de croire, Madame, Monsieur, en l'expression de mes sincères salutations.

Marie Françoise Marais

Présidente de la Haute Autorité

TABLE DES MATIERES

SYNTHESE DU PROJET DE SPECIFICATIONS FONCTIONNELLES

La synthèse des fonctionnalités pertinentes des moyens de sécurisation est la suivante :

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

Cette politique est définie en choisissant des règles et des procédures parmi un catalogue d'actions techniques possibles ; le moyen de sécurisation doit offrir une grande souplesse des fonctionnalités et une granularité d'utilisation ;

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

Élément 1 : Observation 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 définis dans le présent document, et qui incluent notamment le type de flux ou protocoles, selon le protocole applicatif, des listes[1], des caractéristiques de formats, de débits, de volumes, des profils d'utilisateurs, des plages horaires).

Élément 2 : Analyse optionnelle 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 routeur / boîtier ADSL) ; analyse dynamique des logiciels en fonctionnement, et contrôle des utilisations par le titulaire de la connexion.

Élément 3 : Affichage de notifications et d'alertes pédagogiques (ex : « Vous allez téléchargez un fichier en utilisant le protocole pair à pair « *nom du protocole* » : voulez-vous continuer ? »).

Élément 4 : Double journalisation[2] (version normale en clair et version sécurisée ; les deux versions sont identiques, sauf si la version en clair est manipulée) des événements significatifs (ex : éléments de la vie interne du moyen de sécurisation : démarrage, arrêt, activation, désactivation, modification des profils de sécurité, etc. ;

[1] *Listes* :
Les listes peuvent être

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

[2] *Journalisation* :
Les journaux sécurisés doivent être archivés et conservés par le titulaire de l'abonnement pendant la période d'une année, période où le titulaire pourrait demander à une tierce partie de confiance, un déchiffrement des journaux correspondant à des dates fixées et une copie certifiée conforme du déchiffrement de ces journaux.

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). Le journal sécurisé doit être confidentiel, authentique et infalsifiable. Le droit de lire ce journal sécurisé est restreint au titulaire de l'accès qui pourra le faire déchiffrer en faisant appel à un tiers de confiance (ex : une IGC, Infrastructure de Gestion de Clés).

Les éléments 1, 2 et 3 sont à la discrétion et dans les termes choisis par le titulaire. L'élément 4 est obligatoire et s'opère automatiquement dès lors que le moyen de sécurisation est en fonctionnement (même si les éléments 1, 2 et 3 ne sont pas activés).

Les moyens de sécurisation doivent avoir une capacité de sécurisation contre l'usurpation, le contournement ou l'altération. Les moyens de sécurisation 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.

Les moyens de sécurisation doivent inclure une possibilité de mise à jour régulière (listes, actions techniques, alertes, application).

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

L'installation et l'utilisation sont simples : activation, désactivation, administration notamment les mises à jour, ergonomie. Il en va de même pour la désinstallation qui doit être effective à 100% (aucun « reste » informatique après désinstallation).

Les moyens peuvent être réalisés à partir de logiciels libres et/ou fonctionner sur des systèmes d'exploitation libres.

Les moyens peuvent être intégrés comme une extension dans une suite de sécurité (contrôle parental, antispam, antivirus, pare-feu, etc.). Ils peuvent être un système autonome compatible avec les produits et services du marché.

Les moyens ne doivent pas transmettre d'informations à des tiers, à l'exception de la clé de déchiffrement de la version sécurisée du journal qui elle peut être transmise à un tiers de confiance lors de l'installation. Les moyens n'enregistrent pas d'historique de navigation (ex : désignation en clair des sites visités, noms de fichiers téléchargés…).

INTRODUCTION

L'HADOPI ET LES MOYENS DE SECURISATION

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 générale de protection des œuvres et objets auxquels est attaché un droit d'auteur ou un droit voisin 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 Internet de veiller à ce que son accès ne soit pas utilisé à des fins de contrefaçon (article L336-3 CPI).

Elle a pour objectif d'inciter les abonnés à installer et à mettre en œuvre des moyens de sécurisation de leur accès internet, qui feront obstacle à l'utilisation de celui-ci à des fins frauduleuses.

À cet effet, il est prévu que sur saisine des ayants droit, la commission de protection des droits de l'Hadopi peut adresser aux abonnés dont l'accès aura été utilisé pour échanger illégalement des fichiers contenant des œuvres protégées, des recommandations qui constituent un rappel à la loi. Ces recommandations :

- attirent l'attention des abonnés sur l'existence d'actes frauduleux accomplis 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 d'échange illégal de fichiers après deux recommandations dont la seconde est envoyée par courrier remis 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 dès lors que l'abonné malgré la deuxième recommandation envoyée par l'Hadopi par courrier remis contre signature, 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.

LA LABELLISATION DES MOYENS DE SECURISATION

Compte tenu de l'importance que revêtent les moyens de sécurisation, le législateur a confié à l'Hadopi une mission de labellisation desdits moyens de sécurisation.

La labellisation des moyens de sécurisation prévue à l'article L331-26 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 d'accès 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, vérifiant la conformité aux spécifications fonctionnelles rendues publiques par la Haute Autorité ainsi que leur efficacité.

OBJET DE LA PRESENTE CONSULTATION

L'objet de ce document est de proposer une première version de travail de rédaction des spécifications fonctionnelles qui seront rendues publiques par l'Hadopi en application de l'article L331-26 CPI (Spécifications Fonctionnelles Hadopi ou « SFH »).

