HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza K9 antispam alata

CCERT-PUBDOC-2004-06-77

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Komunikacija porukama elektroničke pošte danas se zasigurno smatra jednim od najpopularnijih načina poslovne, ali i privatne komunikacije između korisnika Interneta. Međutim, koliko god ovaj način komunikacije bio jednostavan i praktičan, toliko je i problematičan sa stanovišta sigurnosti s obzirom na sve veći broj nelegitimnih poruka koje se svakodnevno šire sustavom elektroničke pošte. Osim legitimnih korisničkih poruka sustavom elektroničke pošte šire se virusi, crvi i brojni drugi maliciozni programi te veliki broj tzv. spam poruka, odnosno neželjenih poruka elektroničke pošte koje iz dana u dan postaju sve ozbiljniji problem.

Spam ili neželjena elektronička pošta (engl. *Unsolicited Bulk mail*) su one poruke koje nisu zatražene od krajnjeg korisnika i koje se u velikom broju kopija šalju na adrese korisnika. Sadržaj takvih poruka najčešće je komercijalnog karaktera (reklame usluga, roba i servisa) iako su mogući i brojni drugi sadržaji kao što su npr. ponude za brzo bogaćenje, multilevel marketing, porno sadržaji i sl. Korištenje spam poruka u svrhu oglašavanja, odnosno distribuiranja reklamnih i drugih sličnih sadržaja iznimno je pogodno za pošiljatelja s obzirom da većinu troškova procesiranja poruka snosi upravo njen primatelj, a minorni troškovi slanja poruke potpuno su neovisni o broju primatelja. Problem spam poruka dugo je vremena bio prvenstveno njihov iritirajući karakter za krajnjeg korisnika, no tijekom vremena isti je poprimio znatno veće razmjere pa se danas sve više pažnje posvećuje upravo borbi protiv neželjene elektroničke pošte. U nekim zemljama već su doneseni i posebni zakoni i regulative o korištenju informacijske tehnologije kojima se regulira ovaj problem.

Osnovni razlozi borbe protiv spam poruka su upravo sve veći troškovi koje primatelj plaća u vidu procesorske snage, zauzeća diskovnog prostora, mrežne propusnosti i sl. U poslovnim okruženjima dodatan problem predstavljaju i troškovi nabavke specijaliziranih alata za borbu protiv spama te smanjenje produktivnosti djelatnika s obzirom na iznimno velike količine spam poruka koje se svakodnevno primaju. S ciljem suzbijanja brojnih problema vezanih uz spam poruke razvijen je velik broj komercijalnih, ali i besplatnih alata čija je namjena detekcija i filtriranje neželjenih poruka elektroničke pošte. Jedan od besplatnih antispam alata je i K9 koji je analiziran u ovom dokumentu. K9 je programski proizvod čija je namjena filtriranje poruka elektronske pošte s ciljem njihova označavanja i odstranjivanja. Radi u konjunkciji s većinom popularnih e-mail klijenata koji koriste POP3 (engl. ***P**ost **O**ffice **P**rotocol*) protokol. Analiza alata izrađena je obuhvaćajući cjelokupan proces instalacije alata, njegova pokretanja, opis sučelja, popis opcija i njihova podešavanja, funkcioniranje alata u konjunkciji s e-mail klijentima te su iznesene zaključne preporuke.

