MailinBlack veut protéger à 100% contre le spam

Souvent décriée depuis sa sortie, car accusée de radicaliser la lutte contre le 'spam' en interdisant toute latitude dans les choix de l'utilisateur, l'authentification de l'expéditeur s'impose aujourd'hui comme une solution pertinente et probablement la plus efficace.

Son principe se veut simple : l'expéditeur inconnu qui expédie un e-mail reçoit en retour un autre e-mail lui demandant de s'identifier. En l'absence de déclaration, l'e-mail original alors déclaré douteux est placé en quarantaine, ou détruit au bout d'une période définie si l'internaute n'a pas validé son expéditeur. Ce service exploite une faille chez les spammers, l'automatisation de leurs processus. Seuls des serveurs ont la capacité d'expédier des volumes d'e-mails, mais en contre partie, ils ne peuvent pas répondre à une demande d'authentification. Imparable? En revanche, à l'origine, ce type de solution ne laissait aucune latitude aux utilisateurs. Depuis, MailinBlack a adouci son approche. L'annuaire de l'utilisateur pré-autorise les expéditeurs dès l'installation. La réception d'e-mails en provenance de 'clients' de l'internaute est donc transparente. La demande d'authentification, en particulier, peut être personnalisée aux couleurs de l'entreprise ou de l'utilisateur. Important pour rassurer l'utilisateur et qualifier à la demande. Un nouvel expéditeur autorisé, pour une newsletter par exemple, peut être déclaré et donc franchir la barrière. Les messages placés en quarantaine ne sont pas perdus. Ils font l'objet d'un rapport quotidien. **Service en ligne ou appliance** Le premier niveau de service est proposé en ligne. Les serveurs de MailInBlack se substituent aux messageries de l'internaute, analysent les e-mails à la fois par leur authentification et par une détection virale, en partenariat avec BitDefender, puis expédient les e-mails autorisés au client. Parmi les clients de MailInBlack, des dizaines de milliers d'internautes, déçus par les solutions anti-spam des fournisseurs d'accès, ont adopté cette solution simple. Le second niveau est proposé en appliance, c'est-à-dire en produit indépendant qui vient compléter les messageries internes de l'entreprise. Les messageries pointent alors sur les appliances en s'installant sur les Dns. MailInBlack compte parmi ses clients appliance un partenaire de poids avec IBM, qui propose cette solution sur ses serveurs. Mais aussi de nombreux revendeurs. Une solution intermédiaire est proposée aux entreprises qui ne souhaitent pas implémenter d'appliance, mais recherchent une solution maîtrisée, sous la forme de serveurs mutualisés. **Sécuriser par l'authentification** Pour Régis Novi, le président de MailinBlack, « *les solutions de filtrage montrent leurs limites ! Les solutions présentées comme 'spam killer' n'ont pas fait leur preuve. Seule reste l'authentification comme solution efficace*« . Les grands comptes, intéressés par une politique sécuritaire très forte, adoptent volontiers la solution drastique d'authentification. Et pour les internautes, en général, la protection contre le spam est un vrai besoin. Ils sont donc demandeurs de solutions pour protéger leurs adresses. **MailInBlack face à ses concurrents**

MailInBlack annonce 100% de spam bloqué ! Seuls les e-mails en provenance d'expéditeurs autorisés ou capables de s'authentifier parviennent à l'internaute.

Les solutions concurrentes basées sur le filtrage affichent 80% à 90% de blocage. Pourquoi une telle différence ? L'authentification de l'origine de l'e-mail ne filtre pas, elle valide ! En revanche, les spammers s'efforcent en permanence de contourner les solutions de filtrage. De plus, le temps

d'administration des ces dernières est souvent long, et nécessite des ressources, toujours onéreuses et souvent ressenties comme une perte de temps. Enfin, l'une des problématiques les plus délicates dans la lutte contre le spam porte sur les faux positifs, ces e-mails légitimes qui se font malheureusement qualifier de spam par les systèmes anti-spam. Nouvel avantage pour l'authentification, aucun algorithme euristique, aucune liste, quelle soit blanche ou noire ! Les 'clients' sont soit pré-enregistrés, à l'aide des favoris par exemple, soit contrôlés sur les nouveaux contacts. En revanche, et c'est un paradoxe, l'un des avantages de la solution de l'authentification est à l'inverse la force des solutions concurrentes. L'authentification permet en effet de bloquer le spam sans regarder le contenu des e-mails. Et c'est pourtant l'un des arguments des solutions de filtrage, qui permettent de développer des outils autour du contenu, et d'appliquer des règles de gouvernance, comme le Sarbane Oxley Act. Cette capacité de gestion des messageries, droits d'accès, contrôle des sorties, stockage de l'information, etc., militent en faveur des solutions anti-spam basées sur le filtrage. Mais un taux d'échec de 10% à 20% dans le tri des e-mail n'est pas suffisant ! La solution 'idéale', pour peu qu'elle existe, ne serait-elle pas un mix entre l'authentification et le filtrage, avec l'efficacité de l'un et les capacités de gestion de l'autre ?