Par spécification fonctionnelle, il est entendu une description de l'ensemble des fonctions informatiques d'un produit ou d'un service, en vue de sa réalisation. La spécification fonctionnelle est indépendante de la façon dont sera réalisé le produit ou service 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 du produit ou du service 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), environnement informatique ;
- la sécurité exigée, en termes de protection du dispositif, et en termes de respect de la vie privée des utilisateurs et de sécurité des données à caractère personnel ;
- le déploiement de l'application tout au long de son cycle de vie (installation, maintenance, évolution).

Le document décrit les exigences attendues d'un produit informatique et/ou d'un service qui pourra être proposé aux abonnés, titulaire d'un abonnement chez les FAI et/ou les opérateurs de téléphonie mobile, répondant aux spécifications SFH.

DONNEES TECHNIQUES ET ORGANISATIONNELLES PERTINENTES

ARCHITECTURE DES SOLUTIONS

Les présentes spécifications fonctionnelles n'entendent pas imposer d'architecture.

Le produit ou ce service de type informatique conforme aux SFH pourra être composé d'un ou plusieurs dispositifs matériels et/ou logiciels, dans une architecture centralisée et/ou distribuée, selon les solutions définies par les concepteurs.

TYPOLOGIE DES SOLUTIONS SELON LE NOMBRE D'UTILISATEURS

Le produit ou ce service de type informatique 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 entreprises, institutions, associations, d'une part et les particuliers, le grand public, 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.

Une approche informatique pertinente est alors de distinguer les conceptions en fonction du nombre d'utilisateurs que le titulaire du contrat a sous sa responsabilité.

Il appartient au concepteur de logiciels de définir la typologie de solution qui lui semble la plus appropriée. Les paragraphes suivants sont livrés à titre indicatif seulement et décrivent la compréhension par l'auteur de ce document des problématiques liées aux différentes typologies de sites.

SITES AVEC UN NOMBRE RESTREINT D'UTILISATEURS

Pour les particuliers ou les TPE, les moyens de sécurisation peuvent être, par exemple, des dispositifs sous la responsabilité du titulaire de l'abonnement, soit dans les boitiers ADSL, soit sur chacun des ordinateurs, soit répartis sur ces appareils informatiques.

Lorsque l'application est sous la forme de composants informatiques embarqués dans les instruments de communication (modem, routeur, boitier ADSL), l'application est alors plus simple et plus efficace. Pour le moment le parc des boitiers ADSL est très hétérogène, et les boitiers sont dimensionnés de telle manière qu'il est difficile de loger des applications supplémentaires dans ces boitiers. Pourtant, on peut réfléchir à ces solutions pour les futures générations de boitiers, dans le cadre du renouvellement général du parc.

Lorsque l'application est sous la forme de composants installés dans les ordinateurs, les téléphones portables, les consoles de jeux, ces composants peuvent comporter des logiciels (propriétaires ou libres) qui peuvent être installés sur des

systèmes d'exploitation propriétaires (de type Windows ou autres), ou bien sur des systèmes d'exploitation libres de type Unix ou Linux.

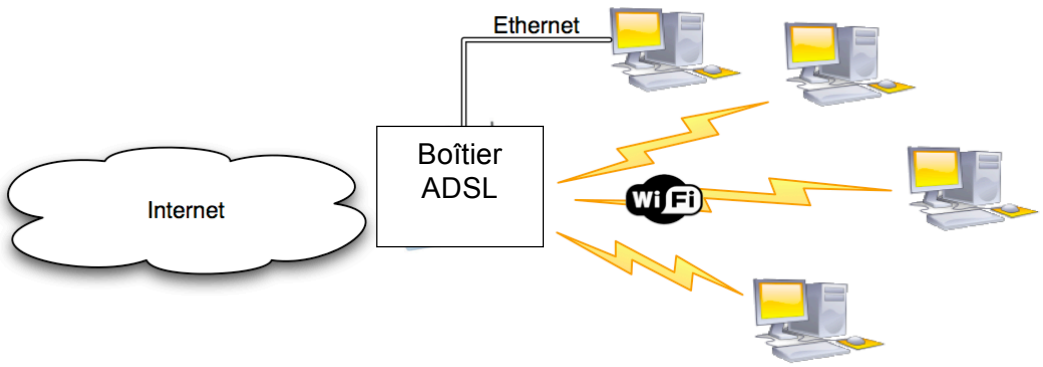

Figure 1 : Architecture informatique chez un particulier : entre internet et les ordinateurs du particulier, le boîtier de connexion (« box ») fourni par le FAI. La liaison s'effectue par Wi-Fi ou par câble Ethernet.

SITES AVEC UN NOMBRE ELEVE D'UTILISATEURS

Pour les organisations et entreprises, les moyens de sécurisation peuvent 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. Ce sont des systèmes 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 de manière passive les indicateurs des sondes branchées sur le réseau. Il 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.

Pour ces sites, les moyens de sécurisation doivent savoir gérer les serveurs qui gèrent des multiutilisateurs et des multisessions.

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

SPECIFICATIONS DES SUITES DE SECURITE EXISTANTES PERTINENTES

Le produit ou ce service de type informatique conforme aux SFH pourra emprunter aux spécifications des suites de sécurité existantes mais devra les compléter et les adapter à l'objectif de lutte contre les contrefaçons en ligne.

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 boitier 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 et un antivirus 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, nouveaux spams, 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 SOLUTIONS DE CONTROLE PARENTAL

Les produits de type « contrôle parental » permettent de restreindre le champ d'application du poste pour les utilisateurs légitimes. Un contrôle parental comporte des profils d'utilisateurs (enfants, adolescent, etc.) pour réguler son utilisation et 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 applications (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. 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.

