

# Principes et fonctionnalités

MailInBlack PRO et ASP

## SOMMAIRE

### . Préambule

- Principes intelligents de MailInBlack
- Solution MailInBlack-Pro
- Solution MailInBlack-Asp

### . Principes de la solution

- Antispam
- Antivirus

### . Fonctionnalités d'utilisation

- Pré-autorisation des contacts connus
- Récupération d'un email stoppé
- Personnalisation de la demande d'authentification
- Bannissement d'un expéditeur autorisé

### . Fonctionnalités techniques

- Inter-opérabilité
- Serveur de messagerie cible
- Haute-disponibilité de messagerie
- Compatibilité Active Directory
- Politique de traitement des emails entrants
- Personnalisation de l'interface administrateur et utilisateur
- Politique antivirale
- Politique de licence
- Gestion des alias et groupes de diffusion
- Auto-suppression des emails stoppés
- Contrôle des effets ping-pong
- Statistiques
- Sauvegardes automatisées
- Export de logs
- Gestion d'alertes
- Surveillance en temps réel
- Confidentialité de l'adresse de l'utilisateur protégé
- Firewall natif
- Langue de l'Espace utilisateur
- Langue de l'Espace d'administration
- Personnalisation du mot de passe de connexion utilisateur

## PREAMBULE

### Principes intelligents de MailInBlack :

La solution antispam MailInBlack est basée sur l'authentification de l'expéditeur : lorsqu'un e-mail est envoyé pour la première fois à un utilisateur, il est demandé à l'expéditeur de s'authentifier, prouvant ainsi qu'il est un expéditeur légitime. Une fois cette procédure effectuée, le message est acheminé au destinataire et l'adresse de l'expéditeur est définitivement autorisée.

### Solution MailInBlack-Pro :

- MailInBlack-Pro est une solution professionnelle (organismes possédant leur propre nom de domaine) pour la sécurisation antispam des emails entrants. Cette solution est offerte sous forme d'appliance (boîtier administré grâce à une interface web) dénommée Mibox, installée dans la Dmz de l'entreprise. En mode Pro, l'administrateur de l'organisme gère toute la configuration de la Mibox.

### Solution MailInBlack-Asp :

- MailInBlack-Asp est une solution professionnelle (organismes possédant leur propre nom de domaine) pour la sécurisation antispam des emails entrants. Cette solution est offerte en mode ASP : par un changement de Mx primaire, les emails sont dirigés vers l'une des Mibox administrées par la société MailInBlack. Les emails provenant d'expéditeurs autorisés sont poussés vers le serveur de messagerie de l'organisme (ou de son hébergeur de boîtes aux lettres). En mode ASP, l'organisme est libéré du travail d'administration relatif aux paramètres généraux et de la surveillance de la Mibox. Ce travail est réalisé par le service technique de MailInBlack. Certaines des fonctionnalités décrites ci-dessous sont de fait uniquement accessibles avec MailInBlack-Pro

## PRINCIPES DE LA SOLUTION

### Antispam :

#### Protection antispam

*MailInBlack stoppe les spams de tous genres :*

- Emails inconvenants
- Texte caché dans une image
- Texte en code Code ASCII
- Langues étrangères
- Scam (escroqueries)
- Spoofing (usurpation d'adresses)

### Antivirus :

#### Protection antivirus

*MailInBlack stoppe tout email porteur de code malveillant :*

- Virus
- Spyware (logiciel espion)
- Phishing (collecte illégale d'informations confidentielles)
- Malware (code malveillant sans signature totalement reconnue)

## FONCTIONNALITES D'UTILISATION

### Pré-autorisation des contacts connus

Lors de la mise en service, il est possible de pré-autoriser ses contacts.

#### . Modes manuel ou automatisé

- connectivité Active Directory (voir détails plus loin)
- téléchargement de fichiers au format texte
- entrées manuelles
- par un simple clic sur le digest des emails stoppés

#### . Pré-autorisation multi-types

- adresses email littérales
- domaines entiers
- listes de diffusion
- forums de discussion

### Récupération d'un email stoppé

Il est toujours possible de récupérer un email (newsletter, commande sur internet par exemple) à tout moment et très simplement.

#### . Récapitulatif interactif des emails stoppés

Chaque utilisateur reçoit régulièrement et personnellement un récapitulatif interactif des e-mails stoppés. La réception du Digest est paramétrable 1 à 3 fois par jour à heures souhaitées, 1 fois par semaine à jour et heure souhaités ou peut être désactivée.

- personnel à chaque utilisateur
- reçu sous la forme d'un email interactif
- par un simple clic, possibilité de récupérer un message ponctuellement ou d'autoriser définitivement l'expéditeur

#### . Espace utilisateur personnel

Chaque utilisateur peut se connecter en à un Espace utilisateur personnel où il retrouve en temps réel les emails stoppés, en attente d'authentification.

- accès sécurisé (login + code d'accès)
- visualisation de la quarantaine (paramétrable jusqu'à 45 jours) en temps réel
- en deux clics, possibilité de récupérer un message ou d'autoriser définitivement l'expéditeur

### Personnalisation de la demande d'authentification

Pour encourager l'expéditeur à s'identifier, la demande d'authentification est fortement personnalisée.

