CONCOURS
TECHNICIEN TERRITORIAL

INTERNE & 3ème VOIE

SESSION 2016

EPREUVE DE RAPPORT

ÉPREUVE D'ADMISSIBILITE :

Rapport technique rédigé à l'aide des éléments contenus dans un dossier portant sur la spécialité au titre de laquelle le candidat concourt.

Durée : 3 heures
Coefficient : 1

SPECIALITE : INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni votre numéro de convocation, ni signature ou paraphe.
- Aucune référence (nom de collectivité, nom de personne, …) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.
- Seul l'usage d'un stylo à encre soit noire, soit bleue est autorisé (bille non effaçable, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou pour souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le Jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 26 pages

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué
S'il est incomplet, en avertir le surveillant

Vous êtes technicien territorial au sein du service informatique de la ville de Techniville (75 000 habitants).

Les systèmes de filtrage ne permettaient plus de répondre aux exigences de consultation des agents. Les fonctions de filtrage ont donc été désactivées il y a deux ans, et ne subsistent que celles de journalisation (traces).

Le Directeur des Systèmes d'Information, vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur la mise en œuvre d'un système de filtrage.

Liste des documents :

DOCUMENT N°01 **« La mairie de Compiègne optimise son accès Internet pour l'ensemble des services municipaux et le grand public avec les appliances Blue coat »**
www.globalsecuritymag.fr – Marc Jacob / 18/11/2010. (2 pages)

DOCUMENT N°02 **« Accès des agents à Internet : quelle responsabilité pour la collectivité »**
Internet.mairie / N°214 - 25/06/2009. (2 pages)

DOCUMENT N°03 **« Analyse d'un ransomware »**
www.lexsi.com – Anthony Barjon / 02/03/ 2015. (3 pages)

DOCUMENT N°04 **« Premier espace public équipé en WiFi. »**
lamontagne.fr / 23/01/2012. (1 page)

DOCUMENT N°05 **« Filtrage et internet au bureau : enjeux et cadre juridique en France »** (Extrait).
www.olfeo.com – Livre blanc juridique Olfeo co-écrit avec le Cabinet d'avocats Alain Bensoussan / 13/06/2014. (10 pages)

DOCUMENT N°06 **« Le Conseil Général du Cantal utilise Websense pour se protéger contre les menaces informatiques sur Internet »**
community.websense.com - Jean-Philippe Lavigne / 19/01/2011. (2 pages)

DOCUMENT N°07 **« Mairie de Mérignac réduit ses coûts de connexion internet grâce à la solution de filtrage d'Olféo »**
www.olfeo.com / 06/09/2012. (2 pages)

DOCUMENT N°08 **« Sept criteres pour l'evaluation de la securite Web et de la messagerie en mode Saas »**
www.itrnews.com - Florent Fortuné (websence.com) / 28/12/2010. (2 pages)

DOCUMENT N°01

La Mairie de Compiègne optimise son accès Internet pour l'ensemble des services municipaux et le grand public avec les appliances Blue coat

www.globalsecuritymag.fr – Marc Jacob / 18/11/2010.

Blue Coat Systems Inc. annonce que la Mairie de Compiègne a déployé ses appliances Blue Coat® ProxySG® sur l'ensemble des 40 sites de la municipalité pour l'optimisation et le filtrage de son accès Internet Grand Public et professionnel.

Grâce à l'appliance ProxySG 510-10 de Blue Coat, la Mairie est en mesure de gérer de façon granulaire la charge de son accès Internet et dispose désormais d'un filtrage Web performant et surtout personnalisable.

Des montées en charge inévitables

Initialement, la Mairie de Compiègne disposait d'un simple firewall doté d'une petite brique de filtrage. Cette solution économique a malheureusement rapidement montrée ses limites car elle n'offrait pas de possibilité d'affinage du filtrage suffisamment granulaire. En d'autre terme, soit tout les utilisateurs avaient accès soit aucuns ne l'avaient. Ce qui, dans le contexte d'une municipalité proposant en même temps un accès au grand public et aux employés municipaux, était un véritable casse tête informatique.

Pour des raisons légales évidentes et pour exercer un meilleur contrôle sur son trafic web la municipalité a souhaitée s'équiper d'une nouvelle solution plus flexible et plus performante pour gérer ses différents flux Internet.

Autre problématique cruciale pour la Mairie, l'accélération de l'accès web pour l'ensemble de ses sites, 40 au total, et les différentes populations utilisatrices (services municipaux et Grand public)

A l'issue d'un appel d'offre auprès des principaux acteurs du secteur, la municipalité s'est tournée vers Blue Coat. L'évolutivité de son offre, les capacités de Proxy cache et la possibilité de supprimer les serveurs distants au profit de boitier d'accélération ont largement contribués à cette décision.

Protéger et Optimiser

A travers les appliances ProxySG de Blue Coat, la Mairie de Compiègne est désormais en mesure de répondre à une problématique récurrente des collectivités locales : Faire cohabiter au niveau informatique et dans un même périmètre, deux types de populations aux objectifs et aux comportements différents. D'abord le grand public qui doit pouvoir disposer d'un accès Internet performant lui permettant d'effectuer certaines démarches administratives ou sociales et ensuite, le personnel de la Mairie, soit environ 500 personnes, qui doivent utiliser le réseau et internet pour des raisons et avec une exigence de performances professionnelles.

La Mairie de Compiègne a mis en œuvre les appliances Blue Coat ProxySG afin de pouvoir définir et appliquer une politique de filtrage web à la fois performante et souple. Elles lui permettent de suivre en temps réel mais également d'anticiper les différentes montées en charge ainsi que le respect par les différentes populations utilisatrice des règles de sécurité sur l'ensemble de ses sites.

Saturation de l'accès Internet

L'appliance ProxySG 510-10 de Blue Coat a permis d'accélérer l'accès Internet grâce au cache mais également simplifiée sa gestion. En effet la solution Blue Coat se connecte à l'active directory du réseau de la Mairie de Compiègne facilitant ainsi l'administration ou la configuration du filtrage Web et le reporting.

Le calendrier du projet s'est décliné en différentes phases avant l'implémentation finale.

Tout d'abord en octobre 2009, Miel, intégrateur partenaire de Blue Coat, s'est chargé de la mise en place de la solution pour une phase de test d'une quinzaine de jours auprès d'une sélection de 10 personnes. Cette première étape a permis d'affiner les différentes catégories de filtrage mais également d'évaluer les capacités de caching de la solution Blue Coat à travers l'envoie de fichier Test d'une dizaine de méga.

Le résultat a été sans commune mesure avec la solution précédente. Que se soit un fichier de 10 mega ou même une vidéo, l'envoi était quasiment instantané.

Bien sûr le retour utilisateur a été rapide et très bon. L'implémentation finale s'est déroulée en une journée, suivie d'une session de formation de la même durée auprès de 3 utilisateurs du service informatique qui ont par la suite défini l'ensemble de la politique de filtrage de la Mairie de Compiègne.

Sylvain Manabre, Directeur des systèmes d'information de la Mairie de Compiègne, déclare à cette occasion : « Nous avons vraiment été très satisfait de la relation avec les équipes de Blue Coat. Leur solution a dépassée nos attentes en répond parfaitement à l'ensemble de nos problématiques. Nous envisageons d'ailleurs d'étendre la solution avec des boitiers d'accélération de flux et de compression en plus du cache afin de pouvoir, à terme, supprimer nos serveurs distants et accélérer la partie applicative de notre réseau »

DOCUMENT N°02

« Accès des agents à Internet : quelle responsabilité pour la collectivité »

Internet.mairie / N°214 - 25/06/2009.

RENDEZ-VOUS

NOUVELLES TECHNOLOGIES ET CONCERTATION

L'association "Décider ensemble" organise ses troisièmes rencontres, sur le thème des nouvelles technologies au service de la concertation. Au programme : TIC et formes participatives de la démocratie, dispositifs et méthodes pour une nouvelle gouvernance... Assemblée nationale, 1er juillet.
www.deciderensemble.com

LES TIC AU SERVICE DE LA SANTÉ

Systèmes d'information hospitaliers, télémédecine, maintien à domicile sont parmi les thèmes abordés par la *mêlée e-santé*, le 2 juillet à Castres (Tarn). Salon organisé par Castres-Mazamet Technopole et l'association La Mêlée numérique.
www.melee-esante.com

LES ÉTÉS TIC DE BRETAGNE

Du 1er au 3 juillet, les étés Tic de Bretagne auront pour thème : culture(s) et connaissances en réseau. Proposés par la région Bretagne et plusieurs partenaires (Rennes Métropole, ville et université de Rennes, Mégalis...), ils réuniront associations, collectivités, entreprises, étudiants... Deux rencontres distinctes concerneront les territoires et l'éducation, et 25 tables rondes se dérouleront en parallèle : bibliothèques 2.0, livre numérique... Le 1er juillet, le carrefour des possibles présentera dix projets d'usages innovants.
www.lesetestic.com

LIBERTÉS

UNE SOCIÉTÉ DE TRANSPORTS DOIT PROPOSER DES CARTES ANONYMES

La Cnil a adressé un avertissement à la société de transports urbains rennais. Elle ne proposait pas de façon équitable le passe nominatif et le passe anonyme. La société fournissait à peine d'information sur ce dernier, qui coûtait en outre entre 2,5 et 4 fois plus cher que le passe contenant des données personnelles. C'est pourquoi seulement 53 cartes anonymes avaient été distribuées contre... 186 650 cartes nominatives. Le respect de la vie privée nécessite de pouvoir choisir dans des conditions équivalentes.
www.cnil.fr

DROIT

Accès des agents à internet : quelle responsabilité pour la collectivité ?

Il est impossible d'interdire aux agents une utilisation non professionnelle d'internet, de façon générale et absolue, mais l'accès peut être restreint. En ne filtrant pas cet accès, la collectivité risque d'engager sa responsabilité civile, voire pénale.