LES ANTIVIRUS

Un antivirus détecte les virus, les vers, les logiciels espions, qui s'immiscent subrepticement parmi les applications légitimes des utilisateurs.

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 flux montant et descendant, les fichiers entrants, les courriers, etc., en temps réel ou bien analyse 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, etc.

LES PARE-FEU

Les produits de type pare-feu permettent de prévenir la prise de contrôle illégitime du poste par un tiers extérieur. Le pare-feu personnel permet de contrôler l'accès au réseau des applications installées 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.

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.).

Les pare-feu sont des logiciels qui appliquent une politique de contrôle d'accès dans toutes les couches des piles protocolaires : 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.

LES SPECIFICITES DE SFH

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

- Un pare-feu mais avec une reconnaissance plus fine des protocoles applicatifs observés.

- 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. Par ailleurs, une application SFH ne journalisera pas d'historique de navigation.

- Un antivirus car l'application devra se protéger contre les différentes attaques qui ne manqueront pas de surgir contre elle-même. Elle devra détecter des logiciels de contournement, etc.

- 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 conforme à SFH se rapproche des pare-feu et des antivirus. En termes de présentation et de gestion informatique, une application conforme à SFH se rapproche du contrôle parental. Une application conforme aux SFH sur l'ordinateur de l'internaute doit être une application compatible avec l'existant, qui cohabite avec les logiciels des suites de sécurité, c'est-à-dire les pare-feu, les antispams, le contrôle parental et les antivirus.

Les moyens de sécurisation sont compatibles avec la majorité des suites de sécurité du marché. Les moyens n'empêchent pas les logiciels légitimes du marché de fonctionner, et les moyens ne sont pas reconnus comme un « malware » par les antivirus du marché.

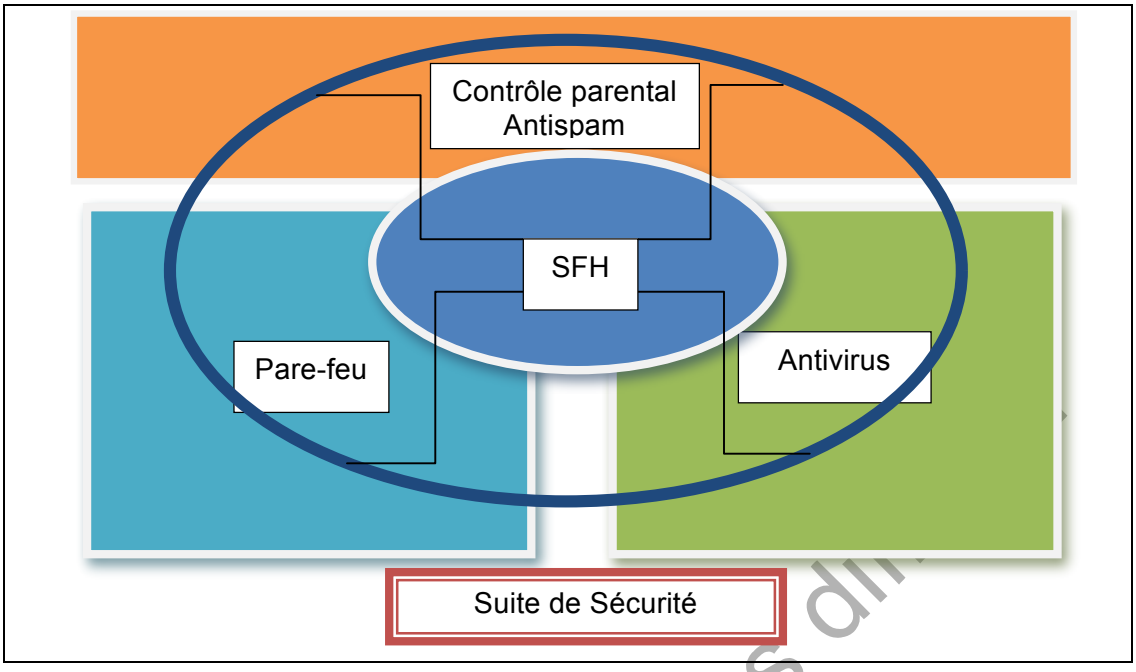

Figure 2 : Positionnement de SFH par rapport aux fonctions du contrôle parental, du pare-feu, de l'antivirus et de l'antispam.

DIRECTIVES SUIVIES POUR L'ELABORATION DE CE PROJET

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

- respect de la vie privée et responsabilisation du titulaire de l'abonnement (le moyen de sécurisation est essentiellement une « boite à outils », dans laquelle le titulaire de l'abonnement décide de tout, sous sa responsabilité). Le titulaire de l'accès reste souverain de son informatique (logiciels et données associées) à tout moment.

- exigences de sécurité ;

- possibilité de suivi infalsifiable de la politique de sécurité choisie par le titulaire de l'abonnement, ce suivi restant toujours maîtrisé par lui ; l'application conforme à SFH fournit au titulaire des arguments intrinsèques (examen de l'application dans son contexte a posteriori) ou extrinsèques (examen des journaux l'historique de l'application) pour vérifier sa politique de sécurité choisie et suivie ;

- à aucun moment le titulaire n'est dessaisi de ses enregistrements des données d'historique d'utilisation du moyen de sécurisation et il n'y a pas d'enregistrement de la navigation d'un internaute ; (ex : désignation en clair des sites visités, noms de fichiers téléchargés…) ;

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

- mise à jour régulière et obligatoire ;

- établissement d'une politique de sécurité générique, universelle, pour les particuliers et les organisations, avec possibilité de l'instancier pour les différentes cibles (particuliers, entreprises, établissements publics, associations, universités, hôpitaux, hôtels, cybercafé, etc.), et capacité d'implémenter des solutions évolutives avec le temps, de l'ajuster selon la taille de l'écosystème numérique (de 1 personne à des dizaines de milliers d'utilisateurs). Cette politique de sécurité sera adaptée, ajustée et personnalisée par le responsable 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 au contexte local des diverses situations présentées.

