MailInBlack bloque le 'spam' grâce à l'authentification

Lancée en 2003 par des amis d'enfance, cette start-up française originaire de Marseille est en pleine expansion européenne avec l'ouverture prochaine de centres en Grande-Bretagne et en Allemagne, et plus récemment d'une agence commerciale dans l'Ouest parisien. Elle revendique 21 salariés.

Spécialisée dans la lutte contre les 'spams', ou courriels indésirables qui polluent nos boîtes de réception, la société a une approche originale. Elle préfère protéger ses clients grâce à une authentification forte (ndlr : *Test de Turing*) plutôt que d'essayer de surveiller les paquets qui arrivent dans le réseau d'entreprise – à l'instar de la majorité des éditeurs.

« Nos clients ont quatre objectifs: 1- bloquer les spams ; 2- essayer d'éviter le blocage des e-mails valides, ce que dans le jargon l'on nomme les faux positifs ; 3- ne pas apporter une charge d'administration supplémentaire au service informatique ; et 4- faire en sorte que la solution soit simple d'utilisation pour les collaborateurs », déclare le fondateur de MailInBlack, Régis Novi.

Sur le marché, l'on trouve deux grandes offres, le filtrage ordinaire des mails et l'authentification forte qui est la spécificité de la solution proposée par la startup.

Pourquoi une telle approche ? *« Tout d'abord, nous sommes partis de deux constats majeurs : d'abord que tous les spams sont envoyés par des réseaux Botnet, ensuite qu'à l'heure actuelle, il n'existe pas de définition universelle du spam. Par exemple le CAN Spam Act américain fait plus de 20 pages, et en Europe la situation est similaire. Ce flou total concernant la définition du terme empêche la mise en place de règles de filtrage précises. Un emailing peut être perçu comme de l'information ou non, cela dépend de son activité »,* poursuit Régis Novi.

« On nous demande souvent pourquoi nous sommes les seuls a utiliser l'authentification pour bloquer le spam. Et bien, les éditeurs d'antivirus ont une approche différente, ils se sont calqués sur les modes de fonctionnement des solutions antivirales, c'est a dire de définir la signature des virus et de les bloquer. La solution est compatible avec tous les OS, et permet également de protéger les terminaux de type Blackberry. »

Un petit bémol tout de même. Si l'authentification forte semble être la seule solution technologique pour réellement bloquer 100 % des spams, d'aucuns diront que la procédure d'authentification est trop contraignante. Reste qu'à choisir entre passer chaque jour une heure à supprimer ses pourriels et prendre une journée pour authentifier la plupart de ses contacts, le calcul est vite fait?

Quid de la nouvelle appliance Mibox V3!

Au menu de cette nouvelle version, disponible depuis la fin février, de l'antispam, la synchronisation avec l'annuaire LDAP, la personnalisation de l'interface et de la demande d'authentification, et enfin la haute-disponibilité de messagerie.

La MiboxV3 est développée depuis plus de six mois. Elle intègre de nouvelles fonctionnalités.

– La synchronisation LDAP et Active Directory de l'entreprise est répercutée dans la Mibox V3. Ceci

permet à l'administrateur de gérer ses licences de manière optimale et de faire des économies : une licence peut-être transférée d'un utilisateur à un autre sans contrainte. Cette synchronisation gère par ailleurs les changements de nom ou d'adresse email.

– La personnalisation de la demande d'authentification et de la Mibox. L'espace privatif des utilisateurs, la demande d'authentification, la procédure d'authentification et le Digest (le récapitulatif des emails stoppés envoyé aux utilisateurs peut maintenant être personnalisé au nom de l'entreprise cliente).

– La haute-disponibilité de messagerie (*Fail Over Service*). Dans une architecture de messagerie où les services doivent être disponibles 24h sur 24, MailInBlack assure une haute disponibilité en cluster, ce qui signifie que même si la Mibox est indisponible, les utilisateurs continuent de recevoir leurs emails.

La Mibox V3 est disponibles sous deux formules

MIB-Pro :

– l'appliance est directement installée dans la DMZ de l'organisme protégé. Tarification HT jusqu'à 200 boites aux lettres Mibox V3 : 1.420 euros + 2,35 euros par BAL et par an.

MIB-ASP :

– Protection externalisée via une redirection du flux de messagerie.

– Tarification HT jusqu'à 200 boites aux lettres : frais d'installation 300 euros + 2,80 euros BAL par an.