JDN
l'économie demain

Chronique de Vincent Nicaise
Chef produit, Zyxel

Hadopi, le casse-tête de la mise en conformité pour les entreprises

Si le sort des particuliers a largement été évoqué l'an dernier, il faut aussi garder à l'esprit que les entreprises devront, elles aussi, se conformer à la nouvelle contrainte législative.
Votée fin 2009, la loi Hadopi ne cesse de défrayer la chronique. Après de nombreux rebondissements, nous devrions finalement voir les premières sanctions tomber courant avril 2010. Son objectif est simple : protéger les droits d'auteurs et sanctionner le téléchargement illégal. Si le sort des particuliers a largement été évoqué l'an dernier, il faut aussi garder à l'esprit que les entreprises devront, elles aussi, se conformer à cette nouvelle contrainte législative. D'où les inquiétudes des chefs d'entreprise : quelles sont les mesures et choix techniques à privilégier ? Comment faire pour que la mise en conformité ne devienne un gouffre financier ? La technologie est-elle capable de tout résoudre ?

Le chef d'entreprise est aujourd'hui tenu d'empêcher toute utilisation illicite de l'accès Internet de la société. Bien que la riposte graduée ne soit pas imposée aux entreprises, celles «contrôlées positivement» (en flagrant délit d'utilisation illégale d'Internet) recevront une injonction de pallier le manquement constaté en mettant en place des solutions de filtrage ou des pare-feu. Elles devront en rendre compte dans le délai déterminé par l'injonction. Il est aussi important de rappeler que la loi Hadopi sanctionne les propriétaires de la ligne, même si celle-ci a été piratée par un tiers, et si l'entreprise ne s'est pas donnée les moyens de surveiller et de sécuriser sa connexion. Le propriétaire risque une coupure de la ligne pendant une période de 1 à 3 mois, une amende de 300 000 euros et une peine de 3 ans de prison pour contrefaçon.

Autrement dit, pour être en conformité avec la loi Hadopi, le recours à des outils de sécurité spécifiques s'impose. En effet, nombreuses sont les entreprises, et plus particulièrement les TPE et les PME, qui n'ont aucune idée de la manière dont leurs salariés utilisent la connexion Internet de l'entreprise. Les récents sondages révèlent que les salariés français surfent en moyenne une heure et demie par jour au bureau, essentiellement pour un usage personnel. On peut également anticiper une augmentation de l'usage illégal d'Internet au sein de l'entreprise puisqu'il deviendra risqué pour l'internaute de s'adonner à ce type de pratique depuis son domicile. Le sentiment d'anonymat au sein de son entreprise pourrait l'encourager à poursuivre cette activité depuis son lieu de travail.

Dans ce contexte, l'intégration d'une solution de sécurité unifiée qui mutualise un pare-feu avec les applications spécifiques de type «UTM» peut s'avérer un choix judicieux pour combiner : protection du réseau, interconnexions de sites, accès à distance, haute-disponibilité, filtrage de contenus, anti-virus ainsi que détection et prévention d'intrusions.

En effet, le premier rempart au téléchargement illégal se fait traditionnellement par l'analyse des types de fichiers qui transitent vers le réseau d'entreprise. Cette analyse est réalisée avec l'aide d'un antivirus configuré pour détecter et interdire, par exemple, le téléchargement des fichiers avec une extension .mp3 ou .avi. Cependant, force est de reconnaître le caractère imparfait de cette méthode utilisée seule notamment pour les internautes avertis.

Gageons toutefois que l'antivirus sur le pare-feu évitera la propagation de virus au sein de l'entreprise et effectuera un premier niveau de protection, notamment pour les utilisateurs les moins aguerris.