SPECIFICATION GENERALE

OBJECTIF

La mise en œuvre d'une application conforme à SFH 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 ;

- De disposer d'un outil conforme à des spécifications définies par l'Hadopi, dans le cas où le titulaire souhaite pouvoir faire état des dispositions qu'il a prises pour sécuriser son accès internet.

CARACTERISTIQUES GENERALES

L'installation de ce logiciel est facultative et la décision dépend du titulaire de l'abonnement. L'installation doit être simple et pouvoir être faite en quelques clics. Il en va de même pour la désinstallation qui doit être effective à 100% (aucun « reste » informatique après désinstallation).

Pour les sites avec un nombre réduit d'utilisateurs, chaque copie de l'application est personnalisée et tout ou partie de l'application doit être installée sur chacun des ordinateurs utilisant la connexion du titulaire de l'abonnement internet. La personnalisation de la copie se fera par l'insertion d'un identifiant propre (dérivé d'une clé publique) au titulaire du compte dans l'exécutable même à l'installation (par téléchargement sur le réseau ou en version préinstallée à l'achat d'un Netbook ou PC).

L'application ne doit pas pouvoir être usurpée ou remplacée. En cas de tentative d'usurpation, il doit être possible de la détecter, via la personnalisation de l'application. Dans un contexte où il y a de nombreux utilisateurs (entreprises), l'application est sécurisée par des mesures organisationnelles.

L'application ne doit pas pouvoir être contournée. En cas de tentative de contournement, le logiciel devra la détecter.

CADRE TECHNIQUE

La spécification repose sur les outils suivants :

Les réseaux publics avec leurs piles protocolaires standardisées (Ethernet, IP, TCP, UDP, HTTP, etc.) ;

Système d'exploitation (Windows, Unix, Linux, etc.) ;

Primitives cryptographiques (authentification, chiffrement, cryptographie symétrique et asymétrique, signature électronique, certificat) ;

Infrastructure de Gestion de Clés publiques (IGC), ou PKI en anglais ;

Serveur de temps pour l'horodatage ;

Système de base de données (pour l'archivage des répertoires des journaux).

INTRODUCTION DES MODULES

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

Les fonctions d'administration : installation, désinstallation, mise à jour, activation, désactivation. Le module administration comprend des fonctions techniques (interface graphique personne-machine).

Les fonctions 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).

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.

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 : par exemple, les moyens de sécurisation utilisent la sécurisation classique de la connexion, c'est-à-dire le protocole cryptographique WPA entre les ordinateurs et le boitier ADSL.

MODULE 1 : LE MODULE D'ADMINISTRATION

BUT – FONCTIONNEMENT

L'application conforme à SFH comporte un module de gestion du cycle de vie et de gestion de la configuration générale, car l'application est mise à jour en temps réel, automatiquement via le réseau.

Lorsque l'application conforme à SFH est un système autonome (dans une entreprise), il est géré par le responsable de sécurité.

Lorsque l'application conforme à SFH est destinée aux particuliers ou aux TPE, les mises à jour sont automatiques, sous la responsabilité du titulaire.

ERGONOMIE

Le dispositif (matériel et/ou logiciel) est un système facile à installer (et à désinstaller). Il est facile à activer (et à désactiver) par l'administrateur.

Le dispositif doit pouvoir être mis à jour de manière automatique.

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

Pour certaines configurations dans les entreprises, le système est transparent (rien n'est installé sur le poste des utilisateurs).

Pour certaines configurations, le système est embarqué dans les systèmes de communication (modem, routeur, boitier ADSL). Dans ce cas, les prestataires autorisés effectuent les mises à jour automatiquement.

Lorsque les configurations sont dans les terminaux des utilisateurs, le système doit pouvoir être mis à jour automatiquement, via le réseau, au démarrage de l'application et par la suite à intervalles réguliers.

INTERFACE GRAPHIQUE

L'interface graphique effectue la liaison entre l'utilisateur et l'application. Cette interface doit être aussi discrète que possible lorsque la machine a un comportement normal sur le réseau. Mais quand la machine a un comportement à risque, l'interface doit le signaler clairement à l'utilisateur. L'utilisateur doit aussi pouvoir d'un simple coup d'œil apprécier le niveau global correspondant au comportement de la machine.

Lorsque l'analyse de haut niveau aboutit à la détection d'anomalies, l'interface a les caractéristiques suivantes :

Semi invisibilité en temps normal (mais avec niveau global visible) ;

Affichage visible des notifications de haut niveau ;

Possibilité de mettre en veille l'application (en quelques clics) ;

Gestion des profils (en quelques clics pour les usagers du grand public, envoi d'un message électronique aux utilisateurs dans les entreprises).

CYCLE DE VIE DE L'APPLICATION

INSTALLATION

Il est nécessaire d'être administrateur pour installer le logiciel. Certains composants du logiciel seront signés électroniquement. L'installation sera automatique pour une configuration standard. L'intervention manuelle sera minimale pour utiliser des profils. À l'installation, un couple de clés de cryptographie asymétrique est mis en place, la clé publique pour le titulaire, une clé privée, conservée par un tiers de confiance.