Comme une entreprise privée, l'employeur public peut engager sa responsabilité, civile et pénale, liée à l'utilisation des outils informatiques. Pour limiter ces risques, la collectivité doit notamment installer des outils de filtrage d'accès à internet. Objectif : ne pas autoriser le surf sur des sites illicites (racistes, pédophiles, pornographiques...). **Les inconvénients ne sont pas uniquement juridiques.** ◗ En effet, lorsque les agents abusent d'internet pour des motifs personnels, ils mettent aussi en péril la sécurité du réseau — les sites pornographiques, par exemple, contiennent souvent des virus et des logiciels espions *malwares*. ◗ En utilisant trop de bande passante, s'ils téléchargent abusivement des films, ils saturent le réseau interne. ◗ La collectivité peut craindre, également, la fuite d'informations confidentielles ou sensibles lorsque les employés participent, sans contrôle, à des forums, à des *chats* ou à des réseaux dits sociaux (*Facebook*, réseaux professionnels...). ◗ Sans parler de la chute de productivité : en 2008, les internautes ont passé en moyenne, chaque jour, plus d'une heure sur internet pour leur utilisation personnelle tandis que 39% d'entre eux y ont passé 3h15 (étude Olfeo) ! **Le temps perdu équivaudrait à une perte de productivité de 15,7% par an, soit six semaines de congé...**

DE NOMBREUX TEXTES JURIDIQUES PEUVENT S'APPLIQUER

Que ce soit parce que la loi l'impose ou par principe de précaution, il semble qu'une collectivité a tout intérêt à adopter des procédés de filtrage pour empêcher l'accès à des sites dont le contenu, les produits ou les services sont illicites. "*Il existe, en effet, plusieurs dispositions légales qui imposent à l'employeur de prendre des mesures pour empêcher les accès illicites au sein de son établissement*, précise Éric Barbry[1], directeur du pôle Droit du numérique au cabinet d'avocats Alain Bensoussan. *Il paraît donc essentiel pour lui de vérifier les conditions d'utilisation de ses outils*." **Il n'existe pas de texte de principe sur le filtrage, ni de définition.** Toutefois, certains textes reconnaissent expressément le droit d'opérer un filtrage : circulaire du 18 février 2004 sur l'usage d'internet dans le cadre pédagogique et la protection des mineurs, rapport de la Cnil[2] sur la cybersurveillance sur les lieux de travail... D'autres textes, sans prononcer le terme de filtrage, prévoient la mise en œuvre de moyens techniques visant à restreindre ou à contrôler l'accès à des sites internet : loi pour la confiance dans l'économie numérique du 21 juin 2004 (article 6-I.-1°), code de la propriété intellectuelle (article L.335-12), projet de loi Hadopi, droit communautaire. ◗ Parallèlement, le code des postes et communications électroniques (articles 34-1 et R. 10-12 et suivants) reconnaît la possibilité de vérifier les traces (logs) d'accès à internet. La Cour de Cassation a également établi que **les connexions d'un salarié, avec les ordinateurs fournis par son employeur pour exécuter son travail, sont présumées professionnelles** ; et qu'il peut, à ce titre, rechercher ces données de connexion sur son ordinateur en l'absence du salarié.

LA COLLECTIVITÉ PEUT LÉGALEMENT INTERDIRE AUX AGENTS DE TÉLÉCHARGER DES LOGICIELS

Selon la Cnil, s'il est impossible d'interdire l'utilisation non professionnelle d'internet de manière générale et absolue, **rien n'empêche de limiter cet**

accès (sites révisionnistes, pornographiques...), **sans pour autant porter atteinte à la vie privée du salarié.** Interdire aux agents de télécharger des logiciels, de se connecter à des chats ou d'accéder à une messagerie personnelle pourrait aussi se justifier, pour des motifs de sécurité — **à condition de les en avertir.** Il faut alors consulter le comité technique paritaire, déclarer à la Cnil les dispositifs de filtrage qui permettent un contrôle individuel, et respecter les principes liés à la protection des données personnelles.

La collectivité peut engager sa responsabilité civile

En ne filtrant pas les accès à internet, l'employeur engage sa responsabilité et il risque de ne pas pouvoir se séparer d'un agent qui utilise abusivement internet. Sur le plan civil, tout d'abord, la collectivité peut être tenue responsable d'un usage illicite d'internet commis par un de ses agents (article 1384, alinéa 5 du code civil). La jurisprudence précise que **la responsabilité est toutefois limitée, si l'employé a agi hors du cadre de ses fonctions, sans autorisation et en dehors de ses attributions.** En 2006, la cour d'appel d'Aix-en-Provence a considéré qu'un employé de Lucent Technologies, qui devait utiliser quotidiennement un ordinateur et internet, avait agi dans le cadre de ses fonctions ; qu'il avait l'autorisation de son employeur, car une note de service permettait au personnel de consulter des sites autres que ceux présentant un intérêt en relation directe avec leur activité ; qu'il n'avait pas agi à des fins étrangères à ses attributions, puisque cette note autorisait l'accès à internet, y compris en dehors des heures de travail.

L'employeur n'est pas pénalement responsable des salariés

En matière pénale, si l'employeur n'est pas, en principe, responsable des infractions commises par son personnel (article 121-1 du code pénal), il peut l'être lorsque les outils professionnels mis à leur disposition ont été utilisés pour les commettre et que l'entreprise en est bénéficiaire. ◗ L'employeur, titulaire de l'accès à internet auprès du fournisseur d'accès, est tenu d'adopter des outils de restriction d'accès pour éviter les actes de contrefaçon en matière de droit d'auteur (code de la propriété intellectuelle, article L.335-12). ◗ De même, la possibilité de laisser accéder les employés à des contenus pédophiles (ce qui est interdit par le code pénal, article 227-23) pourrait engager la responsabilité de l'employeur. Par ailleurs, si la collectivité emploie des stagiaires mineurs, elle s'expose aux sanctions de l'article 227-24 du code pénal, qui vise à empêcher l'accès des mineurs à des messages à caractère violent ou pornographique de nature à porter gravement atteinte à la dignité humaine.

Sauf exception, les administrateurs de systèmes ne doivent pas communiquer les données de messagerie des agents

Quant aux administrateurs de systèmes, ils peuvent être amenés à accéder à des informations personnelles sur les utilisateurs (messagerie, historique des sites consultés, fichiers temporaires ou *cookies* stockés sur les disques durs...). La Cnil considère que cet accès ne se justifie que s'il est nécessaire au bon fonctionnement des systèmes. Les administrateurs sont soumis à une obligation de confidentialité et ne doivent pas communiquer les données de messagerie, qui entrent dans le champ du secret des correspondances privées, sauf si elles portent atteinte au bon fonctionnement technique, à la sécurité ou à l'intérêt de l'entreprise. **Cette confidentialité doit être rappelée dans leur contrat de travail ainsi que dans la charte** d'utilisation des moyens de communication électronique.

1- "Filtrage et internet au bureau : enjeux et cadre juridique", Livre blanc Olfeo, co-écrit avec le cabinet d'avocats Alain Bensoussan : www.olfeo.com
Olfeo propose les seules solutions de filtrage qui respectent les règles juridiques du droit français (civil, pénal, social...). La société équipe environ 500 entreprises en France, dont la moitié dans le secteur public (ville de Grenoble, région Rhône-Alpes...).
2- www.cnil.fr

Droit

Flux RSS : prévoir un contrat de licence fixant les règles de rediffusion

De plus en plus, les collectivités diffusent leurs informations sous forme de *flux RSS*, qui permettent aux internautes de connaître les dernières actualités sans avoir à se rendre sur un site, en utilisant un navigateur, un moteur de recherche ou un *agrégateur* de flux (*Netvibes*...). Le flux présente le titre et le *chapô* (premières lignes) des articles ; un lien permet d'accéder au texte intégral. Les sites de collectivités peuvent aussi proposer des flux provenant d'autres sites, d'actualité par exemple. Un contrat de licence protège généralement les titres et les chapôs, en matière de droit d'auteur ; l'accord de l'organisme éditeur est donc nécessaire pour diffuser un flux. L'autorisation d'intégrer un flux RSS est généralement gratuite, la contrepartie étant que cela permet d'augmenter la fréquentation d'un site. Le contrat de licence interdit la modification du titre et du contenu des flux. La source doit être clairement mentionnée pour éviter des litiges en contrefaçon. Il est important de faire figurer des clauses relatives à l'affichage des articles, en particulier pour obliger le diffuseur à mettre un lien vers l'article référencé. Le contrat peut aussi prévoir d'interdire leur diffusion sur un site commercial.

In "Le droit de l'internet - Lois, contrats, usages", Vincent Fauchoux, Pierre Deprez, Litec, 351 p., 45 euros.

Choix et dépôt de noms de domaine, responsabilité de l'employeur en matière d'utilisation d'internet, création de chartes d'utilisation des moyens électroniques, déontologie sur internet... Cet ouvrage de référence, réalisé par deux avocats, passe en revue les aspects juridiques (textes de droit et jurisprudence) d'internet dans tous les domaines. www.lexisnexis.fr

Comptes

Finances locales en ligne

La direction générale des Finances publiques a publié, en ligne, les premiers résultats 2008 des finances locales.
www.colloc.minefi.gouv.fr

DOCUMENT N°03

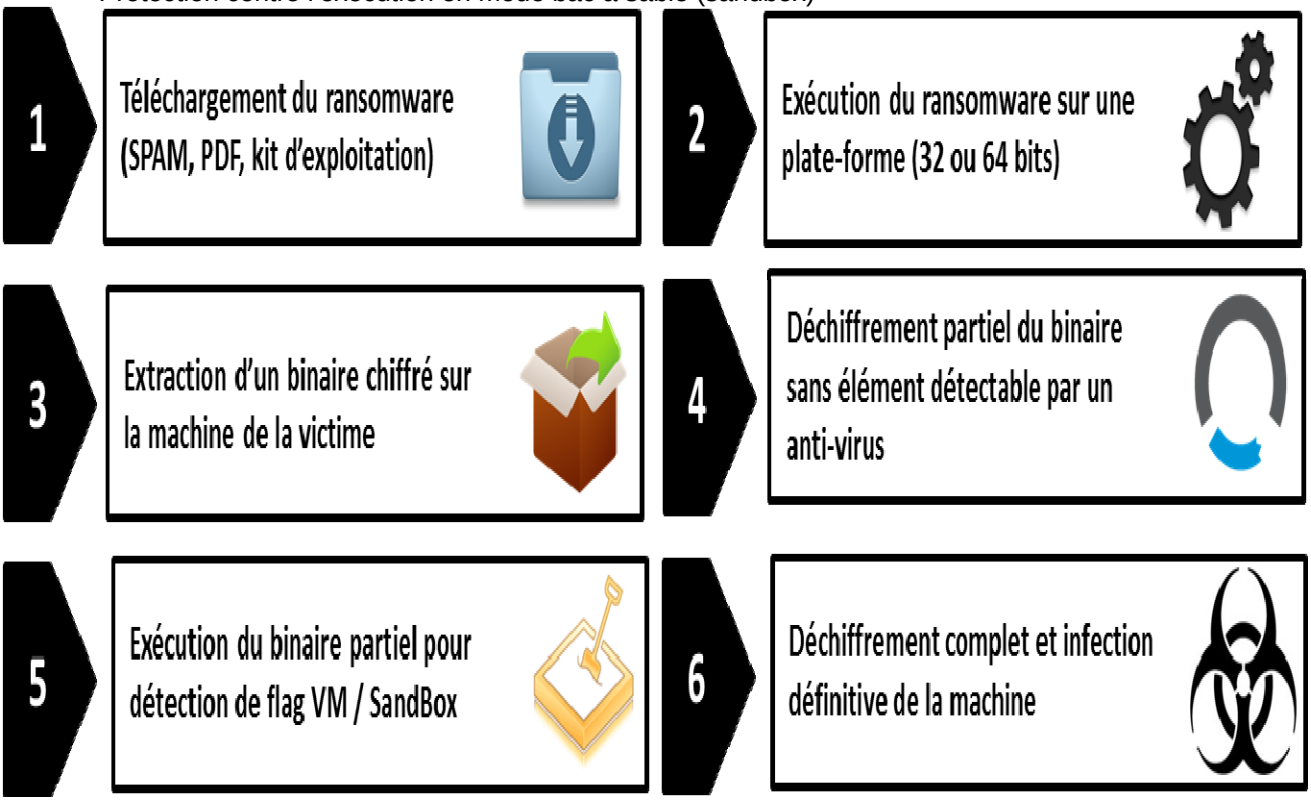
ANALYSE D'UN RANSOMWARE / CRYPTOLOCKER

www.lexsi.com – Anthony Barjon / 02/03/ 2015.