De plus, la mise en conformité avec la loi Hadopi impose de facto d'empêcher l'utilisation des logiciels de Peer-to-Peer, tels qu'Emule, Bit Torrent, etc. qu'il est fréquent de voir installés sur des ordinateurs de bureau. Bloquer ce type d'applications grâce à une licence de détection et de prévention d'intrusions installée sur le pare-feu s'avère la façon la plus efficace de lutter contre le téléchargement illégal. Bloquer ces sites de téléchargement libèrera également de la bande passante et améliorera par la même grandement la qualité de la connexion Internet, et donc le confort de travail des salariés. Un conseil : préférez une solution qui analyse les trames plutôt qu'un simple outil de blocage de ports facilement contournable par un utilisateur aguerri.

Mais, ce n'est aujourd'hui pas suffisant car les pratiques de piratage ont évolué. Ainsi, d'autres sources telles que le streaming, dont certains sites sont devenus plus populaires que les réseaux Peer-to-Peer, et le téléchargement sur des sites d'hébergement de fichiers (sites de torrents, newsgroups ou encore blogs musicaux, etc.) doivent également être contrôlées. Celles-ci peuvent être bloquées directement par un service de filtrage de contenus installé sur le pare-feu en choisissant parmi des catégories de sites (peer-to-peer, blogs, newsgroup ; streaming, media/mp3...). Les catégories sont, bien entendu, mises à jour très régulièrement de manière à prendre en compte tous les nouveaux sites qui fleurissent sur le net chaque jour.

Ce type de solution flexible offre aussi l'avantage de pouvoir s'adapter aux besoins des entreprises en activant ces fonctionnalités par service ou sur certains ordinateurs de l'entreprise ou encore à certaines heures de la journée. En outre, une des dernières tendances des sites de streaming vidéo est de mettre en place une liaison cryptée sécurisée pour diffuser des films ou des séries télévisées : celle-là même qu'utilisent les sites de consultation bancaire. La solution par filtrage de contenus devient ici inopérante puisqu'elle ne pourra contrôler les flux cryptés qui transitent. Dans ce cas, il est recommandé de paramétrer le pare-feu afin de bloquer ce protocole pour les employés qui ne sont pas amenés à avoir un accès à ce type de site (on peut l'autoriser par exemple pour le service financier).

En parallèle, un logiciel de reporting peut être utilisé pour analyser les flux du réseau qui transitent à travers le pare-feu. Grâce à cet outil, il est possible de connaître la bande passante utilisée, d'effectuer une analyse des habitudes de surf non nominative et ainsi appliquer les règles de filtrage les plus adaptées à l'entreprise.

Enfin, cet outil ne saurait être parfaitement efficace sans une charte informatique qui définit les droits, devoirs et responsabilités des employés quant à l'utilisation des outils informatiques mis à disposition par l'entreprise. La charte informatique doit avant tout être intégrée dans le règlement intérieur de l'entreprise et communiquée aux employés, au comité d'entreprise et à l'inspection du travail. Elle devra, de plus, être consultable par tous les employés. Selon la CNIL, cette charte doit inviter les employés «à un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité». La communication et l'explication sont les maîtres mots pour responsabiliser les salariés.

Ainsi, l'enjeu de la loi Hadopi pour les entreprises consiste bien à contrôler l'accès Internet afin de ne pas engager la responsabilité de l'employeur et de ne pas subir les risques qui pourraient frapper l'entreprise contrevenante.

La solution technique apportée par la mise en place d'un pare-feu unifié de type UTM (avec les services antivirus, filtrage de contenus, de détection et de prévention d'intrusions, paramétrés en fonction de la typologie, de l'organisation et des besoins de l'entreprise), couplée à une charte informatique claire et comprise dans son sens par les salariés s'avère être une réponse adaptée à la loi Hadopi. Le chef d'entreprise pourrait faire évoluer la contrainte que représente la mise en conformité à la loi Hadopi en opportunité pour améliorer la qualité de la connexion Internet ainsi que le confort de travail des employés, et in fine optimiser la productivité de l'entreprise, atout clef pour toutes celles qui, dans un contexte économique difficile, souhaitent tirer leur épingle du jeu.