FLEXIBILITE, EVOLUTIVITE DES SPECIFICATIONS

Les spécifications devront évoluer en fonction des diverses mesures qui ont été observées et prises sur le réseau : estimation du volume de téléchargement illégal, détermination des protocoles les plus utilisés pour télécharger.

MISE A JOUR

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'évolution des listes (noires, grises, blanches), l'émergence de nouveaux protocoles, de nouveaux logiciels de détournements, de nouveaux comportements vis-à-vis du téléchargement illégal.

Un certain nombre de composants de l'application doivent régulièrement être mis à jour. Ces composants sont :

Les listes noires, grises ou blanches : Il existe plusieurs sortes de listes, par exemple liste noire des sites web interdits par décision de justice, la liste grise des applications suspectes, la liste grise des mots-clés suspects, la liste blanche de l'offre légale. Ces listes peuvent être aussi relatives à des ports TCP, à d'autres entités informatiques.

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. Une fréquence de mise à jour du logiciel raisonnable est de 6 mois.

Les mises à jour sont un problème crucial. Elles doivent être sécurisées et le service de mise à jour ne doit pas pouvoir être victime d'une attaque DDoS (déni de service distribué).

CONFORMITE DE L'APPLICATION

Le logiciel doit être conforme aux spécifications et à la documentation.

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

PERFORMANCES DES APPLICATIONS

Au domicile, une application conforme à SFH permet de surveiller sur chacun des ordinateurs du foyer, les entrées et sorties à un débit de 20 Mégabits par seconde (ADSL), voire 100 Mégabits/s (fibre optique). Une application de type SFH est un logiciel léger, capable de surveiller le trafic de plusieurs connexions Internet ; il est en mesure d'atteindre les performances nécessaires à un trafic important.

MODULE 2 : LE MODULE DE TRAITEMENT

BUT – FONCTIONNEMENT

Le module de traitement comprend en fait deux sous-modules : un sous-module d'analyse dynamique de flux de réseau et un sous-module d'analyse statique de configurations.

Le module de traitement utilise plusieurs sortes de triplets de listes :

- Les listes noires : entités interdites (par exemple, la liste des sites web interdits par décision de justice) ;

- Les listes grises : entités qui peuvent présenter des risques en matière de contrefaçon et qui nécessiteront une action de l'utilisateur pour outrepasser la notification du risque ; par exemple la liste grise des applications suspectes, la liste grise de plages de ports ou d'adresses qui rentrent en jeu dans certains protocoles ou certaines applications ;

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

Les listes s'appliquent à des entités informatiques : des sites (URLs), des ports de communications, des plages d'adresses, des logiciels, etc.

Les listes noires, grises et blanches d'une entité sont disjointes. Un élément de l'ensemble (des URL, des ports, des adresses, des logiciels, 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.

Le titulaire peut modifier ces listes. Ces modifications sont journalisées.

L'utilisateur peut modifier ces listes. Ces modifications sont journalisées. Le titulaire est alerté.

LE 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 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 machine de l'utilisateur.

Ce module réalise en temps réel une analyse contextuelle et syntaxique des flux du contenu (sans analyser le contenu sémantique des fichiers, dans la mesure où ne sont pas analysés à ce jour les attributs de DRM ou les empreintes des contenus des

fichiers légaux). Il observe en temps réel et sans enregistrement les flux et protocoles qui transitent par l'accès, il 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 responsable, l'utilisateur détermine librement les risques et décide de la suite à poursuivre (passer outre ou arrêt) à moins que le responsable ait décidé d'arrêter la connexion.

Ce module a pour but d'identifier de manière précise les protocoles d'applications, 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 quel que soit le port utilisé pour garantir une identification exhaustive, y compris pour les protocoles dynamiques. Des algorithmes de détection performants garantissent une qualité de service auprès des utilisateurs finaux.

Les actions possibles s'étendent sur toute la palette des protocoles de l'Internet. Le module détecte et contrôle les protocoles répertoriés par l'éditeur du moyen de sécurisation.

Dans une organisation ou chez le particulier, ces actions, portant 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 sur lequel est installé le logiciel, de détecter toutes connexions et le cas échéant de générer une notification de bas niveau.

Le moyen de sécurisation prévoit par défaut une liste non exhaustive des connexions à surveiller.

Il y aura deux types de détection et d'analyse des connexions suspectes :

- 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.

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.

Il existe en 2010, environ 150 piles protocolaires utilisées sur Internet : par exemple HTTP/TCP/IP est un exemple de pile protocolaire applicative pour consulter

le Web, Bittorrent/TCP/IP est un exemple de pile protocolaire applicative pour télécharger des fichiers avec une méthode dite de pair à pair.

LE MODULE D'ANALYSE STATIQUE DES CONFIGURATIONS

Le module statique d'analyse des configurations 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.

Cette analyse doit prendre en considération (entre autres) :

Les logiciels installés sur l'ordinateur. Ces logiciels doivent être comparés avec ceux des listes (noires, grises) des logiciels. En cas de découverte d'une application suspecte, une notification de bas niveau est générée au titulaire de l'abonnement. Cette analyse statique des logiciels est optionnelle.

La configuration réseau de l'ordinateur. L'analyse doit signaler toutes configurations réseau atypique (utilisation d'un proxy douteux, connexion à un réseau Wi-Fi non sécurisé, 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 boitier 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.