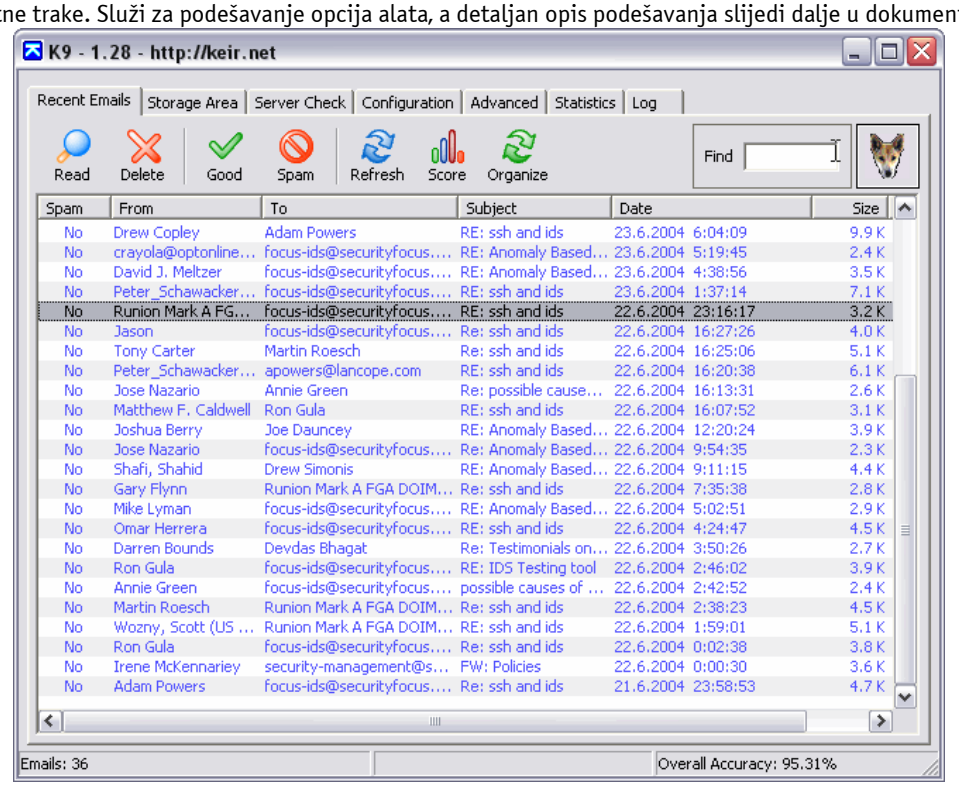
2. Instalacija i pokretanje

Za instalaciju antispam alata K9 potrebno je dohvatiti izvršnu datoteku s referentne adrese http://keir.net/k9.html i spremiti ju unutar određene mape na računalu. Datoteka je dostupna u `.zip` formatu pod imenom `k9v1.zip`, veličine 77 KB te u `.exe` formatu imena `k9v1setup.exe` i veličine 113 KB. Zadnja dostupna verzija alata iz travnja 2004. godine je 1.28. Ukoliko korisnik dohvati .zip datoteku, njenim raspakiravanjem pojavit će se dvije datoteke: `readme.txt` i `K9.exe`. Pokretanjem `K9.exe` datoteke, alat se automatski pokreće. Ukoliko se dohvati `.exe` datoteka, njenim pokretanjem započet će instalacijski postupak koji će instalirati program unutar mape `Program Files` na računalu.

3. Sučelje

Nakon pokretanja alata otvara se sučelje koje je prikazano na slici 1. Sučelje čini sedam kartica. To su `Recent Email`, `Storage Area`, `Server Check`, `Configuration`, `Advanced`, `Statistics` i `Log`. Na kartici `Recent Emails` nalazi se popis svih poruka elektroničke pošte koji su prošli filtriranje kroz alat. Ova kartica ujedno nudi mogućnost analiziranja i klasificiranja svih poruka. Na kartici se nalazi alatna traka s gumbima za čitanje sadržaja poruke (`Read`), brisanje poruka (`Delete`), korisničko klasificiranje poruka oznakom da nije spam (`Good`) ili je spam poruka (`Spam`), osvježavanje popisa poruka (`Refresh`), ocjenjivanje poruka od strane alata (`Score`), organiziranje poruka na disku (`Organize`), pretraživanje poruka (`Quick Find`) te ikona psa koja otvara K9 web

stranicu. Kartica `Storage Area` ima funkciju čuvanja poruka prema klasifikaciji na tzv. dobre poruke (engl. *Good*) ili na spam poruke (engl. *Spam*). Za razliku od prethodne kartice na kojoj se nalazi sedam prethodno opisanih naredbi, na ovoj su dodane dvije nove i to naredba koja otvara mapu u kojoj su spremljene dobre poruke (`Good`) i ona koja otvara mapu sa spam porukama (`Spam`). `Server check` kartica spada u napredne opcije alata. Njena funkcija je provjera POP3 poslužitelja pri čemu korisnik ima uvid u poruke prije nego li ih dohvati e-mail klijentom. Nove dvije naredbe, osim već spomenutih, su naredba za provjeru poruka na poslužitelju (`Check`) čime je omogućen pregled zaglavlja novih poruka te naredba za dohvaćanje poruka s POP3 poslužitelja (`Get`). Naredba `Get`, pri tome, ostavlja poruke na poslužitelju sve dok se one ne dohvate e-mail klijentom ili ne obrišu naredbom `Delete` na ovoj kartici. Kartica `Configuration` podijeljena je na četiri područja: `Proxy`, `Interface`, `Mark emails as Spam by...` i `Cleanup and Storage` i nema alatne trake. Služi za podešavanje opcija alata, a detaljan opis podešavanja slijedi dalje u dokumentu.