#### . Personnalisation par l'image

- logo de l'organisme, ou
- photo de l'utilisateur, ou
- autre image

#### . Personnalisation par du texte

- le nom de l'utilisateur protégé apparaît comme expéditeur
- l'objet du message initial est repris dans l'objet
- texte personnel entièrement paramétrable
- 2 langues au choix

### Bannissement d'un expéditeur autorisé

Le concept de black-listage est particulier chez MailInBlack. En effet, la notion de "Bannir" un expéditeur n'est utile que lorsque cet expéditeur a pris la peine de s'authentifier, et que l'on ne souhaite plus recevoir ses futurs messages. Avec MailInBlack, nul besoin de chercher à black-lister les spammeurs : leurs spams sont stoppés sur l'appliance MailInBlack, avant qu'ils n'atteignent votre serveur de messagerie, et s'auto-détruisent au bout de la période de quarantaine (paramétrable jusqu'à 45 j). On ne les voit donc pas apparaître sur les postes utilisateurs et personne n'a d'intervention à faire. Les bannir serait une pure perte de temps et ne servirait pas à rien car les spammeurs changent d'adresse d'expédition en permanence.

#### . Récapitulatif interactif des emails stoppés

En plus des emails stoppés, le digest reçu individuellement par chaque utilisateur fait apparaître la liste des adresses des expéditeurs s'étant récemment authentifiés.

- personnel à chaque utilisateur
- reçu sous la forme d'un email interactif
- par un simple clic, possibilité de bannir un expéditeur qui s'est authentifié

#### . Espace utilisateur personnel

Dans son Espace utilisateur personnel l'utilisateur se connecte à la liste des utilisateurs authentifiés.

- accès sécurisé (login + code d'accès)
- en deux clics, possibilité de bannir l'expéditeur

## FONCTIONNALITES TECHNIQUES

### Inter-opérabilité

- . Réseau
- . Matériel

### Serveur de messagerie cible

Possibilité de choisir un serveur de messagerie cible différent pour chaque domaine, si besoin.

### Haute-disponibilité de messagerie

Possibilité de mettre en place un système de Haute-Disponibilité de messagerie de type Fail Over Service.

### Compatibilité Ldap et Active Directory

- . Mises à jour des informations des utilisateurs : création, modifications, suppression
- . Traitement des mises à jour : semi-automatique  
(l'administrateur valide manuellement une partie des nouvelles informations collectées sur l'annuaire Ldap ou Active Directory. Les changements de noms et de prénom se font automatiquement)
- . Connexion automatisée ou sur demande
- . Fréquence de connexion paramétrable

### Politique de traitement des emails entrants

- . Distinction de 3 catégories d'adresse email
  - Adresse d'un collaborateur protégé par MailInBlack (utilisateur)
  - Adresse d'un collaborateur non-protégé par MailInBlack (utilisateur virtuel)
  - Adresse inconnue comportant le nom de domaine de l'organisme
- . Traitement
  - Utilisateur : antivirus + antispam
  - Utilisateur virtuel : antivirus
  - Adresse inconnue : traitement au choix : refus catégorique de l'email (filtrage strict) ou acceptation et traitement comme pour un utilisateur virtuel

### Personnalisation de l'interface utilisateur, du Digest et de la Demande d'authentification

- . MailInBlack-Pro
  - Logo
  - Textes multilingues de la demande d'authentification
- . MailInBlack-Asp
  - Logo

### Politique antivirale

Tout email accepté par MailInBlack est traité par l'antivirus.

- . Choix de traitement
  - Destruction totale du message
  - Nettoyage des messages infectés si réalisable

### Politique de licence

- . Protection totale ou partielle des collaborateurs  
*Liberté de ne pas protéger toutes les adresses d'un domaine et de limiter la protection aux personnes spammées*
- . Facturation au nombre de licences utilisateurs
  - Contrats de 3 ou 5 ans
  - Gratuité de l'antivirus de mail pour les utilisateurs virtuels
  - Gratuité de 6 alias et/ou groupes de diffusion par utilisateur
- . Nombre illimité de domaines  
*Il est possible de créer autant de domaine que de licences.*
- . Suppression, création et modification d'une licence  
*Les licences ne sont pas nominatives. L'administrateur peut librement gérer ses licences, dans la limite du nombre maximal contracté.*

### Gestion des alias et groupes de diffusion

Gratuité de 6 alias et/ou groupes de diffusion par utilisateur.

- . Intra ou inter domaines

### Auto-suppression des emails stoppés

- . Auto-suppression des emails non authentifiés après le temps de quarantaine
  - quarantaine paramétrable jusqu'à 45 jours
  - quarantaine accessible en temps réel
- . Absence de tout travail de purge

### Contrôle des effets ping-pong

- . Gestion adaptée
  - compatibilité avec les messages d'absences
  - compatibilité avec d'autres utilisateurs protégés par MailInBlack

### Statistiques

Etats mensuel des mails infectés, bannis, stoppés et autorisés

### Sauvegardes automatisées

Configuration système, domaines, utilisateurs et personnalisations, whitelists et blacklists

### Export de logs

Traitement des emails (transmis, stoppé, infecté, récupéré, authentifié)  
Actions des utilisateurs (récupération d'un email, autorisation d'un expéditeur)  
Mise à jour de l'antivirus

### Gestion d'alertes

Alertes pour dysfonctionnement de la mise à jour de l'antivirus, de la sauvegarde ou de l'export des logs

### Surveillance en temps réel

Etats des messages traités, Etats des services (interface web, MTA, réseau et bdd), Etats du système (charge, mémoire vive, espace libre disque dur, nombre processus)  
Antivirus

### Confidentialité de l'adresse de l'utilisateur protégé

*Même si le nom et le prénom de l'utilisateur protégé apparaît comme expéditeur de la demande d'authentification, c'est une adresse générique qui envoie cette demande afin de garder la confidentialité de l'adresse email de l'utilisateur.*

### Firewall natif

#### Langue de l'Espace utilisateur

. Français ou anglais au choix

#### Langue de l'Espace d'administration

. Français

#### Personnalisation du mot de passe de connexion utilisateur

*Modification et gestion confidentielle des mots de passe par l'utilisateur.*