À peine plus de 2 mois après la publication de la version 2.0 sur internet (et décortiquée par les équipes sécurité de Cisco), les développeurs du ransomware Cryptowall viennent de publier une version 3.0.

Bien que cette nouvelle version n'apporte pas de grandes évolutions par rapport aux précédentes, elle maintient les fonctionnalités ayant fait leurs preuves et en améliore d'autres :

- Protection contre l'exécution en mode bac à sable (sandbox)



Principe de fonctionnement de la protection contre l'exécution en mode bac à sable

- Utilisation des réseaux Tor et I2P (nouveauté Crowti / V3.0) pour la communication avec les serveurs C&C
- Suppression des Shadow-Copy

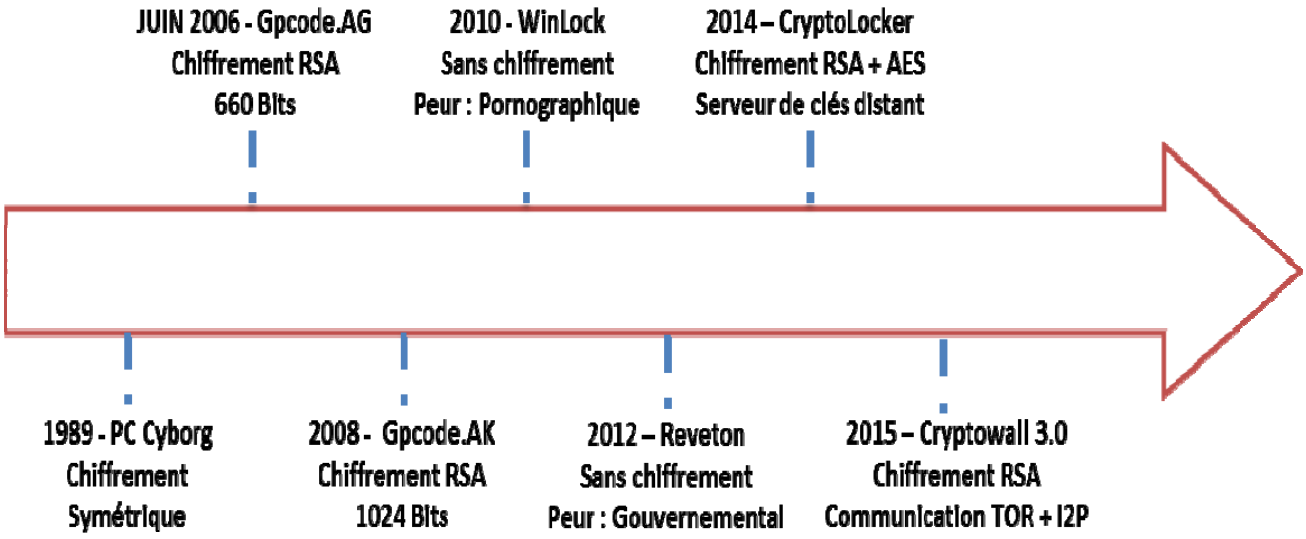
Cryptowall marche sur les traces de son prédécesseur Cryptolocker, éradiqué à la suite de la dissolution du botnet Gameover Zeus à l'été 2014, en lui empruntant certaines fonctionnalités et certains mécanismes (suppression des Shadowcopy, utilisation d'algorithme RSA 2048). Il fait partie d'une nouvelle génération de ransomware cryptographique développé dans le but unique de récolter un maximum d'argent de la façon la plus industrialisée possible.
Malgré les attaques subies (forces de l'ordre, chercheurs, solutions antivirus), des botnets constitués par de nouvelles familles de ransomware continuent d'apparaître et à évoluer, grâce à une forte capacité d'évolution, une réaction rapide des développeurs et un très fort appât du gain.

Mais c'est quoi un ransomware ?

Contrairement à d'autres logiciels malveillants, dédiés à prendre le contrôle d'une machine distante pour voler des informations ou l'exploiter pour mener des attaques en déni de service, les ransomwares vont tenter d'extorquer de l'argent à un utilisateur en **verrouillant logiquement l'accès à sa machine et/ou à ses documents**.

La première apparition recensée d'un ransomware date de 1989 avec « PC Cyborg ». Ce ransomware rendait inopérant le système de la victime en modifiant le nom de l'ensemble des fichiers systèmes et réclamait 189$ pour effectuer un retour arrière.

Une preuve de concept de malware basée sur de la cryptographie asymétrique a été présentée au début de l'année 1996 par les chercheurs Adam L. Young et Moti Yungen[1]. Il a cependant fallu attendre l'année 2006 pour commencer à voir apparaître des versions de ransomware exploitant massivement ce principe.



Chronologie (non exhaustive) des ransomware de 1989 à nos jours.

Le chiffrement réalisé par le ransomware touche les fichiers avec une extension spécifique (notamment les documents bureautique, personnels type photo/vidéo, multimédias, fichiers de configuration, etc.). Les malware peuvent s'installer à la suite de l'exécution par un utilisateur d'un binaire (ex : ouverture d'un fichier téléchargé en P2P ou depuis un site Web, d'une pièce jointe au sein d'un spam, via une clé USB infectée, etc.).

Les ransomwares cryptographiques tels que Cryptolocker ou Cryptowall utilisent des algorithmes de chiffrement robustes afin de limiter ou de bloquer l'accès de la victime à son ordinateur ou à ses données. La victime devant débourser une somme d'argent (voir ci-dessous) pour espérer retrouver ses données sans engagement d'une désinstallation complète du ransomware sur la machine. Les montants demandés varient entre les familles de malware et même pour un même ransomware, les cybercriminels pratiquant parfois un prix à la « tête » du client (victime). Les informations ci-dessous ont été estimées à partir du taux d'un Bitcoin au mois de juin 2014 (640$/BTC) et des différents tarifs fixes identifiés sur les versions étudiées.

Moyenne des rançons demandées par famille de ransomware cryptographique

Et je fais comment pour m'en protéger ?

Il faut avoir conscience qu'une fois les données chiffrées par un ransomware cryptographique de dernière génération, **le déchiffrement de celles-ci se révèle quasiment impossible avec les moyens à la disposition des particuliers et même des grandes entreprises** (ex : brute force, ingénierie inverse).

Parmi les méthodes pouvant dès lors aider à la prévention des risques posés par les ransomwares figurent :

1. Des moyens techniques, pour empêcher l'infection de survenir :

- **L'antivirus** : même si cela est valable pour l'ensemble des logiciels malveillants et que cette solution est très largement insuffisante, **avoir un antivirus fonctionnel et à jour** sur l'ensemble des postes et serveurs reste une première défense nécessaire.

- **Les mises à jour de sécurité :** au même titre que pour la recommandation précédente, **installer les mises à jour de sécurité** demeurent prépondérant. Il convient de mettre à jour à la fois pour les postes utilisateur le système d'exploitation et les applications (lecteur PDF, lecteur messagerie, navigateur et greffons, etc.).

- **Le blocage des points de connexions** : la majorité des ransomwares cryptographique actuels ont besoin d'un accès internet pour être fonctionnels (récupération de clé publique, envoi de clé symétrique). Il est donc recommandé de **vérifier que les solutions de filtrage (proxy, IPS, pare-feu) mises en œuvre au sein de l'entreprise bloquent le plus rapidement possible l'accès à l'ensemble de ces sites distants et aux connexions sortantes via le réseau Tor (ex : points de connexion), souvent utilisé par les ransomwares**.

- **La restriction logicielle** : depuis Windows 7 pour les clients et Windows 2008 R2 pour les serveurs, il est possible **de mettre en place des stratégies de restriction logicielle**. Même si une solution exhaustive n'est pas réalisable, il est conseillé de configurer des restrictions logicielles (SRP/AppLocker sous Windows) permettant d'empêcher l'exécution de code à partir d'une liste noire de répertoires à définir.

2. Et des démarches limitant le nombre d'occurrences et les impacts associés :

- **La sensibilisation** : la prévention passe avant tout par **l'information et la sensibilisation des utilisateurs aux risques associés aux messages électroniques.** Il est important de mener des campagnes régulières en direction des différents publics internes à risque, afin de limiter au maximum le nombre de victimes.
- **La sauvegarde** : une des rares méthodes, à l'heure actuelle, pour limiter les impacts reste la mise en place d'une politique de **sauvegarde** régulière des postes de travail et serveurs. Le déchiffrement via paiement de la rançon aux attaquants ne devant pas être considéré comme une option crédible, restaurer les fichiers à partir d'une sauvegarde récente demeure la principale solution pour limiter les impacts relatifs aux ransomwares. Attention néanmoins à :

    - protéger les sauvegardes pour ne pas qu'elles puissent être impactées par les effets d'un Ransomware (ex : chiffrement des données).

    - contrôler les données sauvegardées pour ne pas écraser des données viables vec des données chiffrées par un ransomware cryptographique.

DOCUMENT N°04

Premier espace public équipé en WiFi à Chamalières.

Le premier espace équipé en WiFi a été inauguré le 19 janvier à la Maison des associations.

lamontagne.fr / 23/01/2012.

A Chamalières, Internet devient accessible dans les lieux publics.

Internet est désormais accessible à la Maison des associations. La municipalité a fait installer le WiFi afin de permettre aux nombreuses associations, hébergées dans la maison du même nom, d'accéder dans des conditions optimisées au réseau Internet. L'inauguration a eu lieu jeudi 19 janvier, en presence du maire et de nombreux élus.

L'installation du réseau a été assurée par la société Noodo, jeune entreprise clermontoise spécialisée dans l'installation, la gestion et la maintenance de réseaux WiFi publics. Elle a déjà à son actif l'installation et la gestion du réseau public clermontois, place de Jaude, place de la Victoire, du 1er mai et au jardin Lecoq.

Le matériel et le réseau sont conformes aux normes actuellement en vigueur, notamment en ce qui concerne les émissions radioélectriques, la puissance maximale d'émission en sortie des bornes WiFi étant de 100 mW. A la maison des associations, l'utilisateur peut se connecter à Internet à l'aide d'un ordinateur fonctionnant sous Windows ou MacOs, un smartphone, un PDA ou une tablette.

Le maire et les membres du Conseil municipal écoutent les explications d'Eric Garand.

Un accès au réseau libre et gratuit.

