Sécurité : les 3 rôles du proxy (avis d'expert)

L'ouverture du système d'information implique pour les entreprises des **contraintes sécuritaires et juridiques nouvelles** qui doivent permettre de sanctionner toute forme d'abus sans porter atteinte aux droits de leurs employés.

Juridiquement, l'entreprise doit en effet se positionner face à des comportements liés aux menaces internes : le **téléchargement de contenus musicaux et/ou pédophiles**, et le **téléchargement de contenus avec un ordinateur appartenant à l'entreprise**. Celle-ci doit aussi faire face aux menaces externes via l'infection malicieuse (virus) et la fuite d'information (documents confidentiels, bases de données).

L'administrateur doit donc être en mesure de **différencier les sites à risques pour l'utilisateur** et par conséquence pour l'entreprise, et veiller aux transferts de contenus illicites car l'objectif des pirates est clairement défini : inciter les utilisateurs à se connecter sur un site infecté via des liens corrompus ou des scripts intégrés (Malware, Drive-by-Download, Phishing, Pharming, Spam, Botnet…) pour récupérer des informations « monnayables » (Spyware, Trojan…).

Les rôles du proxy

1) Le proxy permet de répondre en partie à ces problématiques en assurant une **première barrière de protection avec des fonctionnalités de filtrage** avancé des URL via des politiques de blocage des sites web corrompus connus. L'ensemble des sites est ainsi regroupé par classes pour permettre aux entreprises de bloquer les sites malveillants aux contenus dangereux.

2) Le proxy permet également de déchiffrer le flux SSL pour certaines catégories de sites au travers d'une technologie de type « *Man in the Middle* » embarquée sans ajout de ressources additionnelles. Cela permet d'avoir **de la visibilité sur les flux SSL** et de bloquer les sites web inappropriés qui communiquent via le protocole SSL.

3) Étant donné que les cybercriminels se basent souvent sur des malwares construits via l'utilisation de kits (donc faciles à implémenter), les **moteurs anti-malwares** peuvent donc être très utiles dans la configuration du proxy pour contrer en temps réel les menaces. Il est cependant possible de déjouer cela via certaines techniques de compression et de cryptage. Mais, là encore, le proxy prouve son efficacité en limitant l'accès aux sites à risque.

Du proxy à la responsabilité

Au-delà de la configuration, il est important de bien **identifier les problèmes remontés**, via des modules d'analyse regroupant des fonctions innovantes et évoluées pour la création de rapports sur les activités Internet et l'ensemble des risques qui sont liés à l'utilisation quotidienne des employés. Cela permet de mettre en place une vraie politique de reporting avec une vision claire des sites à risque.

Toutes ces mesures permettent de limiter les risques liés à l'utilisation d'Internet en entreprise.

Mais, au-delà de la technologie, il est important d'adopter une politique de sécurité permettant de comprendre et d'identifier les dangers pour que l'employé en prenne lui-même conscience. Adopter les bons gestes et responsabiliser l'ensemble des acteurs afin de se protéger juridiquement devient le maître mot de la sécurité en entreprise.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes