

# KHSS - KASPERSKY HOSTED SECURITY SERVICES

## Email Security - Caractéristiques

### **Protection contre les virus**

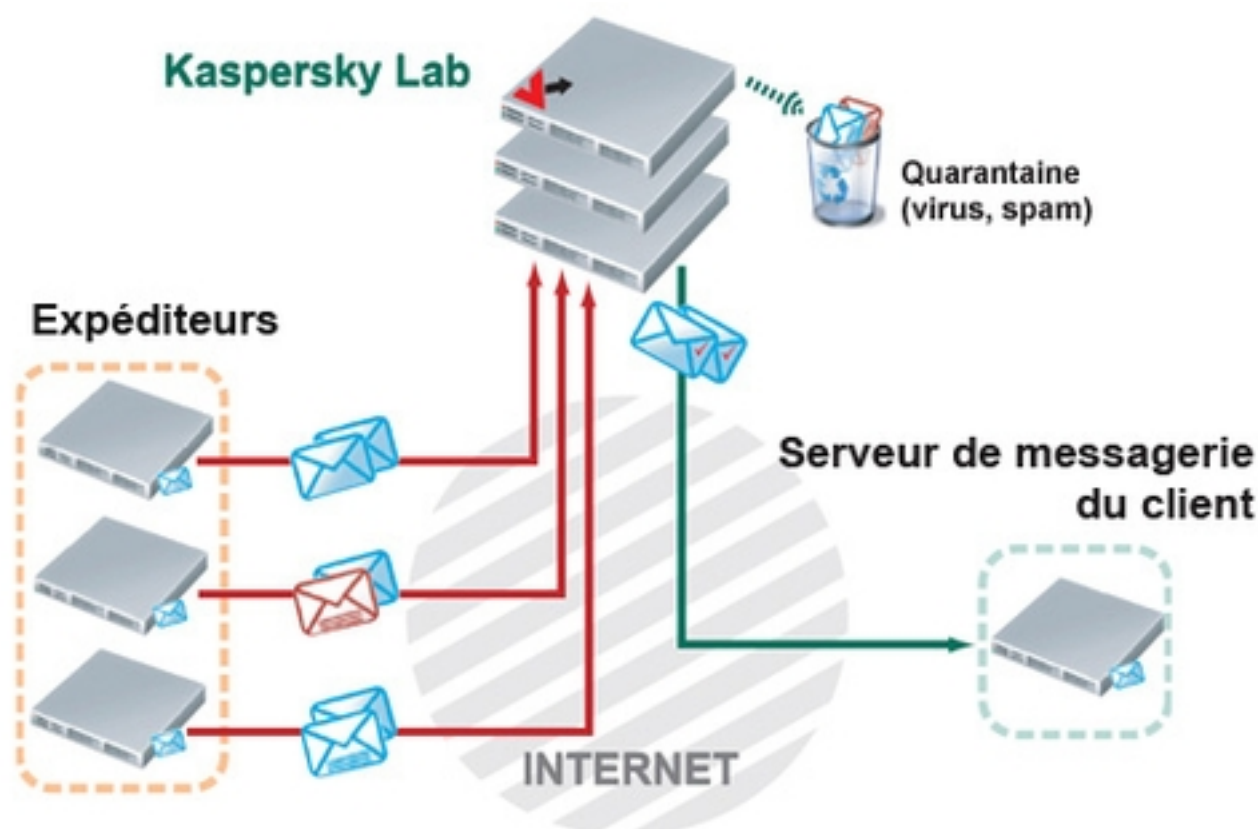
Tous les messages adressés au client sont soumis à plusieurs niveaux d'analyse avant d'atteindre le système de messagerie du client.

**Service d'analyse précoce.** Détecte les programmes malveillants déjà reconnaissables mais pour lesquels des mises à jour de l'antivirus n'ont pas encore été délivrées.

**Filtrage par format.** Interdit certains types de pièces jointes. Ceci réduit les risques de pénétration d'objets infectés à travers le réseau de l'entreprise.

**Kaspersky Anti-Virus.** Les mises à jour des bases antivirus sont récupérées dès leur diffusion. Lorsque de nouveaux programmes malveillants sont détectés, des mises à jour sont spécialement délivrées pour y faire face. Avant leur réception, les composants Pre-Scan et BitHunt assurent une protection efficace et détectent jusqu'à 100 % de tous les programmes malveillants diffusés à travers le courrier électronique.

**BitHunt.** Actuellement, plus de 95 % de tous les logiciels malveillants se présentent sous différents paquets. Pour la plupart des solutions antivirus, ce constat suffit déjà à stopper la détection des programmes malveillants déjà connus. Le composant AllUnpack, incorporé au système, permet de décompresser et de décoder pratiquement tous les fichiers exécutables compressés ou chiffrés.



### Protection contre le courrier indésirable

Le filtre antispam de Kaspersky Hosted Security, Email Security, s'appuie sur Kaspersky Anti-Spam et sur le système BitHunt pour la détection proactive des menaces. Le filtre unifie tous les algorithmes connus de détection de courrier indésirable dans sa méthodologie de filtrage du contenu des messages, moyennant l'analyse heuristique de phrases et mots-clés indésirables et la comparaison avec des listes noire et blanche, à l'intérieur du trafic normal du système client.