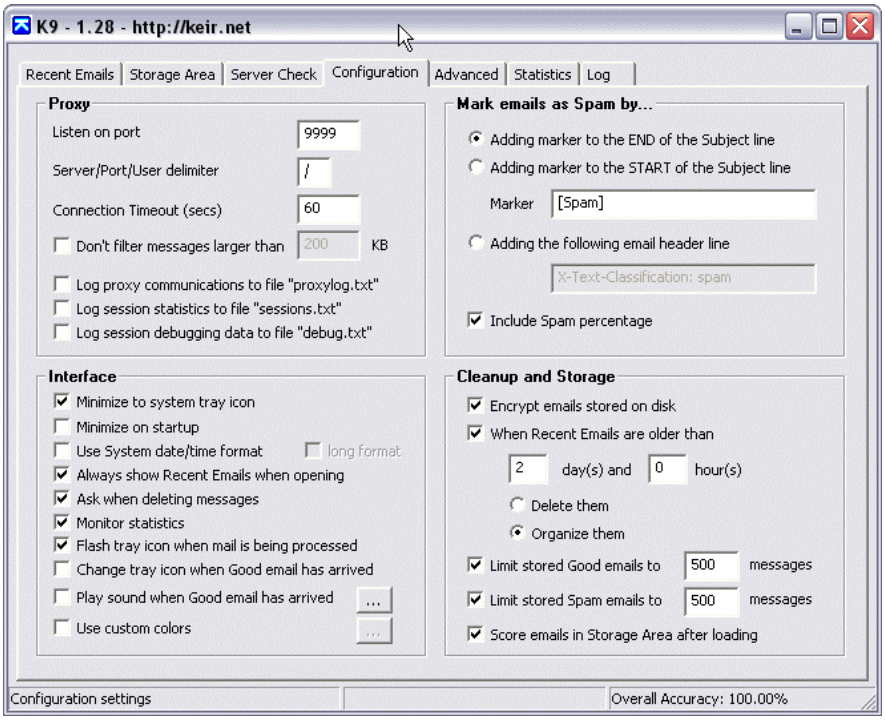
Slika 1: Sučelje K9 antipam alata K9

Za napredne korisnike alata kartica `Advanced` nudi mogućnost podešavanja naprednih opcija čiji detaljan opis također slijedi. Obzirom da alat nudi mogućnost klasifikacije poruka te njihova ocjenjivanja, opravdano je postojanje kartice `Statistics`. Kao i prethodna, nema alatne trake, a podijeljena je na dva područja po kojima se vodi statistika: `Email` i `Word databasess`. Posljednja kartica je kartica `Log` koja nudi pregled zapisa svih događaja i to u području `POP3 Proxy` te `Server Check`.

4. Podešavanje

Kao što je spomenuto, podešavanje opcija alata K9 izvodi se na kartici Configuration koja je prikazana na slici 2. Kartica je podijeljena na četiri područja: `Proxy`, `Interface`, `Mark emails as Spam by...` i `Cleanup and Storage`, a ta područja nude podešavanje postavki koje će utjecati na filtriranje poruka. Prilikom podešavanja opcija dovoljno je izmijeniti opciju i alat se odmah ažurira te sprema nove postavke. Nema posebne naredbe za spremanje postavki niti za vraćanje na standardne postavke. Obzirom da alat izvodi filtriranje poruka tako da ih presreće i analizira u trenutku kada e-

mail klijent pristupa POP3 poslužitelju, potrebno je izvršiti određene preinake i u postavkama e-mail klijenta.

