Kaspersky Anti-Spam 3.0 oferă protecție completă împotriva mesajelor de tip spam pentru utilizatori sistemului de e-mail al companiilor și ai serviciilor publice de e-mail.

Funcții

- Protecție antispam
- Administrare
- Cerințe de sistem

Protecție împotriva mesajelor de tip spam

Filtrare pe bază de listă. Adresele IP ale expeditorului sunt verificate dacă figurează pe lista neagră a spammer-ilor, care este furnizată de serviciile de Internet și organizațiile publice (DNS - bazat pe listele Blackhole). Administratorul de sistem poate adăuga adrese de corespondență, pe care le consideră sigure, pe o listă, asigurându-se că mesajele vor fi trimise fără a fi filtrate.

Tehnologii SPF și SURBL. Procesul de filtrare implică verificarea expeditorilor folosind Sender Policy Framework. Detectarea adreselor IP ale spammer-ilor folosind DNSBL, este suplimentată de tehnologia SURBL (Spam URI Real-time Block List), care poate identifica URL-urile mesajelor de tip spam în corpul mesajului.

Analiza atributelor formale. Programul recunoaște mesajele de tip spam după caracteristici tipice ca deformarea adresei expeditorului sau absența adresei IP din DNS a expeditorului, un număr extrem de mare de destinatari sau adrese ascunse. Mărimea și forma mesajelor sunt luate și ele în considerare.

Analiza semnăturilor. Baza de date de semnături este actualizată 24 ore pe zi, șapte zile pe săptămână. Folosind semnătură pentru mesajele de tip spam, programul poate recunoaște chiar și versiunile modificate a mesajelor de tip spam care au încercat să evite filtrele.

Algoritmi euristici lingvistici. Programul scanează mesajele pentru a detecta fraze sau cuvinte care sunt tipice pentru mesajele de tip spam. Sunt analizate atât conținutul mesajelor cât și atașamentele

Mesaje de tip spam grafice. O bază de date cu semnături pentru mesajele de tip spam grafice ajută programul să blocheze mesajele care conțin imagini de tip spam, acestea fiind în creștere în ultimii ani.

Cerințe UDS în timp real. Sistemul de Detecție Rapidă este actualizat cu informații despre mesajele de tip spam, doar la câteva secunde după ce au apărut pe Internet. Mesajele cărora nu li se poate oferi un anumit status (ex. spam, no-spam) pot fi scanate folosind Sistemul de Detecție Rapidă.

Administrare

Management flexibil. Interfața noastră web permite administratorului de sistem să utilizeze aplicația atât local cât și de la distanță. Nivelul de filtrare este ușor de configurat, la fel și lista neagră și cea sigură. Este posibil să fie activate/dezactivate reguli individuale de filtrare și poate bloca automat, e-mailurile setate în limbile asiatice.

Administrarea grupurilor de utilizatori. Administratorul poate crea grupuri de utilizatori fie folosind liste de adrese sau măști de domeniu (de exemplu XXX@domain.com) și aplicând setări individuale și reguli de filtrare pentru fiecare grup.

Opțiuni pentru procesarea mesajelor de tip spam. Programul poate fi configurat să proceseze mesajele de tip spam ștergându-le automat, redirecționându-le într-un fișier de tip carantină cu o notificare către utilizator sau trimițându-le către clientul de e-mail pentru o filtrare mai specială.

Rapoarte detaliate. Administratorii pot monitoriza cu ușurință aplicația, nivelul protecției și pe cel al licenței, utilizând rapoarte HTML sau urmărind fișierele jurnal. Datele pot fi transmise în formate CSV sau Excel.

Actualizarea bazei de date în funcție de un program. Actualizările bazei de date antivirus pot fi descărcate în funcție de un program stabilit de administrator (se actualizează implicit, la fiecare 20 de minute). Când un mesaj suspect nu poate fi clasificat în nici un fel, aplicația face o cerere către serverul UDS.

Cerințe hardware :

Procesor Intel Pentium III 500 MHz sau mai mare (recomandat Intel Pentium IV 2.4 GHz);
Cel puțin 512 MB RAM (recomandat 1 GB).

Cerințe software :

Sisteme de e-mail

- Sendmail 8.13.5 cu suport pentru Milter API.
- Postfix 2.2.2
- Qmail 1.03
- Exim 4.50
- Communigate Pro 4.3.7

Sisteme de operare

- Red Hat Linux 9.0
- Red Hat Fedora Core 3
- Red Hat Enterprise Linux Advanced Server 3
- SuSe Linux Enterprise Server 9.0
- SuSe Linux Professional 9.2
- Mandrake Linux version 10.1
- Debian GNU/Linux version 3.1
- FreeBSD version 5.4
- FreeBSD version 6.2

Cerințe suplimentare : Utilitarul bzip2 utility cu interpret Perl este esențial