CONCOURS INTERNE DE TECHNICIEN TERRITORIAL - SESSION 2016

Spécialité «INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION»

ÉPREUVE DE RAPPORT

NOTE OBTENUE : 14.5 / 20

Mairie de Techniville
Service informatique

le 14/04/2016

RAPPORT : Mise en œuvre d'un système de filtrage
A l'attention du Directeur des Systèmes d'information

Dans un contexte où les menaces informatiques ne cessent d'attaquer les réseaux internet et bien qu'il soit difficile de contrôler entièrement l'accès internet au sein d'une administration, il convient de mettre en place un système de filtrage des contenus web autorisés. Après avoir listé les enjeux d'un système de filtrage, il sera défini la mise en œuvre d'une nouvelle politique de filtrage.

I Les enjeux d'un système de filtrage

1) Pourquoi mettre en place un tel système ?

La mise en place d'un système de filtrage des contenus web autorisés est nécessaire pour la lutte contre les contenus abusifs. En effet, certains sites peuvent causés des dommages qu'il convient d'éradiquer, tels que les sites prônant la pédopornographie, le terrorisme, les jeux de hasard…

Il est aussi obligatoire de protéger la propriété intellectuelle, les droits d'auteur, des contenus hébergés par certains sites.

Un système de filtrage permet aussi en limitant les accès à certains sites, chat ou réseaux sociaux, de sécuriser le réseau informatique local et les données sensibles des usagers traitées par les services de l'administration. Ainsi cela éviterait, ou du moins limiterait, les menaces informatiques, telles que les ransomware par exemple, qui crypte l'accès aux machines ou documents.

Enfin cela augmenterait la productivité des agents qui perdraient moins de temps à consulter des sites d'un point de vue personnelle.

2) Quels sont les risques engagés ?

De nombreux textes de loi régissent l'obligation de filtrage, et notamment les lois HADOPI, le droit européen, ainsi que la jurisprudence. Ainsi toutes entreprises ou administration, dont le siège est situé en France est dans l'obligation de mettre en place un système de filtrage pour restreindre l'accès à Internet et conserver les données d'identification.

L'administration en tant qu'abonné d'un fournisseur internet, devient ainsi fournisseur d'accès pour l'ensemble de ses employés. Ainsi la responsabilité civile et pénale est engagée, dès lors que l'un de ses agents exerce des activités illicites en lien avec une connexion internet sur son lieu de travail, même s'il est prouvé que celui-ci a agit en dehors de ses fonctions et sans autorisation.

II La mise en œuvre d'un système de filtrage :

1) Bien définir sa politique de filtrage :

Afin d'élaborer une architecture de filtrage, l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) met à disposition une note technique pour venir en aide aux personnes qui souhaitent mettre en place un système de filtrage.

Dans le but de ne pas nuire aux libertés des agents de la collectivité, il est nécessaire de consulter le Comité technique paritaire avant le démarrage du projet. Cela permettra de tenir informer et de consulter l'ensemble des agents, pour connaître leurs besoins professionnels en matière de connexion internet, et ainsi éviter de nuire à leur productivité.

Lorsque la politique à mettre en œuvre sera adoptée, une déclaration à la CNIL devra être déposée contenant l'ensemble des dispositions de filtrage qui sera mise en place.

2) Mise en œuvre d'une solution de filtrage

Il est tout d'abord nécessaire de bien choisir l'éditeur de la solution. En effet, il convient de vérifier que la solution soit souple, que le paramétrage du filtrage puisse être affiné correctement pour ne pas nuire à la productivité des agents. Ils doivent pouvoir avoir accès aux sites nécessaires à leurs tâches professionnelles. Le paramétrage doit pouvoir se faire selon des profils utilisateurs afin qu'il soit le plus juste possible et s'administrer à distance. La solution doit aussi pouvoir s'appliquer sur le réseau local mais aussi sur les machines des agents en déplacement. La solution doit donc être souple pour répondre aux besoins spécifiques en constante évolution.

Il faudra de plus apporter une attention particulière à la réactivité et à la qualité du service rendu par l'éditeur afin de pouvoir bloquer ou débloquer un site mal classé.

En tout état de cause, une fois des solutions sélectionnées, il sera nécessaire de procéder à une phase de test des différentes solutions ainsi le filtrage pourra être affiné, la rapidité du réseau sera testé et la solution la plus performante et adaptée pourra être choisie.

Lorsque l'éditeur sera choisi, il conviendra de rédiger une charte informatique régissant notamment la politique de filtrage, les droits d'accès, les droits de rectification des accès et le droit d'opposition des agents. Cette charte sera alors soumis à validation du Comité technique paritaire pour être diffusée à l'ensemble des agents de la collectivité.

Enfin il sera nécessaire de former les agents du service informatique qui seront chargés de mettre en place la solution et de la paramétrer.

Par conséquent, une politique de filtrage doit être mise en place dans un soucis de sécurisation du réseau informatique et des données hebergées ou consultées, la responsabilité civile et pénale de l'administration étant engagée. Il conviendra de sélectionner la solution la plus adaptée aux besoins de nos services, sans favoriser la solution la plus économique qui serait sûrement plus contraignante. Enfin l'information des utilisateurs de ce système est nécessaire et obligatoire pour le bon fonctionnement de nos services.