La procédure est simple : l'internaute se connecte sur le WiFi "Maison des associations" et accède au portail d'authentification Noodo. Une fois l'authentification effectuée, il peut accéder à Internet librement et gratuitement. Le service est en effet gratuit pour les usagers. Le portail est disponible en français et en anglais. Pour éviter tout utilisation abusive du réseau, la solution WiFi adoptée comporte un filtrage qui bannit certaines recherches (pornographie, toxicomanie, violence, virus, vente d'alcool...). Le financement de l'opération a été fait par la ville, pour un total de 2.566 € (matériel et installation), l'abonnement annuel étant de 908 €. Si la Maison des associations est la première structure à être équipée en WiFi, l'accès à Internet sera prochainement accessible dans d'autres espaces chamalièrois : c'est le cas du parc Montjoly et du parc Thermal où, en partenariat avec la municipalité de Royat et l'Office de tourisme de Chamalières-Royat, un accès WiFi sera disponible.

Noodo, une entreprise clermontoise en pleine expansion

En japonais, Noodo signifie : nœud, lien. Une appellation en totale adéquation avec cet opérateur de télécommunications indépendant spécialisé dans l'intégration de systèmes WiFi pour les professionnels.

Fondée en 2007 à Clermont-Ferrand par Eric Garand et Loïc Devaux, la société Noodo est devenue en peu de temps une référence dans le domaine de l'installation de systèmes WiFi. Elle équipe en particulier de nombreux hôtels et restaurants de la France entière, mais également des entreprises et de nombreux espaces publics, à la demande des municipalités. "Huit personnes travaillent dans l'entreprise confie Eric Garand. Nous avons récemment signé un partenariat avec PSA Peugeot-Citroën. Ce sont désormais plus de 1050 établissements publics et privés qui sont gérés par Noodo à l'échelle nationale ".

DOCUMENT N°05

Filtrage et internet au bureau : enjeux et cadre juridique en France.

www.olfeo.com – Livre blanc juridique Olfeo co-écrit avec le Cabinet d'avocats Alain Bensoussan (Extrait). 13/06/2014.

LES ASPECTS JURIDIQUES DU FILTRAGE

Il n'y a plus de doute aujourd'hui, le filtrage est admis sur tous les plans :

- Au plan légal
- Au plan jurisprudentiel
- Au plan normatif et des bonnes pratiques
- Et sur le plan des usages

Cette reconnaissance s'étend naturellement au-delà des frontières hexagonales.

Mais comprendre le droit du filtrage c'est aussi s'intéresser :

- Au droit des logs, car tous les outils de filtrage comportent des logs et fichiers qui seront le cas échéant exploités pour sanctionner un abus

- Au droit des chartes d'usage des systèmes d'information car il ne saurait être question de filtrer sans informer et fixer des règles.

I.1 **LE DROIT DE FILTRER - ASPECT LÉGAL** I.1

Le terme de « filtre » ou de « filtrage », n'est pas inconnu des textes actuels.

On trouve effectivement des références et des renvois exprès à ces termes dans différents documents :

- **Lois dites Hadopi** :

  - la loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet précise ainsi que la Haute Autorité, dite l'Hadopi, «évalue, en outre, les expérimentations conduites dans le domaine des technologies de reconnaissance des contenus et de **filtrage** par les concepteurs de ces technologies la matière, notamment pour ce qui regarde l'efficacité de telles technologies, dans son rapport annuel prévu à l'article L. 331-14 » ;

  - le rapport Hadopi de février 2013 sur les moyens de lutte contre le streaming et le téléchargement direct illicite énonce que «d'un point de vue technique, la mesure de **filtrage** pourrait passer par l'installation d'un module chez l'utilisateur (plug-in) »

- **L'arrêté du 27 juin 1989**, relatif à l'enregistrement du vocabulaire de l'informatique dont l'article annexe II définit notamment le **filtrage** comme « mise en correspondance de formes selon un ensemble prédéfini de règles ou de critères »

- **La circulaire 2004-035 relative à l'usage de l'Internet dans le cadre pédagogique et de la protection des mineurs du 18 février 2004** prévoyant « la mise en oeuvre d'outils de **filtrage** dans les établissements ou écoles »

Le droit européen reconnaît depuis plus longtemps encore le droit de filtrer :

- **La décision 276/1999/CE du 25 janvier 1999 du Parlement européen et du Conseil**1 adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la **lutte contre les messages à contenu illicite** et préjudiciable diffusés sur les réseaux mondiaux. Le considérant n°5 met en avant le fait que les outils de filtrage constituent des éléments essentiels pour assurer un environnement plus sûr sur Internet

- De nombreuses recommandations du **Comité des Ministres aux États Membres** (notamment recommandation 2008-6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des **filtres Internet**, recommandation 2001-8 sur l'autorégulation des cyber-contenus, recommandation 2007-11 sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication)

Au-delà des mots « filtre » et « filtrage », il existe bon nombre de textes qui utilisent d'autres terminologies ou d'autres notions qui sont synonymes de « filtre » ou de « filtrage » :

- **L'article 6 I.–1 de la loi n°2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique (« LCEN ») retient la formule suivante : « **moyens techniques permettant de restreindre l'accès** à certains services de communication au public en ligne ou d'opérer une sélection de ces services »2

- Les articles L.331-25 ; L331-26 ; L331-27 ; L335-7-1 et R331-4 du **Code de la propriété intellectuelle** utilisent les termes « **moyens de sécurisation** »3

- **L'article L.336-2 du Code de la propriété intellectuelle** vise « toutes mesures propres à prévenir ou à faire **cesser une telle atteinte à un droit d'auteur** ou un droit voisin »

- **Le décret n°2010-1630 du 23 décembre 2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation** destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne

- **L'article 61 de la loi n° 2010-476 du 12 mai 2010 relative à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne** :

  - « l'arrêt de l'accès à ce service aux personnes mentionnées au 2 du I et, le cas échéant, au 1 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. »
  - « toute mesure destinée à faire cesser le référencement du site d'un opérateur mentionné au deuxième alinéa du présent article par un moteur de recherche ou un annuaire. »

- **L'article L.141-1 VIII 3° du Code de la consommation**, crée par l'article 76 VIII de la loi Hamon du 17 mars 2014, autorise la DGCCRF à demander à l'autorité judiciaire de prescrire aux hébergeurs ou fournisseurs d'accès à Internet «toutes mesures proportionnées propres à prévenir un dommage ou à faire cesser un dommage causé par le contenu d'un service de communication au public en ligne»

- **L'article 12 de la loi n°2014-1353 du 13 novembre 2014** renforçant les dispositions relatives à la lutte contre le terrorisme et la pédopornographie a créé l'article 6-1 de la LCEN, qui prévoit notamment la possibilité pour l'autorité administrative de demander aux hébergeurs et éditeurs de site Internet de retirer les contenus pornographiques de mineurs ou faisant l'apologie du terrorisme, et d'en informer simultanément les fournisseurs d'accès Internet, à qui elle pourra communiquer les adresses électroniques des internautes devant être bloqués pour tout accès Internet, si le retrait n'a pas été fait sous vingt-quatre heures

- **Un de ses décrets d'application n°2015-125 du 5 février 20154** relatif à la protection des internautes contre les sites provoquant à des actes de terrorisme ou en faisant l'apologie, et les sites diffusant des images et représentations de mineurs à caractère pornographique, pris pour l'application de l'article 6-1 de la loi n°2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique

  S'appliquant expressément aux fournisseurs d'accès à Internet, le décret **décrit les modalités de blocage des sites** contrevenant **aux dispositions des articles 227-23 et 421-2-5 du Code pénal à savoir :** « la procédure permettant d'empêcher l'accès des internautes aux sites incitant à la commission d'actes de terrorisme ou en faisant l'apologie et aux sites diffusant des images et représentations de mineurs à caractère pornographique. »
  Il précise notamment que la technique de blocage des sites est celle qui consiste à intervenir sur le nom de domaine.

CE QU'IL FAUT RETENIR…
NOMBREUX SONT LES TEXTES DE LOI QUI IMPOSENT OU LÉGITIMENT LE RECOURS AU FILTRAGE

I.2 **LE DROIT DE FILTRER - ASPECT JURISPRUDENTIEL** I.2

Le terme de « filtre » ou de « filtrage » est retenu dans plusieurs jugements et arrêts.
Le filtrage a dès les premiers contentieux du web pris un sens tout à fait particulier pour le juge.

L'obligation de filtrage s'est imposée naturellement comme l'une des solutions à l'accès à des contenus/plates-formes illicites dans beaucoup de domaines :

- Vente d'objets nazis sur le site yahoo.com accessible depuis la France5
- Vente de parfums Christian Dior en dehors de leur réseau de distribution sélectif
- Diffusion de pages à contenus racistes6
- Diffusion de propos négationnistes7
- Jeux en ligne et paris hippiques8
- Site d'hébergement de vidéos (YouTube9, Dailymotion10)

Déjà en 2010, **le Président du Tribunal de grande instance de Paris**11 a ordonné, en application de la loi du 12 mai 2010 relative à la concurrence et à la **régulation du secteur des jeux d'argent et de hasard en ligne**, aux fournisseurs d'accès à Internet, de prendre « toute mesure de filtrage, pouvant être obtenu, ainsi que les défendeurs l'exposent, par blocage du nom de domaine, de l'adresse IP connue, de l'URL, ou par analyse du contenu des messages, mises en oeuvre alternativement ou éventuellement concomitamment de manière à ce qu'elles soient suivies de l'effet escompté sur le territoire français ».

La Cour d'appel de Paris a reproché à une société de courtage **de ne pas avoir mis en oeuvre un filtrage efficace**12, et le même jour de ne pas avoir détaillé le fonctionnement effectif d'un tel filtrage ni détaillé ses résultats13.

Dans une décision du 14 décembre 2010, **le Tribunal de grande instance de Créteil**14 a fait injonction à un hébergeur **d'installer sur son site un système de filtrage efficace et immédiat** des vidéos dont la diffusion illicite a été ou sera constatée par l'Institut National de l'Audiovisuel (INA).

Cette jurisprudence en matière de filtrage s'est développée depuis le début des années 2000, en particulier en parallèle du développement de la vente sur Internet, ce qui a soulevé un certain nombre de problématiques liées à l'accès à des sites illicites.

De 2011 à 2014, la position de la jurisprudence en matière de filtrage à l'égard des fournisseurs d'accès à Internet et des hébergeurs s'est assouplie, avec notamment deux arrêts du même jour de la Cour de cassation. **Il en ressort que les fournisseurs d'accès à Internet ne sont pas astreints à effectuer un contrôle permanent et à priori d'Internet.**15.

La question de la mise en place des outils de filtrage connaît donc une multitude d'applications jurisprudentielles, à chaque fois que s'est posée la question de mettre en place des mécanismes faisant obstacle à la consultation des sites illicites.