Après analyse, l'application conforme à SFH doit conseiller et guider le titulaire dans sa sécurisation (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, Boitier multimédia, etc.) mais qui sont susceptibles de posséder des fonctions de téléchargement avec une problématique de contrefaçon.

LE MOTEUR D'ANALYSE PROTOCOLAIRE

Une application conforme à SFH 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 selon le degré d'âge ou de maturité informatique des utilisateurs autorise une flexibilité dans le paramétrage des

politiques de sécurité : gestion selon des quotas en volume, en durée, selon des plages horaires, etc.

DECOUPAGE EN DEUX NIVEAUX

Une application conforme à SFH 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 application, présentation, session, transport, réseau des couches OSI, dans un poste terminal (ordinateur ouvert, et plus tard dans une version ultérieure, téléphone mobile). La SFH n'examine pas le contenu applicatif des échanges.

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 applications seraient problématiques ou suspectes.

L'application opère en deux temps :

LE MOTEUR DE BAS NIVEAU

Dans un premier temps un moteur de bas niveau, à l'intérieur de l'OS, 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 URLs à des URLs 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. L'identification des protocoles utilisés, des applications 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. 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 de la solution, mises à jour au fil du temps.

LANGAGE DE REGLES

Une règle de sécurité 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 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).

Ces règles doivent être écrites dans une norme commune à tous les fournisseurs des applications. Le format de ces règles reste encore à définir. Le langage est aussi à définir.

LA NATURE DES REGLES

Les moyens de sécurisation préviennent l'utilisateur que les modes et les outils de communication utilisés (les URLs, les piles protocolaires, les ports, les adresses, etc.) sont potentiellement à risque.

Pour les règles, il existe des indices de situation courante, de conduite ordinaire, et des indices de situation remarquable, spécifiques de conduites à risque ou anormale. 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 conduites à risque, (décrites en termes d'événements et de signatures) et d'anomalies (VPN chiffré vers des sites problématiques, présence de connexions de l'utilisateur vers certains services, tentatives de connexions infructueuses, etc.).

LES NOTIFICATIONS ET 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 conforme.

- Les notifications de haut niveau sont générées par l'analyseur haut niveau de l'application conforme. Elles sont destinées à être vues

en temps réel par les utilisateurs. Elles indiquent aux utilisateurs une anomalie importante et un moyen de corriger cette anomalie.

Chaque notification dans son contexte doit être inscrite dans le journal.

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.

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 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 conforme à SFH peuvent être de :

- bloquer certaines connexions, la communication 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 conforme doit automatiser toutes les procédures qu'il 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 conforme à SFH.

FLEXIBILITE ET MISE A JOUR DES REGLES DU MOTEUR DE HAUT NIVEAU

L'application conforme utilise pour décrire ces règles un langage particulier (on prendra un langage standard) qui permet au logiciel d'être flexible (pour sa 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

Le but de ce module est de produire des journaux d'événements qui retracent sur une période d'environ une année, l'historique de l'activité des différents utilisateurs de la ligne Internet.

La journalisation consiste en la sauvegarde, chez le titulaire de l'abonnement (sur chacun des postes, par exemple) de toute l'activité réseau notable, des notifications générées et des choix de réponse aux notifications de l'utilisateur dans un journal.

Les événements seront enregistrés selon le format suivant :

Date et Heure : 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 Bittorrent lancée

Jeudi 20 Mai 2010 20 : 32 : 10 : Notification recherche avec mots-clés interdits lancée

Le premier exemple indique qu'une notification de haut niveau concernant la connexion à un protocole sur liste grise 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 recherche contenant les mots-clés interdits 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 du logiciel : Lorsque l'administrateur décide d'arrêter l'application conforme à SFH, 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 conforme SFH (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 conforme à SFH. 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 du logiciel : L'administrateur peut temporairement désactiver l'application conforme à SFH, 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>).

SECURITE DES JOURNAUX ENGENDRES

Une application conforme à SFH engendre des journaux détaillés, qui sauvegardent 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.

La sécurité de l'application conforme repose donc essentiellement sur l'existence et l'intégrité de ce journal pour la date incriminée. La fiabilité des journaux repose sur leur résistance à la falsification, qui doit être au moins égale à la résistance du logiciel à son propre contournement.

Un journal (on parle de logs ou de traces, en informatique) pour chaque ordinateur est engendré selon un format standard (heure GMT, on utilise les standards de logs), éventuellement en utilisant le système de gestion de l'OS.

Il existe deux sortes de journaux qui sont produits en temps réel dans deux bases de données distinctes :

Un journal en clair que les utilisateurs et l'administrateur peuvent consulter.

Un journal sécurisé. Ce journal est confidentiel, authentique et infalsifiable. Toute tentative de falsification éventuelle est détectable. Pour des raisons de sécurité, cette seconde version du journal est en mode binaire, compressée, signée électroniquement, chiffrée, et archivée pendant une période d'au moins une année. Ce journal sera accessible en clair à la demande du titulaire de l'abonnement. Il permettra de vérifier, après déchiffrement avec la clé privée correspondant au logiciel, laquelle est détenue par le tiers de confiance, la mise en œuvre du logiciel de sécurisation à une date et heure donnée, et l'activité informatique de l'internaute concerné. Ce journal permet de refléter, sans interférence possible du titulaire de l'abonnement, les événements de l'accès Internet considéré.

