

COMMUNIQUÉ

Quatre jours pour doper son site Web

Ergonomie, enquêtes en ligne, accessibilité, gestion de contenus : les clés pour faire de son site un dispositif efficace. Séminaires Benchmark Group du 7 au 10 novembre.

Simplifier ses tâches d'exploitation avec l'anti-spam hébergé

[« En savoir plus](#)
[Les solutions du marché »](#)

La fourniture d'applications hébergées s'étend au domaine de la sécurité et en particulier aux anti-spam. Gestion de la mise en quarantaine, techniques d'analyse et d'authentification sont notamment à surveiller de près.

En matière de spam, les entreprises peuvent bien sûr implanter des outils de filtrage dans leur système d'information (*lire l'article du 19/07/2006 : [Armer ses passerelles et serveurs de messagerie contre le spam](#)*) mais aussi **recourir à des offres hébergées** (modèle ASP pour *Application Service provider*).

Dans ce dernier cas, elles peuvent se tourner soit vers les **éditeurs "traditionnels" de sécurité** proposant un service hébergé (Symantec, Secure Computing...) ou bien vers un **pure player ASP** (MailInBlack, Oktey...).

L'atout principal des offres hébergées ? Il réside dans les **"gains d'exploitation et de disponibilité**, ne nécessitant pas d'internaliser ses relais de messagerie SMTP" pour Nicolas Berchoux, responsable marketing au sein de DCI, intégrateur dans le domaine des solutions réseaux et sécurité.

Les critères de choix

- 1 Mise en quarantaine et espace de stockage alloué
- 2 Enregistrement DNS et authentification
- 3 Anti-virus intégré

La **mise en quarantaine** des e-mails suspects est gérée de façon automatique ou manuelle - l'établissement de listes blanches restant possible - et aboutit après **l'écoulement d'un laps de temps propre à chaque offre hébergée**, à la destruction du message. Il sera bien sûr possible d'augmenter cette durée, moyennant toutefois une facturation supplémentaire. De même, en cas de chute du serveur interne de messagerie, l'espace de stockage alloué par défaut pour chaque utilisateur variera en fonction des offres.

Parallèlement aux techniques anti-spam les plus fréquemment utilisées pour identifier un e-mail non sollicité (analyse lexicale, filtres bayésien, listes noires...), les offres hébergées peuvent également

s'appuyer sur **l'enregistrement DNS** (*Domain Name System*) et la technique de DNS inverse (Reverse DNS) pour **vérifier la correspondance entre l'adresse IP de l'expéditeur et son nom de domaine**. De même, pour assurer d'un taux de reconnaissance de 100% des spams, certaines solutions demandent à l'expéditeur d'un e-mail de s'authentifier pour s'assurer que l'e-mail ait bien été envoyé par un individu et non par un robot.

Les offres hébergées peuvent également être **adossées à un anti-virus** fourni soit gratuitement et par défaut, ou bien **en sus du service anti-spam**. En outre, les éditeurs et fournisseurs d'applications hébergées d'anti-spam proposent (dans une très large majorité) un support mail et téléphonique 24h/24 et 7j/7.

[« En savoir plus](#)

[En savoir plus](#)

[Les solutions du marché »](#)

Copyright 2006 Benchmark Group - 4, rue Diderot 92156 Suresnes Cedex, FRANCE

[Lancer l'impression](#)