CE QU'IL FAUT RETENIR…
LES JUGES ORDONNENT COURAMMENT LA TECHNIQUE DE FILTRAGE POUR IMPOSER UNE RESTRICTION D'ACCÈS

I.3 LE DROIT DE FILTRER - BONNES PRATIQUES ET NORMES

La Commission Nationale de l'Informatique et des Libertés (CNIL) s'intéresse également au filtrage, notamment aux mesures de filtrage mises en place au sein des entreprises par le biais d'un certain nombre de documents, et en particulier :

- **Les fiches de synthèse « Cybersurveillance sur les lieux de travail »** du 11 février 2002
- **Le rapport de la CNIL** « **La cybersurveillance sur les lieux de travail** » édition mars 2004
- **Le guide « la sécurité des données à caractère personnel** », édition 2010
- **Le guide pratique de la CNIL** « **pour les employeurs et les salariés** », édition 2010 dont la fiche n°6 porte sur le « Contrôle de l'utilisation d'Internet et de la messagerie »
- **L'évaluation des salariés : droits et obligations des employeurs,** 11 mai 2011
- **La fiche « les outils informatiques au travail** », janvier 2013
- **La fiche pratique Keylogger** : des dispositifs de cybersurveillance particulièrement intrusifs du 20 mars 2013
- **L'article de la CNIL sur « l'analyse des flux https : bonnes pratiques et questions »** du 31 mars 2015

Dans son guide pratique pour les employeurs et les salariés16, la CNIL considère que s'il n'est pas possible d'interdire « de manière générale et absolue » l'utilisation d'Internet à des fins non professionnelles, en se référant notamment au contexte de développement des moyens de communication ainsi qu'au contexte jurisprudentiel actuel, rien n'empêche l'employeur de limiter notamment l'accès de ses employés à Internet.

Selon la commission, une telle limitation de l'accès à Internet ne constitue pas par principe une atteinte à la vie privée des employés et se justifie notamment parce que l'usage d'Internet est en général reconnu à condition qu'un tel usage soit, selon elle : raisonnable, ne réduise pas la productivité, ni les « conditions d'accès professionnel au réseau ».

D'un point de vue pratique, la CNIL reconnaît la possibilité de mettre en place des dispositifs de filtrage de sites non autorisés : sites à caractère pédophile, révisionniste, raciste… .

Selon la Commission, l'employeur peut imposer certaines mesures dans l'utilisation des systèmes d'information, justifiées pour la sécurité de l'organisme, telles que : l'interdiction de télécharger des logiciels, de se connecter à des forums « chat », ou d'accéder à une messagerie électronique personnelle, à condition d'en informer les salariés.

En tout état de cause, les instances représentatives du personnel doivent être informées ou consultées avant l'installation d'un dispositif de contrôle de l'activité.

Chaque employé doit être notamment informé :
- Des finalités poursuivies
- Des destinataires des données
- De son droit d'opposition pour motif légitime
- De ses droits d'accès et de rectification

La CNIL a également encadré l'utilisation des keyloggers, qui tracent tous les caractères saisis sur un clavier par un utilisateur sur son ordinateur. Ils permettent ainsi à un employeur de connaître les mots saisis lors de la rédaction d'un email, d'un échange sur messagerie instantanée ou de la consultation d'un site Internet.

Elle a ainsi considéré que ce dispositif portait une atteinte excessive à la vie privée des salariés concernés, et qu'il était dès lors, illicite au regard de la loi Informatique et Libertés.

Elle a rappelé en outre que la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 punit de 5 ans d'emprisonnement et de 300 000 € d'amende l'utilisation de certains dispositifs de captation de données informatiques à l'insu des personnes concernées.17

Par ailleurs, l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) a publié deux documents techniques traitant des outils de filtrage :

- La **note technique portant sur la Recommandation du 30 Janvier 2013** pour la définition d'une politique de filtrage réseau d'un pare-feu.

  Ce document vise à procurer les éléments organisationnels qui permettent de structurer la base de règles sur lesquelles s'appuie la politique de filtrage réseau appliquée sur un pare-feu d'interconnexion.
  Il est destiné à toutes les personnes ayant pour mission d'élaborer et d'appliquer ou d'administrer des architectures d'interconnexion sécurisées, qui désirent s'assurer que leurs politiques de filtrages réseau appliquées sur les pare-feu sont bien pérennes.

- **La recommandation sur le filtrage des flux HTTPS du 9 octobre 2014** (cf supra II 3) à laquelle se réfère expressément la CNIL dans son article du 31 mars 2015.

CE QU'IL FAUT RETENIR…
LE FILTRAGE FAIT ASSURÉMENT PARTIE DE CE QU'IL EST CONVENU D'APPELER LES « BONNES PRATIQUES » EN TERMES DE MANAGEMENT DU SYSTÈME D'INFORMATION ET DE SÉCURITÉ

II.2 **LES ACCÈS INVITÉS AU RÉSEAU INTERNET DE L'ENTREPRISE**

L'accès au web pour un public tiers se développe comme une traînée de poudre.
Hier limité aux cybercafés et à quelques aéroports pionniers dans le domaine des hotspots, aujourd'hui l'accès public au web est partout : salons, hôtels, restaurants, points d'information publics.

Cette pratique, de plus en plus développée dans les entreprises et les administrations, laissant accès uniquement à Internet via leur Wi-Fi, est souvent appelée la pratique du Wi-Fi « invité » ou « visiteur ».

Il faut ici rappeler deux réalités juridiques :

- **L'article L. 34-1 du Code des postes et des communications électroniques** dispose « Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article ».

  En langue naturelle cela signifie que les hotspots professionnels sont soumis aux mêmes obligations que les hotspots mis à disposition par les opérateurs de télécommunications notamment en termes **d'identification des utilisateurs et de conservation des données de trafic**.

  Les entreprises, offrant un réseau interne ouvert au public au sein de l'entreprise, sont considérés comme fournisseur de **réseau interne ouvert au public**41. Ces réseaux **ne sont pas soumis à l'obligation de se déclarer opérateurs auprès de l'ARCEP**, seuls les réseaux ouverts au public sont soumis à l'obligation de déclaration42.

- **L'article L. 336-3 alinéa 1 du Code de la propriété intellectuelle issue de la loi dite Hadopi**, dispose « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'oeuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. Le manquement de la personne titulaire de l'accès à l'obligation définitive au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé sous réserve **des articles L 335-7 et L 335-7-1 du Code de la propriété intellectuelle** ».

De fait, les personnes qui gèrent des accès publics ou invités au web seraient très inspirées de mettre en oeuvre des mesures de filtrage, de recueil de leur identité et d'en informer les utilisateurs. Il est également évident qu'ils ont l'obligation de loguer.

Comment un employeur peut-il encadrer les accès Wi-Fi invités ?

Il est possible d'encadrer l'accès Wi-Fi invités mis à disposition par un organisme à ses invités ou même d'un employeur à ses salariés en prévoyant :

- **La limitation de l'accès à certains sites et services**, par conséquent, il est nécessaire de mettre en oeuvre un système de filtrage

- **La conservation des données** de connexion

- **Une charte Wi-Fi** présentant à minima une clause de mise en garde : « L'organisation se réserve le droit de mettre en place des dispositifs de sécurisation afin de s'assurer que l'accès ne fasse pas l'objet d'une utilisation frauduleuse ou illicite. L'entreprise pourra à sa seule discrétion, et sans avis préalable, modifier, suspendre ou interrompre l'accès à tout ou partie du Wi-Fi»

LE SAVIEZ-VOUS ?
TOUTE PERSONNE QUI « OFFRE » UN ACCÈS PUBLIC PEUT VOIR SA RESPONSABILITÉ ENGAGÉE DU FAIT DES ACCÈS ILLICITES DES TIERS

II.3 **LES FLUX SÉCURISÉS : HTTPS, FTPS…**

Parmi les flux qui transitent sur le réseau de l'entreprise, les flux sécurisés constituent un cas particulier. Le protocole HTTPS offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web.

Pour ce faire, le HTTPS fait usage du protocole SSL/TLS qui utilise des méthodes de cryptographie asymétrique pour l'authentification, et des méthodes de cryptographie symétrique pour le chiffrement des échanges.

Ainsi, en principe, l'utilisation du protocole SSL/TLS permet d'assurer :

- **L'authentification de l'une ou des deux parties communicantes**
- **La confidentialité des échanges**
- **L'intégrité des données échangées**

Son usage s'étend aussi bien aux contenus professionnels qu'aux contenus personnels : banques en ligne, commerce en ligne…

Le flux étant chiffré entre le poste utilisateur et le serveur web, l'entreprise ne dispose pas de moyen de contrôle sur son contenu. L'antivirus de flux est, par exemple, inopérant. Des sites mal intentionnés pourraient donc utiliser ce protocole pour introduire du contenu indésirable dans l'entreprise à son insu.

Une technique de cryptanalyse, dite Man In The Middle, jusqu'ici utilisée par les pirates et les agences de renseignement, permet cependant de pouvoir déchiffrer ce flux et donc y appliquer des techniques de contrôle de contenu.

III. **NE PAS FILTRER, NE PAS LOGUER : QUELLES CONSÉQUENCES ?**

La conséquence se mesure nécessairement à l'aune du droit applicable. Mais dans cette hypothèse le droit français apparaît comme la seule référence possible pour toutes les entreprises françaises ou étrangères disposant de personnel sur le territoire national.

Une fois la question du droit applicable posée, il est possible d'apprécier le risque d'une part et la responsabilité d'autre part.

QUEL DROIT APPLIQUER ? III.1

Pour une entreprise française, salariant du personnel sur le territoire national et commercialisant en France, la question ne se pose pas.

Elle se pose à l'inverse pour les entreprises multinationales ou pour les entreprises étrangères salariant des personnels en France.

Or sur ce point le principe de droit international privé est simple :

- **L'article 1837 du Code civil** dispose que « **Toute société dont le siège est situé sur le territoire français est soumise aux dispositions de la loi française**. Les tiers peuvent se prévaloir du siège statutaire, mais celui-ci ne leur est pas opposable par la société si le siège réel est situé en un autre lieu. »

- **L'article 14 du code civil dispose que :** « L'étranger, même non résidant en France, pourra être cité devant les tribunaux français, pour l'exécution des obligations par lui contractées en France avec un Français ; il pourra être traduit devant les tribunaux de France, pour les obligations par lui contractées en pays étranger envers des Français. »

- **Au plan pénal** la chose est tout aussi simple et fixée par **l'article L. 113-2 du Code pénal** qui précise que « **La loi pénale française est applicable aux infractions commises sur le territoire de la République**. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ».

Par principe, à partir du moment où l'entreprise, sa filiale et ses salariés sont sur le territoire français, ils sont soumis à la loi française.

LE SAVIEZ-VOUS ?
LE DROIT FRANÇAIS S'APPLIQUE À TOUTES LES ENTREPRISES DONT LE SIÈGE EST SITUÉ EN FRANCE AINSI QU'AUX INFRACTIONS COMMISES EN FRANCE

III.2 **QUELS RISQUES ?**

Les risques de ne pas filtrer sont de deux niveaux :

- **Un risque direct** de ne pas respecter la loi ou une décision de justice
- **Un risque de devenir responsable** des accès des autres

III.2.a **LE NON-RESPECT DE L'OBLIGATION LÉGALE DE FILTRAGE**

Pour certains acteurs

Le droit impose à certains acteurs de mettre en oeuvre ou de mettre à la disposition de leurs propres utilisateurs des moyens de contrôle ou de restriction des accès à Internet, c'est-à-dire en pratique de mettre en oeuvre des outils de filtrage. Le droit impose également à certains acteurs de conserver les journaux de logs.