Exemple de Journal engendré	Signification des étapes
Jeudi Mai 20 12 : 30 : 48 2010 : Mise en marche du logiciel <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 <2>	
Jeudi Mai 20 12 : 30 : 50 2010 : Rapport (Signale programme sur liste grise : aMule) <5> Jeudi Mai 20 12 : 30 : 50 2010 : Notification programme sur liste grise aMule lancée <5> Jeudi Mai 20 12 : 30 : 50 2010 : Rapport (Signale programme sur liste grise : eMule) <5> Jeudi Mai 20 12 : 30 : 50 2010 : Notification programme sur liste grise eMule lancée <5> Jeudi Mai 20 12 : 30 : 52 2010 : Continue malgré Notification : programme sur liste grise : eMule <6> Jeudi Mai 20 12 : 30 : 53 2010 : Continue malgré Notification : programme sur liste grise : aMule <6>	Détection des programmes sur Liste grise
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 grise) <5> Jeudi Mai 20 13 : 29 : 28 2010 : Notification site sur liste grise lancée <5> Jeudi Mai 20 13 : 29 : 28 2010 : Rapport (Signale site sur liste grise) <5> Jeudi Mai 20 13 : 29 : 29 2010 : Rapport (Signale site sur liste grise) <5> Jeudi Mai 20 13 : 29 : 30 2010 : Rapport (Signale site sur liste grise) <5>	Sites sur Liste grise
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 du logiciel <3> Jeudi Mai 20 18 : 41 : 28 2010 : Réactivation du logiciel <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 du logiciel <1>	

Figure 3 : Exemple de Journal

MODULE 4 : LE MODULE DE SECURITE

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 des politiques de sécurité par utilisateur ou par groupe d'utilisateurs.

Il a premièrement pour finalité de sécuriser la ligne qui relie le poste de l'internaute à Internet et de protéger l'application et les résultats de cette application. L'application doit être disponible (éviter les menaces de dénis 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 (limites de 15 minutes de streaming), par des volumes de flux (entrant ou sortant) des ordinateurs ou de la ligne.

OBJECTIFS DE SECURITE

L'application doit viser les objectifs de sécurité suivants :

INTEGRITE DU CONTEXTE DU POSTE ET DE LA LIGNE RESEAU QUI RELIE L'ORDINATEUR A INTERNET.

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

Il faut, pour atteindre cet objectif, utiliser des fonctions d'identification et d'authentification pour identifier les sujets (login, logiciel en exécution, etc.) et les objets en situation (matériel, logiciel, données). Il faut mettre en œuvre plusieurs fonctions de sécurité, notamment l'identification de l'application conforme à SFH qui fonctionne dans un environnement identifié. Précisément, il ne faut pas prendre trop de paramètres pour identifier le lieu, sinon les modifications de l'identification seront trop fréquentes. 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.

INTEGRITE ET DISPONIBILITE DE L'APPLICATION

« Le logiciel fonctionne correctement, il n'est pas contourné, ni détourné ».

On peut atteindre cet objectif notamment en identifiant chaque logiciel installé par un certificat numérique fourni par une IGC (Infrastructure de gestion de clés). Un certificat (nom du logiciel avec sa version et sa date, couplé à une clé publique) est distribué avec le logiciel.

La clé publique permet de vérifier la signature électronique du contenu exécutable du logiciel. La clé publique est aussi utilisée pour chiffrer les journaux.

La clé privée, conservée par le tiers de confiance, permettra de déchiffrer les journaux engendrés par ce logiciel. Le tiers, digne de confiance, ne peut pas créer de leurres de 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 par les utilisateurs, au moyen de « proxys » anonymes ou autres accès intermédiaires sophistiqués.

Les moyens de sécurisation ne doivent pas affaiblir le niveau de sécurité des systèmes d'exploitation, si une partie de l'application conforme à SFH est construite dans le noyau des systèmes d'exploitation.

Les mises à jour de l'application sont sécurisées, en particulier la mise à jour des règles.

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

CONFIDENTIALITE, AUTHENTICITE ET INTEGRITE DES JOURNAUX AVEC HORODATAGE DES EVENEMENTS

« Ces journaux sont confidentiels, authentiques, intègres, ont été engendrés par le logiciel donné, et les événements se sont passés à cette date-là ».

Il sera utilisé un ensemble de primitives cryptographiques afin de garantir la confidentialité, l'authenticité, l'intégrité et la justesse des journaux, et leur disponibilité lorsqu'un utilisateur les demandera, et de garantir la conformité et la disponibilité de l'application qui aura engendré ces journaux.

Les journaux sont intègres, signés électroniquement, enregistrent la chronologie des événements avec des dates et heures dignes de confiance (horodatage 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 les journaux engendrés associés). La datation des traces s'opère à partir d'une date et heure récupérée sur un serveur NTP (*Network Time Protocol*). Le serveur est 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 SSH.

Le chiffrement des journaux s'opère avec de la cryptographie asymétrique, en utilisant la clé publique fournie, avec le logiciel, par un tiers de confiance. Afin de renforcer le respect de l'intimité numérique du titulaire de l'abonnement, une application conforme à SFH peut fournir au titulaire une fonction cryptographique complémentaire afin qu'il gère lui-même la confidentialité de ses journaux (chiffrement double pour déchiffrement nécessitant à la fois l'intervention du tiers de confiance et du titulaire).

Il faudra prévoir une application automatique supplémentaire (à proposer par les fournisseurs de solutions de moyens conformes à SFH) à disposition des titulaires afin de récupérer des journaux en clair, certifiés conforme, déchiffrés à partir des secrets correspondant à l'application qui les a engendrés, afin de pouvoir les lire et les étudier.