**Listes.** L'application vérifie la présence de l'adresse IP de l'expéditeur dans les listes noires de fournisseurs et d'organismes publics (DNSBL - DNS gestionnaires de listes noires). Si l'adresse IP a été ajoutée par un administrateur dans la liste blanche, le message est accepté sans traverser tous les niveaux de filtre mentionnés plus haut.

**Attributs formels du message.** Le logiciel filtre le courrier indésirable en examinant certains attributs courants, comme la modification de l'adresse du destinataire ou l'absence de l'adresse IP dans les DNS (Système de Nom de Domaine), la présence d'un nombre anormalement élevé de destinataires, ou la dissimulation de l'adresse du destinataire. En outre, la taille et le format du message sont contrôlés.

**Contenu du message.** Le logiciel analyse dans les messages la présence et la position de certains textes ou mots qui sont typiques des courriers indésirables. Le texte proprement dit

du message, mais aussi celui des pièces jointes est analysé.

**Signatures (échantillons)** . Le logiciel utilise une base de données de signatures linguistiques qui est mise à jour toutes les heures. Ceci permet l'identification de versions modifiées de messages indésirables connus, générées pour contourner les filtres anti-spam.

**Module de détection d'images indésirables**. La technologie GSG-3 permet de bloquer des messages indésirables contenant des informations sous forme graphique. Ce type de messages est récemment devenu très courant.

**BitHunt**. Le système de protection proactive inclut un filtre fondé sur la " réputation ", qui accorde un taux de confiance à l'adresse IP de l'expéditeur. Il existe de nombreux critères pour calculer le degré de confiance ? volume de courrier indésirable et de programmes malveillants envoyés depuis une adresse IP donnée, si l'adresse IP est dynamique ou pas, etc. Si la réputation d'un hôte est particulièrement mauvaise, tout le courrier expédié par lui est alors refusé.

**Système de détection urgente (UDS)** . La technologie UDS (Urgent Detection System) permet d'être informé sur les derniers publipostages indésirables, immédiatement après leur détection. Cette information est utilisée pour analyser les messages qui n'ont pas encore été classés (indésirables ou pas).

**Analyse sémantique du contenu du message**. Le filtre classe automatiquement tous les messages, c'est à dire, il distribue les messages entrants dans l'une ou l'autre des catégories, d'après les résultats de l'analyse sémantique de leur texte.

### **Paramètres de protection avancés**

En plus d'une protection antivirus et antispam, le composant Kaspersky Hosted Security : Email Security est capable de bloquer les fichiers de formats différents. Normalement, le type de pièce jointe est déterminé en fonction de la structure interne du fichier, de son nom et de son extension. Cette technologie assure un niveau élevé de sécurité et permet de réduire les pertes de temps du personnel.

Cette solution prend en charge les formats suivants :

pièces jointes (EXE, SYS, DLL, etc.)

documents Microsoft Word (DOC, DOT)

livres Microsoft Excel (XLS, XLT)

présentations Microsoft PowerPoint (PPT, PPS)

documents RTF (RTF)

archives ZIP (ZIP), RAR (RAR) et ARJ (ARJ)

clips vidéo (AVI, MPG)

fichiers audio (MP3, OGG).

## **Administration**

Une interface aisée facilite la configuration individuelle du service et la génération de rapports d'activité. L'accès à l'interface est contrôlé par un canal SSL sécurisé. Il est possible de générer les rapports suivants :

**Courrier reçu.** Informations sur le courrier reçu par chaque domaine client, sur une période de temps spécifique, avec le volume de correspondance indésirable contenu.

**Courrier renvoyé.** Le nombre de messages renvoyés peut être ordonné par domaines et utilisateurs.

**Courrier indésirable.** Il est possible de générer un rapport avec des informations sur la quantité, le volume et les sources principales de courrier indésirable\*.

**Programmes malveillants.** Il est possible de générer un rapport avec des informations sur la quantité et le volume de fichiers analysés, et les programmes malveillants les plus fréquents, dans la période couverte par le rapport.

**Top 10.** Il est possible de spécifier les 10 programmes malveillants les plus répandus, les 10 premières sources de courrier indésirable, les 10 destinataires les plus actifs, etc., pour n'importe quel rapport généré.

**Rapport récapitulatif.** Ce rapport présente un résumé de toutes les informations associées aux domaines clients. Toutes les informations spécifiées dans cette liste sont ajoutées au document\*.

**Rapport exécutif.** Il est possible de générer un rapport abrégé, à l'attention du directeur exécutif ou de la direction\*.

**Note : il convient de rappeler que Kaspersky Hosted Security est un produit spécialement destiné à la protection des serveurs de courriels.**

Principaux atouts



## Commentaires

2009-02-26 14:48:27 - Alice

Merci pour tous ces conseils que vous nous offrez ici. Car il est évident que la protection contre les virus des documents surtout des documents financiers est le problème qui concerne chaque entreprise.

2009-02-26 15:53:00 - Liam

Je ne suis pas sûre que mon commentaire sera publié tout de même je voudrais vous dire un grand merci pour votre travail. Car je visite votre blog assez souvent puisque j'y trouve de l'info bien utile. J'apprécie votre aide. Merci.

Copyright : khss - 2008-03-06 20:12:07

Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- \* de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

\* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

\* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>