L'obligation légale la plus exemplaire dans ce domaine correspond à celle qui pèse sur les fournisseurs d'accès à Internet :

- **L'article 6 I. – 1° de la LCEN** dispose que « **Les personnes dont l'activité est d'offrir un accès** à des services de communication au public en ligne **informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès** à certains services ou de les sélectionner et leur proposent au moins un de ces moyens. »

Cet article, s'il impose directement au fournisseur d'accès de proposer à ses abonnés un moyen technique permettant de restreindre l'accès à Internet, implique indirectement l'obligation pour ledit abonné de le mettre en oeuvre, sous sa responsabilité.

Les fournisseurs d'accès et les hébergeurs sont également tenus à une obligation de conservation des données d'identification :

- **L'article 6 II. de la LCEN** dispose que : « **Les personnes** mentionnées aux 1 et 2 du I **détiennent et conservent les données de nature à permettre l'identification de quiconque** a contribué à la création du contenu ou de l'un des contenus dont elles sont prestataires. »

De même le fait pour un tribunal d'ordonner à une entreprise de mettre en oeuvre des outils de filtrage devient une obligation à part entière.

Au plan jurisprudentiel, l'arrêt **de la Cour d'appel de Paris du 4 février 2005**55, aurait pour certains auteurs, assimilé l'employeur qui donne accès à Internet à ses employés, à un fournisseur d'accès.

De fait, si cette interprétation devait s'avérer exacte, tout employeur qui mettrait à disposition de ses employés, de ses agents ou de toute autre personne un accès à Internet, pourrait se voir opposer l'obligation légale posée à l'article 6 de la loi pour la confiance dans l'économie numérique :

- De **mettre à disposition des outils de filtrage** et d'en informer les utilisateurs

- De **conserver les données d'identification** énumérées au sein du décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication de données, permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

Le risque spécial : Code de la propriété intellectuelle

L'article L. 336-3 du Code de la propriété intellectuelle précise que « **La personne titulaire de l'accès** à des services de communication au public en ligne a **l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation** à des fins de reproduction, de représentation, de mise à disposition ou de communication au public **d'oeuvres ou d'objets protégés par un droit d'auteur** ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ».

L'article ne vise en effet pas expressément le filtrage, l'abonné a « simplement » l'obligation de veiller à ce que l'accès à Internet ne permette pas de contrevenir aux droits de propriété intellectuelle par un téléchargement illégal d'oeuvres protégées par le droit d'auteur. Pour ce faire, il doit mettre en place un moyen de sécurisation de son accès au réseau, qui consiste selon les lois Hadopi en un moyen de reconnaissance des contenus et de filtrage.

De fait, cela implique pour lui de mettre en place des moyens de filtrage de l'accès aux réseaux.
L'abonné a par conséquent une obligation spéciale de contrôle de l'utilisation de l'accès à Internet qu'il utilise et met à disposition.

Il faut bien distinguer l'abonné de l'internaute. L'abonné est la personne physique ou morale qui est « juridiquement » liée à un fournisseur d'accès, l'internaute n'est pas nécessairement un abonné à Internet. Il est celui qui navigue sur Internet et accède aux services en ligne.

L'employeur titulaire de l'abonnement qui met à disposition de ses salariés un accès à Internet dans le cadre de leur travail est qualifié d'abonné et est par conséquent, responsable de leur activité sur les réseaux sur le fondement des lois Hadopi, et plus particulièrement en ce qui concerne le téléchargement d'oeuvres protégées par un droit d'auteur.

LE SAVIEZ-VOUS ?
LE CODE DE LA PROPRIÉTÉ INTELLECTUELLE RENFORCE L'OBLIGATION DE FILTRAGE DES ENTREPRISES

III.2.b **LE RISQUE DE NE PAS FILTRER POUR UNE ENTREPRISE OU ADMINISTRATION**

L'entreprise peut voir sa responsabilité engagée sur au moins trois fondements :

- L'article **1384** du Code civil
- L'article **121-2** du Code pénal
- L'article **L 336-3** du Code de la propriété intellectuelle

Sans oublier l'impact toujours réel mais difficilement mesurable aujourd'hui de **l'arrêt de la Cour d'appel de Paris du 4 février 2005**57.

Le risque civil

L'article 1384 alinéa 5 du code civil dispose « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. (…) Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ».

En d'autres termes **l'employeur est responsable des dommages causés par ses salariés** dans l'exercice de leurs fonctions.

Le risque civil consiste à devoir répondre des préjudices causés et donc de réparer le dommage causé et d'indemniser la victime par le paiement de dommages et intérêts.

Le risque pénal

L'article 121-2 du Code pénal dispose « Les personnes morales, à l'exclusion de l'État, sont responsables pénalement, selon les distinctions **des articles 121-4 à 121-7**, des infractions commises, pour leur compte, par leurs organes ou représentants ».

En d'autres termes **l'employeur est responsable des actes de ses salariés au pénal si l'entreprise est bénéficiaire de l'acte illicite.**

Le risque pénal consiste à devoir répondre de la commission d'infractions et donc d'être sanctionné pénalement.

L'entreprise pourrait donc voir sa responsabilité engagée pour des accès illicites :

- **À des sites en raison de leurs contenus** portant notamment atteinte :
- **Aux mineurs**, tels que les contenus pédopornographiques ou encore les contenus incitant à l'anorexie.58
- **À des sites de jeu en ligne illégaux** (ceux qui sont accessibles depuis le territoire français alors qu'ils n'ont pas bénéficié de l'agrément délivré par l'Autorité de régulation des jeux en ligne)
- **À la protection des auteurs**, s'agissant des sites contrefaisants
- À des sites faisant **l'apologie du terrorisme**

Il s'agit également de sites dont les contenus dépassent la liberté d'expression, tels que les sites racistes ou révisionnistes59.

- **À des sites au regard des produits et services qu'ils commercialisent** tels que notamment :

    - Des organes et produits du corps humain
    - Des drogues
    - Des objets à caractère pédophile
    - Des armes à feu et explosifs
    - Des médicaments
    - Du tabac
    - De l'alcool
    - Des logiciels permettant de porter atteinte à un système de traitement automatisé de données
    - Des logiciels de contournement de mesures techniques de protection ou d'information

Plus généralement, des produits interdits ou réglementés.

LE SAVIEZ-VOUS ?
L'ENTREPRISE PEUT VOIR SA RESPONSABILITÉ ENGAGÉE

III.3 **QUI EST RESPONSABLE ?**

LA RESPONSABILITÉ DE L'EMPLOYEUR III.3.a

Au civil

Selon l'article 1384 alinéa 5 du code civil, l'employeur est responsable des dommages causés par ses salariés dans l'exercice de leurs fonctions.

Aujourd'hui la question se pose clairement de savoir si un employeur, qu'il soit un acteur privé (entreprise, association, fédération) ou public (ministère, collectivité territoriale, établissement public) est tenu ou non de mettre en place au sein de sa structure des outils de filtrage et de loguer.

Le débat porte essentiellement sur le niveau de responsabilité de l'employeur face à un usage illicite de l'Internet par ses employés et lorsqu'il donne accès à Internet à des tiers.

Il existe une jurisprudence abondante qui fixe les limites de cette responsabilité.

En est-il de même pour les administrations ou les collectivités territoriales ?

En effet, dans l'hypothèse où une collectivité territoriale n'a pas mis en place des mesures nécessaires pour la sécurité et le contrôle d'Internet utilisé par son personnel, et notamment pas utilisé de logiciel de filtrage, sa responsabilité pénale peut-elle être engagée du fait de la commission d'une infraction par l'un des membres de son personnel (ex : un agent qui aurait téléchargé sur Internet des images pédophiles via le système d'information de la collectivité territoriale63) ?

La réponse est plutôt négative

En effet, l'hypothèse n'entrant pas dans les prévisions **de l'article 121-2 du Code pénal**, l'absence de mise en place de mesures de filtrage pour sécuriser l'utilisation d'Internet par son personnel ne fait pas partie des circonstances dans lesquelles la responsabilité pénale de celle-ci peut être engagée.

Néanmoins, sa responsabilité pourra être engagée en tant que commettant de son préposé si les conditions sont remplies.

Pour s'en défendre, l'administration devra prouver les trois éléments cumulatifs suivants, à savoir que l'agent a agi :

- Hors du cadre de ses fonctions
- Sans autorisation
- En dehors de ses attributions

Mais cela n'exclura pas toujours sa responsabilité. En effet, depuis **l'arrêt Lemonnier**64, les mêmes faits peuvent constituer à la fois une faute personnelle de l'agent et une faute de service pour laquelle l'administration devra rendre des comptes.

À ce titre, la doctrine précise qu'à partir du moment où la faute a un lien avec le service, cette faute personnelle apparaît comme « non dépourvue de tout lien avec le service », du fait qu'elle a été réalisée soit pendant l'exercice des fonctions de l'agent, soit parce que l'exercice de sa mission a pu faciliter sa commission d'une quelconque manière.

De plus, même lorsque la faute personnelle est commise en dehors du temps et du lieu d'exercice des fonctions, qu'elle cause un préjudice et est commise par l'usage d'instruments fournis à l'agent par le service, l'administration est responsable du fait de son agent au titre de la faute de service, ayant contribué de manière quelconque à sa commission.65

La jurisprudence a estimé que dans ce cas **la faute personnelle n'est « pas dépourvue de tout lien avec le service** ».66