RISQUES

L'application SFH doit être protégée notamment contre les risques suivants :

- L'application ne fonctionne pas correctement et les journaux ne sont pas écrits et archivés de manière régulière.

- 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, exploite une défaillance du système. L'environnement informatique n'est pas sécurisé : par exemple le lien de réseau sans fil entre les ordinateurs du domicile et le boitier ADSL est vulnérable à une intrusion ou bien un pirate s'est glissé dans la communication autorisée du titulaire, en brisant la sécurité WEP du Wi-Fi.

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

- L'application est contournée ou détournée de son fonctionnement normal par un utilisateur.

- Un utilisateur fabrique des leurres de journaux.

- Une personne détruit des journaux ou fabrique des leurres de journaux, à l'insu du titulaire.

- Déni de service sur les serveurs de mise à jour et les serveurs de temps.

L'application conforme à SFH doit contrecarrer ces menaces, 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 l'application de la politique de sécurité, lesquels témoignent de la situation informatique *hic et nunc*.

POLITIQUE DE SECURITE

POLITIQUE DE SECURITE DISCRETIONNAIRE

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

La politique de sécurité de SFH est une politique de sécurité discrétionnaire, c'est-à-dire non obligatoire. Même installé, le titulaire de l'abonnement peut désactiver le système quand bon lui semble. Toutefois, le journal enregistrera le fait que le logiciel a été désactivé.

L'application doit être sécurisée et digne de confiance : elle doit fonctionner correctement (intégrité et disponibilité). Le responsable (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.

Le logiciel 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 doit produire des journaux d'événements. L'application et les journaux associés sont liés de manière sécurisée.

Ces journaux ont deux présentations :

- L'une en clair que pourra consulter le titulaire de l'abonnement et l'utilisateur.

- L'autre présentation sera en binaire, compressée, signée, chiffrée et archivée dans une base de données locale. Ces journaux seront confidentiels, authentiques, intègres, infalsifiables, liés de manière sécurisée à l'environnement sur lesquels ils ont été engendrés. Les événements enregistrés, seront datés selon une heure juste.

ROLES DE CHACUN DANS LA POLITIQUE DE SECURITE

Il existe deux rôles principaux :

- L'administrateur : c'est la personne qui a accès aux fonctionnalités d'administration du produit ou du service. Il représente le titulaire de l'abonnement auprès du FAI. C'est le responsable de la politique de la sécurité ou la personne à qui le titulaire de l'abonnement a délégué la responsabilité.

- 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. Ce sont les employés d'une entreprise ou d'une institution, les clients d'un hôtel ou d'un cybercafé, qui ont demandé un accès à internet. Ces personnes ont signé une charte pour l'utilisation d'Internet. Ce sont les proches ou les membres de la famille du titulaire qui utilisent son accès Internet, sous sa responsabilité.

Il existe un autre rôle dédié à tiers de confiance :

- La tierce partie de confiance (ou son représentant) : c'est la personne qui peut, grâce à un secret identifiant le moyen de sécurisation du titulaire de l'abonnement dans son environnement informatique et les journaux correspondants, sur demande de l'administrateur, déchiffrer le journal dans sa présentation sécurisée pour les intervalles de dates et de temps demandés par le titulaire de l'accès pour obtenir une copie conforme au journal sécurisé.

Le titulaire de l'abonnement est administrateur de la sécurité. Il peut déléguer ce rôle à une personne de confiance.

L'administrateur peut être alerté par courriel, des divers avertissements de tous les postes sous sa responsabilité. Dans ce cas, ces courriels seront sécurisés pour esquiver des pourriels intempestifs, par exemple, en utilisant une cryptographie de groupe pour les postes sous la responsabilité du titulaire.

Une fois installé 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.

PROFIL D'UTILISATEURS DANS LE CADRE DE LA POLITIQUE DE SECURITE

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

Pour les administrateurs confirmés, le programme 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.

L'administrateur du système (le titulaire de compte) peut définir différents profils utilisateurs. Ces profils sont 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.

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

1. 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.

2. IP : pour chaque profil, il existe une liste noire d'adresses IP interdites, une liste grise d'adresses IP à notifier, une liste blanche d'adresses IP autorisées. Toutes tentatives de connexions à ces IP sur liste noire sont bloquées et une notification est générée. Toutes tentatives de connexions à ces IP sur liste grise sont notifiées à l'utilisateur et la réponse de l'utilisateur est enregistrée.

3. Ports : pour chaque profil, il existe une liste grise de ports. Toutes tentatives de connexions via ces ports sont notifiées à l'utilisateur et la réponse de l'utilisateur est enregistrée.

4. Type de connexions : pour chaque profil, il existe une liste grise de protocoles ou de type de connexions (streaming, P2P, etc.). Toutes tentatives de connexions sont notifiées et la réponse de l'utilisateur est enregistrée.

5. Applications : pour chaque profil, il existe une liste grise d'applications. Les tentatives pour lancer une application 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 arriver à configurer un ensemble de profils et ce quel que soit son niveau de connaissances en informatique.

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

Ces profils peuvent être par exemple :

- Le logiciel détecte les catégories protocolaires et journalise les catégories incriminées, selon le contexte donné.

- Le logiciel détecte les catégories protocolaires, notifie l'utilisateur et/ou alerte l'administrateur, et journalise les éléments et les événements incriminés.

- Le logiciel détecte les catégories protocolaires, notifie l'utilisateur et alerte l'administrateur, exécute une commande définie par l'administrateur, 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, le logiciel se comporte, non pas passivement, mais activement comme un filtre.

TABLE DES FIGURES