



## **M-Secure IT**

### **Solution AntiSpam – Guide d'Achat**

**28 Novembre 2008**

#### **M-SecureIT**

7C, Place du Dôme  
Immeuble Elysées La Défense  
92056 Paris La Défense Cedex  
Tél : +33-1-7275-7246  
Fax : +33-1-5301-6786  
E-mail : info@m-secureit.com

#### **M-SecureIT Casablanca**

B.P 16544  
Casablanca Technopark  
20150 Casablanca  
Tél : +212-22-502-202  
Fax : +33-1-5301-6786  
E-mail : info@m-secureit.com



# Sommaire

<b>1 INTRODUCTION.....</b>	<b>1</b>
1.1 Comment utiliser ce guide .....	1
<b>2 CRITÈRES D'UNE SOLUTION.....</b>	<b>1</b>
2.1 Taux de blocage de spams.....	1
2.2 Taux faux positifs.....	1
2.3 Performance.....	2
<b>3 TECHNOLOGIES ANTISPAM .....</b>	<b>2</b>
3.1 Heuristiques.....	2
3.2 Empreintes numériques.....	3
3.3 Filtrage par mots clef.....	3
3.4 Liste grise.....	3
3.5 Calculs Bayésiens.....	3
3.6 Listes Maintenues.....	3
<b>4 DÉPLOIEMENT.....</b>	<b>4</b>
4.1 En sous-traitance.....	4
4.2 Solutions logicielles .....	4
4.3 Appliances .....	4
4.4 Poste Client .....	4
<b>5 PRINCIPALES FONCTIONNALITÉS .....</b>	<b>5</b>
5.1 Mise à jour automatique .....	5
5.2 Profils paramétrables.....	5
5.3 Quarantaine et quarantaine/utilisateur.....	5
5.4 Reporting.....	5
5.5 Catégories de spam.....	5
5.6 Blacklisting/Whitelisting.....	6
<b>6 GRILLE D'ÉVALUATION.....</b>	<b>6</b>



# 1 Introduction

L'acquisition d'une solution antispam n'est pas une décision facile au vu de l'offre disponible sur le marché. Les éditeurs et constructeurs de tout horizon se bousculent sur ce segment porteur et apportent des solutions variées, plus ou moins coûteuses et porteuses de confusion. Comment s'orienter et choisir dans ces conditions ?

Même si nous croyons que la solution antispam parfaite n'existe pas, ce guide d'achat a été rédigé dans le but d'aider à formuler des objectifs pour une solution adaptée à la problématique antispam.

## 1.1 Comment utiliser ce guide

Nous avons inséré une grille à la fin de ce document dans le but de vous aider à comparer objectivement les différents produits. La suite du document vous éclairera sur les principaux critères de comparaison.

# 2 Critères d'une solution

## 2.1 Taux de blocage de spams

Le taux de blocage de spams (**TBS**) d'une solution est sa capacité à identifier et arrêter des spams. Il est exprimé en pourcentage des spams arrêtés par rapport à l'ensemble des spams.

Les éditeurs en général exagèrent ce taux. Si vous avez la possibilité d'évaluer les produits, nous vous conseillons vivement de le calculer vous même en laissant le produit tourner quelques jours et en renseignant la formule :

$$\text{(Spams arrêtés / (Spams arrêtés + Spams passés))} \times 100\%$$

Ainsi si une solution bloque 92 spams et laisse passer 8, son TBS serait  $92/(92+8)=92\%$

## 2.2 Taux faux positifs

Le taux de faux positifs (**TFP**) est le critère le plus important d'une solution antispam. Une solution avec un TFP de 0% est facile à réaliser : il suffirait de tout laisser passer ! Une solution avec un TBS élevé et un TFP bas est l'objectif de tout bon éditeur de produit antispam.

Ce taux s'exprime en pourcentage des légitimes bloqués par rapport aux spams bloqués. Nous vous conseillons de le calculez si vous en avez la possibilité, en utilisant la formule :

$$\text{(Mails légitimes bloqués / Mails bloqués)} \times 100\%$$

## 2.3 Performance

Les performances de votre solution sont un facteur très important. Votre solution devrait être adaptée et même plutôt supérieure à la charge de mails que vous échanger quotidiennement.