LE SAVIEZ-VOUS ?
LE PREMIER DONT LA RESPONSABILITÉ SERA RECHERCHÉE EST L'EMPLOYEUR

1 Le considérant n°5 de la décision 276/1999 CE du 25-1-1999 : « Considérant que la promotion de l'autoréglementation de l'industrie et des systèmes de suivi du contenu, le développement des outils de filtrage et des systèmes de classement fournis par l'industrie et une sensibilisation accrue portant sur les services offerts par l'industrie, de même que l'encouragement de la coopération internationale entre toutes les parties concernées, joueront un rôle crucial dans la consolidation de cet environnement sûr et contribueront à lever les obstacles au développement et à la compétitivité de l'industrie concernée ».
2 LCEN art. 6 I.–1° : « Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens ».
3 CPI art. L. 335-12 : « Le titulaire d'un accès à des services de communication au public en ligne doit veiller à ce que cet accès ne soit pas utilisé à des fins de reproduction ou de représentation d'oeuvres de l'esprit sans l'autorisation des titulaires des droits prévus aux livres Ier et II, lorsqu'elle est requise, en mettant en oeuvre les moyens de sécurisation qui lui sont proposés par le fournisseur de cet accès en application du premier alinéa du I de l'article 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
4 Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.
5 CA Paris, 3-9-2010 n°08/12822
6 TGI Nanterre 24-5-2000.
7 TGI Paris 20-4-2005, ordonnance de référé UEJF et a. c/ olm llc et a.
8 TGI Paris, 6-8-2010 RG n°10/56506.
9 TGI Créteil, 14-12-2010 n°06-12815.
10 TGI Paris 13-1-2011 n°09-16645.
11 TGI Paris, 6-8-2010 Président de l'Autorité de Régulation des Jeux en Ligne c/ Neustar et autres, RG n°10/56506.
12 CA Paris, 3-9-2010 RG n°08/12820, CA Paris, 3 9 2010 RG n°08/12821.
13 CA Paris, 3-9-2010 RG n°08/12822.
14 TGI Créteil, 14-12-2010, n°06-12815.
15 Cass civ-1 7 2012 n° 11-15.165 et 11-15.188.
16 Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2010 p. 18, voir également le rapport de la CNIL « La cybersurveillance sur les lieux de travail
17 Fiche pratique CNIL Keylogger : dispositifs de cybersurveillance particulièrement intrusifs, 20 mars 2013.
18 CPCE art. L. 34-1 et R. 10-12 et suivants, concernant notamment la gestion des données de trafic par les opérateurs de communications électroniques et assimilés.
19 Décret n°2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.
20 CJUE C- 293/12 et C-594/12 du 8 3 2014 invalidant la directive 2006/24/CE sur la conservation des données de l'Union européenne.
21 Article 6 II de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication de données, modifié par le décret 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.
41 CPCE : l'article 32définit le réseau interne comme « tout réseau de communications électroniques entièrement établi sur une même propriété, sans emprunter ni le domaine public - y compris hertzien - ni une propriété tierce. »
42 CPCE, art ; D98.
55 CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005
56 Décret modifié par le Décret n°2014-1576 du 24 12 2014
57 CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005
58 Article 223-2-1 du Code Pénal
59 TGI Paris 20-4-2005, ordonnance de référé UEJF et a. c/ olm llc et a.
63 Code pénal, art. 227-23 et 227-28-1
64 CE 26 juill. 1918, Épx Lemonnier
65 Dalloz encyclopédie « Répertoire de la responsabilité de la puissance publique -Faute des agents et responsabilité administrative » – Jean-Pierre DUBOIS – avril 2014
66 CE 18 nov. 1949, Demoiselle Mimeur, Lebon 492 ; JCP 1950. II. 5286, concl. Gazier)..

Conseil Général du Cantal

Le Conseil Général du Cantal utilise Websense pour se protéger contre les menaces informatiques sur Internet.

community.websense.com - Jean-Philippe Lavigne / 19/01/2011.

“L’architecture des solutions Websense constitue un avantage majeur au regard de notre activité propre. Elle assure la protection proactive de notre système et permet à nos agents de bénéficier des ressources et de la latitude qui leur sont indispensables pour réaliser leurs missions”

Description

L’administration départementale du Cantal, qui compte 150 000 habitants, s’évertue quotidiennement à renforcer la solidarité locale. Le Conseil Général du Cantal a la charge d’assurer la cohésion sociale et territoriale dans un environnement complexe alliant faible densité de population et vaste couverture géographique. Le Conseil Général est confronté à la fois à l’extension de ses responsabilités et à la diversification des tâches qui lui sont confiées. La direction informatique du Conseil Général du Cantal a un rôle essentiel à jouer à cet égard : elle doit permettre aux 1 200 agents territoriaux d’accomplir leurs missions et d’accéder aux informations dont ils ont besoin sur le Web tout en assurant la sécurité du système. Elle doit offrir un appui et un soutien efficaces aux agents, qu’ils travaillent dans l’un des 50 sites territoriaux ou qu’ils soient en mission sur le terrain.

Le défi

Face à l’évolution constante des menaces informatiques et des méthodes de travail, le Conseil Général se trouve confronté à des difficultés spécifiques que les solutions de sécurité classiques ne sont pas en mesure d’aborder, comme les problèmes liés à l’analyse des sites web dynamiques, à la configuration personnalisée à distance, au manque de transparence et de clarté de la console d’administration, etc. En définitive, ces difficultés ralentissent le système et limitent la productivité des agents.
Pour relever ces défis, le Conseil Général a choisi une solution évolutive plus complète : Web Security Gateway de Websense. Les critères décisifs qui ont justifié la sélection de la solution Websense ont été à la fois la réactivité et la qualité de service du support technique de la société, ainsi que les capacités propres et l’extensibilité du produit.

Les menaces informatiques sont en expansion et en évolution constante avec l’adoption par les utilisateurs de nouveaux comportements tels que les réseaux sociaux ou l’utilisation de smartphones et d’ordinateurs portables. Les systèmes assurant la sécurité d’accès à Internet doivent anticiper les actes de malveillance et se centrer sur la classification contextuelle pour les mettre en défaut. L’architecture des solutions Websense constitue un avantage majeur au regard de notre activité propre. Elle assure la protection proactive de notre système et permet à nos agents de bénéficier des ressources et de la latitude qui leur sont indispensables pour réaliser leurs missions. La prévention des fuites d’information est une préoccupation centrale en raison de la quantité de données personnelles sensibles gérée par nos agents, et elle ne va pas sans une prise de conscience renforcée des utilisateurs, » souligne Jean-Philippe Lavigne, chef d’exploitation à la direction informatique du Conseil Général du Cantal.

La solution

Au vu du large éventail des missions du Conseil Général, certains agents doivent remplir plusieurs fonctions avec des critères d’accès différents à Internet. Cette diversité des rôles impartis aux différents utilisateurs, ou même à un utilisateur spécifique dans certains cas, nécessite la mise en oeuvre d’un système de gestion des règles simplifié basé sur la notion de rôles et offrant des capacités de contrôle à distance. La solution Web Security Gateway de Websense analyse et sécurise automatiquement le trafic web en temps réel en classant instantanément les nouveaux sites et le contenu dynamiquement. Elle identifie de façon proactive les nouveaux risques pour la sécurité et protège le système contre les logiciels malveillants et les attaques combinées ; elle permet aussi une utilisation en toute sécurité du Web 2.0 sur la base de rôles utilisateur. La solution permet aux utilisateurs de bénéficier d’un accès Internet ciblé en fonction de leurs besoins, qu’ils soient au bureau ou en déplacement. Elle associe une sécurité renforcée et des capacités de gestion de règles hautement intuitives, sans oublier un outil de suivi et de génération de rapports.

Le Conseil Général du Cantal peut utiliser la console d'administration centrale pour configurer à distance les stations de travail et déléguer les tâches d'administration. La configuration simplifiée, centralisée et ciblée permet d'assurer une gestion transparente et, au final, d'optimiser l'accès à Internet et de sécuriser l'accès du Web.

Jean-Philippe Lavigne ajoute : Les services de support technique de Websense nous sont d'une aide précieuse dans le cadre du travail quotidien, notamment en raison de leur fiabilité et de leur disponibilité. Ils nous ont apporté une assistance sans faille pour mettre à niveau notre architecture, mettre en place un système cohérent et répondre aux demandes de modification et de personnalisation de la solution pour satisfaire à nos besoins spécifiques en constante évolution.

La Mairie de Mérignac réduit ses coûts de connexion Internet grâce à la solution de filtrage d'Olfeo.

www.olfeo.com / 06/09/2012.

Paris, le 6 septembre 2012 - Au coeur de l'agglomération bordelaise, Mérignac est une ville incontournable dans le rayonnement économique de la région. Premier Pôle économique et commercial d'Aquitaine, elle représente un important bassin d'emplois et une opportunité pour tous. Mérignac sait aussi être innovante. Grâce à sa diversité économique, elle brasse des industries de Haute Technologie. De l'aéronautique à la recherche en Médecine.
Mérignac est la 2ème ville de Gironde et la 3ème ville d'Aquitaine avec 17 572 familles et 66 916 habitants recensés au 1er janvier 2007.

La Mairie de Mérignac compte 1500 employés répartis sur 35 sites distants (Hôtel de Ville, Médiathèque, Crèches, Stades et salles de sport…).
La Mairie de Mérignac dispose de 700 postes utilisateurs avec un accès Internet pour les employés de la Mairie, et certains de ces postes offrent un accès Internet public, pour les usagers de la Médiathèque notamment.

Problématique

Jusqu'en 2004, dans le cadre d'une politique de protection des utilisateurs et du système d'information, la Mairie de Mérignac, qui disposait à l'époque d'une connexion Internet avec 2 méga de débit, ne permettait pas à ses employés de travailler, ni de se connecter sur Internet. Ainsi, la Mairie de Mérignac souhaitait éviter les virus et l'accès de ses utilisateurs à des sites illicites ou potentiellement dangereux pour la sécurité du système d'information.
Consciente de l'intérêt et des multiples possibilités offertes par Internet, la Mairie de Mérignac a souhaité donner l'accès à Internet à ses employés, sous certaines conditions, et notamment sans augmenter ses coûts de connexion.

Mise en oeuvre

A la fin de l'année 2004, la Mairie de Mérignac a lancé une consultation et sélectionné plusieurs solutions de filtrage afin de réaliser des tests pendant 2 mois environ. Après cette période de tests, la Mairie de Mérignac, à l'aide de l'intégrateur, a retenu la solution d'Olfeo, qui s'est révélée la plus appropriée par rapport à ses besoins.

Au cours du 1er trimestre 2005, la solution d'Olfeo a été paramétrée et installée. En parallèle, l'intégrateur a formé les équipes de la DSI de la Mairie de Mérignac à l'utilisation de la solution.

« *Notre choix s'est porté sur Olfeo pour la pertinence des catégories par rapport à la loi française et pour la relation de proximité que nous avons tout de suite pu établir avec un éditeur à taille humaine* » complète **Vincent Legallais, chargé de projet à la DSI de la Mairie de Mérignac.**

Lors de la mise en place de la solution Olfeo, la DSI de la Mairie de Mérignac s'est rapprochée de chaque direction avec les statistiques des catégories des sites les plus consultés par chacune des équipes. Chaque direction a ensuite validé les catégories de sites qui pouvaient être consultés et ceux que la DSI devait bloquer. Pour les sites à caractère personnel mais autorisés, un système de plage horaire a été mis en place, ce qui permet un accès Internet plus ouvert avant 8h30, entre 12h et 14h puis après 18h30, selon un quota de deux heures par semaine.

« *Comme toute solution qui veille à réguler, voire interdire quelque chose, nous avons du présenter les avantages de la solution Olfeo à chaque direction, qui ont elle-même du faire face aux interrogations des utilisateurs en leur apportant des réponses concrètes, notamment par rapport à leurs besoins*

de se connecter à tel ou tel site » explique **Vincent Legallais, chargé de projet à la DSI de la Mairie de Mérignac.**

Aujourd'hui, la Mairie de Mérignac utilise l'ensemble des modules de la solution de filtrage d'Olfeo : le filtrage url, le filtrage protocolaire, l'anti-virus et le proxy cache, dans sa dernière version logicielle pour l'accès Internet de tous les employés et pour l'accès public offert par la Médiathèque, grâce à la mise à disposition d'ordinateurs.

Bénéfices

La solution de filtrage d'Olfeo permet à la Mairie de Mérignac de contrôler l'utilisation d'Internet par ses employés et d'être en conformité avec la loi en interdisant la consultation des sites illicites.
La simplicité de mise en oeuvre et de paramétrage permet également à la Mairie de Mérignac de personnaliser les catégories de sites interdits et autorisés pour chaque direction, selon leur métier et leurs besoins.

« *La solution Olfeo a énormément évoluée depuis que nous avons commencé à l'utiliser. Aujourd'hui, nous apprécions particulièrement la disponibilité et la réactivité du support, surtout lorsque nous détectons un site mal classé ou pas classé : Olfeo analyse et propose un reclassement très rapide, dans les 15 minutes* » commente **Vincent Legallais, chargé de projet à la DSI de la Mairie de Mérignac.**

Mais la solution d'Olfeo a surtout permis à la Mairie de Mérignac d'optimiser ses besoins en bande passante et même de réduire ses coûts de connexion Internet. Bénéficiant aujourd'hui d'un débit de 6 mégas et en autorisant l'accès qu'à une liste de sites autorisés, le trafic et les connexions ne sont jamais saturés ni même ralentis.

Grâce à Olfeo, la Mairie de Mérignac a également pu mettre en place une politique d'utilisation d'Internet globale pour l'ensemble de ses employés, avec une charte Internet incluant la politique de filtrage.

Jusqu'à présent, les écoles disposent de leur propre outil de filtrage mais la Mairie de Mérignac étudie actuellement l'intégration des écoles dans sa politique de filtrage globale.

A propos d'Olfeo :

Olfeo, éditeur français d'une solution de proxy et de filtrage de contenus Internet est une société indépendante basée à Paris et Bordeaux. Créée en 2003, l'entreprise développe une solution adaptée aux besoins des entreprises et des administrations françaises grâce à une approche innovante basée sur la proximité culturelle. L'entreprise garantit ainsi à ses clients une protection juridique optimale (grâce à une collaboration étroite avec Maître Eric Barbry, avocat au barreau de Paris et directeur du pôle « Droit du numérique » du cabinet Alain Bensoussan*), une qualité de filtrage inégalée, une haute sécurité du système d'information et l'association des utilisateurs à la politique de sécurité.
La solution Olfeo permet de maitriser l'ensemble des accès et l'utilisation d'Internet en entreprise grâce à une suite de 5 produits complémentaires : le Filtrage d'url, le Filtrage protocolaire, le Proxy cache QoS, l'Antivirus de flux, et le Portail public. Grâce à sa console d'administration unique, Olfeo dispose d'une grande richesse fonctionnelle et d'une administration simplifiée. Disponible sous format appliance, virtualisée, logicielle et Saas, la solution s'intègre facilement aux architectures existantes.
Olfeo compte actuellement plus de 1.000 clients satisfaits, représentant plus de 2 millions d'utilisateurs.

DOCUMENT N°08

Sept critères pour l'évaluation de la sécurité Web et de la messagerie en mode SaaS.

www.itrnews.com - Florent Fortuné (websence.com) / 28/12/2010.

De nombreuses entreprises sont déjà conscientes des avantages d'une solution en mode SaaS. Cependant, quelques-unes résistent encore à l'idée d'externaliser leurs besoins en sécurité Web et de messagerie.

Avant toute décision, il est primordial d'évaluer l'efficacité d'un fournisseur de solutions en mode SaaS à traiter des critères clés et sa capacité à offrir une alternative a une solution de sécurité locale qui soit réellement attractive. Les décideurs sont en général les plus préoccupes et ont souvent des idées fausses. Observons la manière dont le modèle SaaS répond à ces préoccupations :

1. Fiabilité : la responsabilité commence ici

Ne pas se sentir en mesure de remédier aux interruptions de service non planifiées contrarie les responsables informatiques bien plus que ces interruptions elles-mêmes. Et ceci explique, en un mot, pourquoi tant d'entreprises sont si peu disposées à faire confiance à un fournisseur de solutions en mode SaaS. Si le service offert par ce fournisseur devient indisponible, elles peuvent se retrouver hors-jeu et sans protection. Leurs messages n'arriveront pas ou peut-être qu'ils arriveront en lots de spams, de programmes malveillants et d'attaques de phishing. Une telle défaillance pourrait rapidement submerger les serveurs de messagerie locaux d'une entreprise ainsi que son infrastructure réseau et ouvrir la voie à une foule de menaces de securite Web et de risques de perte de données internes.

Minimiser ces risques ne suffit pas : une solution efficace en mode SaaS doit les éliminer. Afin d'y parvenir, l'infrastructure de datacenter d'un fournisseur de solutions en mode SaaS doit être : dispersée géographiquement et redondante ; physiquement sécurisée et conçue pour une efficacité optimale.

2. Efficacité : protection contre les menaces actuelles

Les solutions classiques de securite Web et de messagerie sont très efficaces lorsqu'elles répondent à des menaces connues. Cependant, les menaces connues ne représentent aujourd'hui que le haut de l'iceberg. Une avalanche de menaces < *zéro hour* >, notamment de nouvelles variantes de code malveillant et des sites Web compromis par du code malveillant, submergent rapidement les solutions logicielles ne disposant que de mises à jour périodiques de leurs définitions d'antivirus ou de leurs bases de données d'URL.

Les solutions de sécurité Web et de messagerie réellement efficaces offrent une sécurité du contenu unifiée. Cela signifie qu'elles répondent a un environnement fait de menaces en temps réel avec des outils de détection et d'évaluation de ces menaces en temps réel ainsi que des fonctionnalités de prévention contre la perte de données (DLP). Elles peuvent également offrir une plate-forme unifiée, avec gestion unifiée, de plates-formes en local et en mode SaaS pour pouvoir appliquer et faire respecter uniformément les politiques de sécurité au sein des entreprises reparties.

3. Performances : les optimiser

Les préoccupations liées à la fiabilité du mode SaaS peuvent s'étendre aux perceptions d'une entreprise de la qualité des performances d'Internet, ou son manque de performances. Pourquoi un responsable informatique devrait-il amplifier les inquiétudes existantes de son entreprise en termes de latence réseau et de bande passante en routant le trafic Web et de la messagerie via un Datacenter tiers ? La réponse est simple : migrer la sécurité vers le Cloud peut en réalité optimiser les performances et la capacité à faire évoluer une solution de sécurité a la demande.

Prenez tout d'abord en considération le fait que le trafic SMTP peut consommer jusqu'a un tiers de la bande passante Internet totale d'une entreprise et le fait qu'environ 90 % de ce trafic est constitue de spams. Gardez également en tète que la croissance temporaire du trafic spam peut entrainer l'utilisation de la bande passante d'une entreprise a un niveau exceptionnel et même mettre a terre un réseau.

A ce stade, router le trafic Web et celui de la messagerie via une solution en mode SaaS commence à devenir extrêmement logique, en particulier via des solutions offrant haute fiabilité et hautes performances. Le trafic de spam, de code malveillant, et le trafic Web indésirable n'atteignent jamais le réseau local d'une entreprise et n'influent pas sur l'intégrité de son réseau ou de sa bande passante.

4. Flexibilité : développer votre solution actuelle
Même lorsque les entreprises sont favorables au mode SaaS, elles peuvent avoir tendance à éviter toute décision pouvant influencer leurs solutions locales plus tôt que prévu. Les entreprises souhaitent exploiter jusqu'au dernier euro de leurs dépenses d'investissement en informatique actuelles, ce qui est compréhensible. Cependant, une solution de sécurité basée sur une plate-forme en mode SaaS ne doit pas nécessairement remplacer une solution locale. Une solution hybride, telle que l'ajout de sécurité de la messagerie en mode SaaS a une mise en ouvre en local, peut engendrer des bénéfices comme le déchargement du traitement, la réduction de la bande passante et la protection contre la croissance du trafic, éliminant ainsi le besoin de remplacer ou d'augmenter les serveurs de messagerie locaux en raison de pics de croissance du trafic des emails indésirables.

Les entreprises doivent également prendre en considération le fait que les solutions en mode SaaS peuvent compléter les solutions locales de sécurité Web et de la messagerie de nombreuses autres manières. Tout d'abord, en raison de la tendance quasiment universelle envers un effectif reparti ou nomade, les solutions en mode SaaS peuvent intervenir et combler le fosse en termes de couverture laisse par les solutions locales. Ensuite, de nombreuses entreprises exploitent actuellement des produits de sécurité en local ne disposant pas de fonctionnalités clés. Une solution en mode SaaS complète peut apporter les pièces manquantes au puzzle de la sécurité ou offrir une transition fluide vers une suite intégrée de produits de sécurité.

5. Contrôle : vous fixez les règles
Lorsqu'il est question de plate-forme de sécurité en mode SaaS, les inquiétudes concernant < la perte de contrôle > se résument en général a deux préoccupations : les performances et la facilite de gestion. Les performances d'une solution en mode SaaS dépendent en majeure partie de l'infrastructure de Datacenter d'un fournisseur et de sa capacité à traduire ses promesses en termes d'infrastructure par un contrat de niveau de service pertinent.

En ce qui concerne la facilite de gestion, une entreprise gagnera à choisir une solution en mode SaaS offrant des outils d'administration, une accessibilité et une intégration, une facilite d'utilisation et des fonctionnalités de reporting, pour ne pas dépendre d'un tiers.

6. Confidentialité et sécurité : le mode SaaS sait préserver le secret
Une autre préoccupation majeure concerne l'exposition de données sensibles par le fournisseur a des utilisateurs non autorises ou le fait que le système du fournisseur devienne la proie d'attaques qu'il est censé prévenir. L'une des meilleures manières d'évaluer les mesures de sécurité et de confidentialité d'un fournisseur de solutions en mode SaaS consiste à utiliser des procédures de certification tierces. La certification peut-être la plus pertinente ISO 27001, est conçue spécialement pour < *délivrer un modèle permettant d'établir, de mettre en ouvre, d'utiliser, de surveiller, d'analyser, de gérer et d'optimiser un système de gestion de la sécurité des informations.* >
Ce processus rigoureux de certification est axe sur de nombreuses exigences clés, notamment :

- L'utilisation des meilleures pratiques pour garantir la confidentialité, l'intégrité et la disponibilité des données clients.
- La volonté d'un fournisseur de soumettre son Datacenter et les activités associées a des audits de certification périodiques.

Un fournisseur de solutions en mode SaaS devrait également imposer des normes de protection de la sécurité physique de ses Datacenter, couvrant notamment le personnel en continu, le contrôle d'accès et des systèmes de supervision multicouches. Il devrait également soumettre ses installations à des tests de vulnérabilité réguliers, de préférence de concert avec un organisme d'audit de sécurité tiers. Le processus d'évaluation des mesures de sécurité et de confidentialité d'un fournisseur de solutions en mode SaaS ne devrait jamais faire l'objet d'une confiance aveugle !

7. Couts : un avantage majeur de la plate-forme en mode SaaS
Les solutions en mode SaaS peuvent réduire de manière significative le cout total de possession. Avec une solution en mode SaaS, les entreprises peuvent réduire leurs couts en éliminant les taches liées a la distribution, au déploiement et a la mise a jour permanente du matériel local. En outre, aucun système d'alimentation ni de refroidissement n'est requis. Les couts en bande passante sont réduits et la tolérance aux années intégrée élimine d'avantage le besoin en serveurs supplémentaires. Les couts salariaux sont également allégés : au lieu d'investir dans la formation, l'installation, la gestion et la maintenance permanente, les couts salariaux liés à une solution en mode SaaS se concentrent sur la formation minimale du personnel et des fonctions administratives.