La performance s'exprime habituellement en Ko/s (ou KB/s dans les documentations techniques anglophones). Pour calculer la performance minimale requise pour votre solution, utilisez les journaux (logs) de votre serveur de messagerie. La performance se définit par la formule :

$$\text{(Taille totale des messages échangés par jour / 86 400<sup>1</sup>)Ko/s}$$

Si vous ne connaissez que le nombre de mails reçus par jour, estimez la taille moyenne des mails échangés à 20 Ko et appliquer la formule :

$$\text{((Nombre de messages échangés par jour x 20) / 86 400)xKo/s}$$

## 3 Technologies Antispam

A l'instar de ce qui se passe pour les virus, le problème du spam est un défi permanent pour les éditeurs antispam. En effet les spammeurs cherchent et trouvent souvent des angles d'attaques contre les techniques et autres parades des solutions antispam.

Les opérateurs antispam utilisent des techniques différentes mais certaines leurs sont communes à tous. Contrairement à ce qu'affirment certains éditeurs, certaines techniques sont très peu efficaces, d'autres comportent de nombreuses faiblesses et pourront ne plus être utilisés d'ici quelques temps. Il est important de comprendre l'approche derrière les termes des techniques antispam.

Les principales technologies antispam peuvent être regroupés en 6 catégories

### 3.1 Heuristiques

Les heuristiques sont des méthodes empiriques, non formelles, menées par des algorithmes complexes et n'aboutissant pas nécessairement à des solutions optimales. Dans le cadre de l'activité antispam, les heuristiques sont utilisées pour détecter des modèles (autrement dit « pattern matching ») dans des mails associés à du spam. Ces techniques peuvent être efficaces dans la lutte antispam, mais ne sont pas faciles à « tuner » et peuvent conduire à des résultats discutables si elles sont mal utilisées. D'autre part, les spammeurs connaissent bien les heuristiques et inventent tous les jours de nouvelles astuces pour leur échapper.

---

<sup>1</sup> 86 400 est le nombre de secondes dans 24 heures.

## 3.2 Empreintes numériques

Les bases de données d'empreintes numériques (digital checksum en anglais) associent un identifiant unique à un mail, un URL ou une image spam. Ces identifiants sont stockés dans bases à accès rapide afin que chaque mail reçu soit comparé à ces bases. Malheureusement différents moyens sont utilisés pour échapper à leur reconnaissance. Précisons que cette technologie nécessite un accès confortable à la base d'empreinte pour fonctionner de manière optimale.

## 3.3 Filtrage par mots clef

Dite aussi filtrage statique est une méthode archaïque qui génère malheureusement un taux élevé de faux positifs (TFP). De plus, elle est facile à éviter par l'erreur orthographique intentionnelle ou par la manipulation basique de textes. Elle n'est pas recommandée comme principale technique antispam.

## 3.4 Liste grise

Dite aussi « Gray listing » est une technologie astucieuse basée sur la particularité des serveurs de messagerie à renvoyer un mail dont le destinataire demande explicitement le renvoi. Cette technique permet d'éviter de recevoir les mails des machines piratées (botnet) et qui diffusent des spams à l'insu de leurs utilisateurs. Cette technique a un léger inconvénient, celui de retarder des mails qui peuvent être urgents.

## 3.5 Calculs Bayésiens

Technologie basée sur le théorème de Bayes, qui, pour simplifier, affirme dans le contexte antispam, que la probabilité pour qu'un mail contenant certains mots (par exemple « viagra », « rolex ») soit un spam est égale à la probabilité pour que ces mots se retrouvent dans des spams que multiplie la probabilité qu'un mail soit un spam que divise la probabilité que ces mots se retrouvent dans des mails.

$$P(\text{spam}|\text{mots}) = ((P(\text{mots} | \text{spam}) \times P(\text{spam})) / P(\text{mots}))$$

Cette technologie nécessite un apprentissage par l'utilisateur ainsi que l'utilisation de dictionnaires communs ou par utilisateur. Cette technologie offre l'avantage de s'adapter à chaque utilisateur qui s'il accepte de jouer le jeu (c'est à dire d'enrichir son dictionnaire) améliora l'efficacité de son outil constamment.

## 3.6 Listes Maintenuées

Appelées RBLs (Real-time Black Lists) ou DNSBL sont des bases de d'adresses IP de serveurs de spams. Cette technologie n'est pas très efficace puisque beaucoup de serveurs légitimes piégés par des spammeurs peuvent se retrouver injustement dans ces bases. Actuellement, certains RBLs ont un taux de faux positifs de 60%. Ces désagréments peuvent être facilement évités par l'utilisation de listes blanches (White lists) contenant les serveurs dont on est certains de leur légitimité.

## 4 Déploiement

Le déploiement d'une solution est aussi important que le choix d'une solution ou d'une technologie. Nous énumérons quatre méthodologies de déploiement :

### 4.1 En sous-traitance

L'activité antispam peut-être à sous-traité un opérateur spécialisé (MSSP<sup>2</sup>) qui se chargera de fournir une solution antispam et délivrera au client un flux messagerie aussi « propre » que possible et un rapport mensuel sur les statistiques des mails reçus et (éventuellement) envoyés, contre un abonnement mensuel. Le déploiement de ce type de solution est simple, il suffit de pointer son MX sur les adresses du prestataire de service. Ce type de solution nécessite d'établir un certains nombre de critères d'engagement (SLA) que le prestataire devrait respecter : bande passante, envergure de la solution, administration, support ...etc.

### 4.2 Solutions logicielles

Sont des solutions qui se déploient sur des serveurs. Ces solutions permettent à l'entreprise de gérer elle même la problématique antispam et une grande autonomie. Elles nécessitent une administration quotidienne et des compétences au sein de l'entreprise ou chez le prestataire de service. Elles ont comme inconvénient de s'installer sur des serveurs généralistes qui ne sont pas optimisés ou durcis. Ces solutions peuvent dans certains cas manquer de performance voire être clairement vulnérables.

### 4.3 Appliances

Sont des solutions qui matérielles/logicielles. Ces solutions permettent à l'entreprise de gérer elle même la problématique antispam et une grande autonomie. Elles nécessitent une administration quotidienne et des compétences au sein de l'entreprise ou chez le prestataire de service. Elle sont généralement construites sur des environnements optimisés (voir propriétaires) et offrent généralement de meilleurs performances et plus de robustesse que les solutions logicielles.

### 4.4 Poste Client

Sont des solutions qui se déploient sur le poste client des utilisateurs. Ce ne sont pas des solutions recommandées pour les entreprises puisqu'il est judicieux d'arrêter les spams en amont du serveur de messagerie et avant son entrée dans le réseau de l'entreprise.

---

2 MSSP : Managed Security Service Provider littéralement fournisseur de service de sécurité

## 5 Principales Fonctionnalités

Nous énumérons ci-dessous les principales fonctionnalités à vérifier au moment de l'évaluation d'une solution antispam. Ces fonctionnalités apporteront à notre avis efficacité et souplesse à votre solution.

### 5.1 Mise à jour automatique

Cette fonctionnalité est fondamentale pour l'efficacité de votre solution. La solution devrait se mettre à jour automatiquement et régulièrement. Il est vivement conseillé à l'administrateur de vérifier de temps en temps que cette opération se déroule normalement.

### 5.2 Profils paramétrables

Une entreprise n'étant pas toujours uniforme, il est important de garder à l'esprit que le profil de protection antispam peut différer d'une population à un autre voir d'un utilisateur à un autre. La solution devrait donc être dotée de profils de protection paramétrables qui peuvent s'appliquer à différents utilisateurs. Aussi nous conseillons que la solution soit munie d'un module d'auto-apprentissage par utilisateur.

### 5.3 Quarantaine et quarantaine/utilisateur

La solution devrait au minimum disposer d'une quarantaine, sinon des mails légitimes peuvent être définitivement perdus. Une quarantaine par utilisateur permet à l'individu d'apprécier lui même la légitimité d'un mail et économise de façon substantielle le temps des administrateurs.

### 5.4 Reporting

Cet outil permet de rester informé en tout instant sur l'activité messagerie et antispam. Il offre la possibilité de prévenir l'atteinte des limites de la solution ou de l'espace disque ou d'anticiper tout simplement les pics d'activité qui peuvent avoir un impact sur l'utilisation du réseau.

### 5.5 Catégories de spam

Cette fonctionnalité n'est pas présente dans tous les solutions mais offre la possibilité de « tuner » la solution en fonction de son activité. Ainsi si par exemple une entreprise est dans le secteur des IT pourrait recevoir plus de mails non sollicités qui ciblent ce type d'entreprises.

## 5.6 Blacklisting/Whitelisting

Cette fonctionnalité est fondamentale puisque régulièrement le cas se présente où un serveur injustement répertorié comme un serveur de spams se trouve être un serveur légitime. Au contraire, il est également nécessaire de bloquer explicitement certains serveurs ou domaines résolument spammeurs.

## 6 Grille d'évaluation

Critères	Solution 1	Solution 2	Solution 3	Solution 4
TBS				
TFP				
Performance				
Heuristiques				
Empreintes numériques				
Filtrage statique				
Liste grise				
Calculs Bayesiens				
Listes Maintenuées				
Déploiement				
MAJ Automatique				
Profils paramétrables				
Quarantaine				

Quarantaine/Utilisateur				
Reporting				
Catégories de spams				
Blacklisting/Whitelisting				