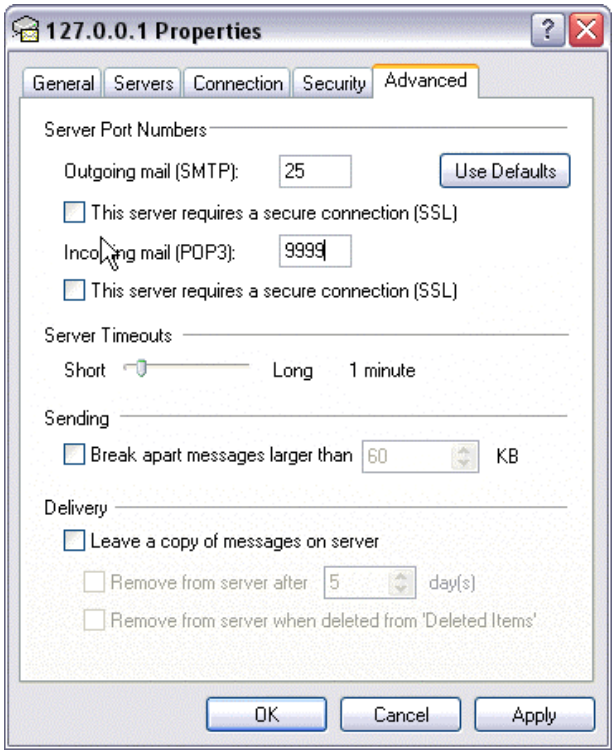


Slika 2: Kartica za podešavanje opcija alata s predefiniranim postavkama

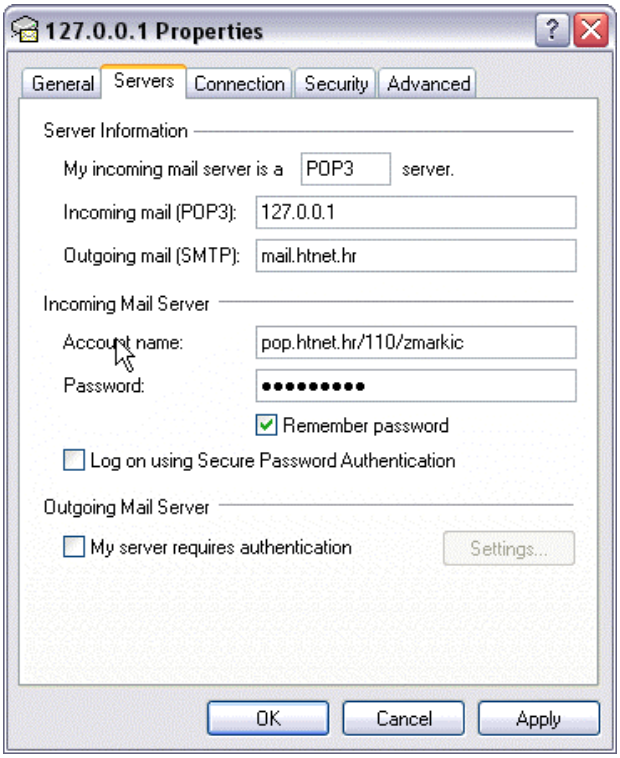
4.1. E-mail klijent

Kako bi se osiguralo da e-mail klijent ispravno komunicira s alatom K9 potrebno je izvršiti određene preinake. Preinake se odnose na promjenu broja porta POP3 poslužitelja i njegovu adresu. Predefinirani broj porta je `110`, dok K9 proxy poslužitelj koristi port `9999`. Također je potrebno promijeniti i adresu POP3 poslužitelja u `127.0.0.1` te korisničko ime. Postupak podešavanja tih opcija je slijedeći:

1. Pokrenuti e-mail klijent i alat K9.
2. Otvoriti dijaloški okvir u kojem se nalaze podaci za korisnički račun elektroničke pošte. U `Outlook Express` klijentu ovaj dijaloški okvir otvara se preko izbornika `Tools`, `Accounts...`, na kartici `Mail` potrebno je označiti željeni korisnički POP račun i kliknuti gumb `Properties` te otvoriti karticu `Advanced`.
3. U polju `Incoming mail (POP3)` broj `110` treba promijeniti u `9999` kao što je prikazano na slici 3.
4. Na kartici `Servers` potrebno je promijeniti adresu POP3 poslužitelja u polju `Incoming mail (POP3)`. Postojeća adresa mijenja se u `127.0.0.1`.
5. Korisničko ime (engl. *account name*) mijenja se iz postojećeg u korisničko ime oblika `POP3 poslužitelj/broj porta POP3 poslužitelja/korisničko ime` (npr. pop.htnet.hr/110/zmarkic). Slika 4 prikazuje nove postavke poslužitelja.



Slika 3: Promjena TCP porta za Incoming mail (POP3) poslužitelj kod Outlook Express klijenta



Slika 4: Podešavanje podataka poslužitelja kod Outlook Express klijenta za ispravnu komunikaciju s alatom

4.2. Proxy sekcija

`Proxy` sekcija ima namjenu kontrole POP3 *proxy* poslužitelja koji alat koristi za propuštanje poruka elektroničke pošte od POP3 poslužitelja do e-mail klijenta. Opcije koje se podešavaju u ovoj sekciji su:

1. Listen on port,
2. Server/Port/User delimiter,
3. Connection Timeout,
4. Don't filter messages larger than,
5. Log proxy communitacions to file „proxylog.txt“,
6. Log session statistics to file „sessions.txt“,
7. Log session debugging data to file „debug.txt“.

`Listen on port` opcija služi za upis broja porta koji *proxy* poslužitelj koristi. Predefinirana vrijednost je `9999`, no korisnik tu vrijednost može izmijeniti u bilo koji drugu imajući, pri tom, na umu da navedeni port ne smije koristiti niti jedan drugi servis ili aplikacija na računalu. Ukoliko se predefinirana vrijednost promijeni ovdje, ista mora biti podešena i u postavkama e-mail klijenta. `Server/Port/User Delimiter` opcija služi kako bi korisnik promijenio separator koji dijeli podatke unesene prilikom podešavanja e-mail klijenta. `Connection Timeout` opcija označava vrijeme nakon kojeg se prekida komunikacija s `POP3` poslužiteljem ukoliko nema odgovora. Opcija `Don't filter messages larger than` onemogućuje filtriranje velikih poruka (npr. poruke koje sadrže priložene datoteke koje korisnik očekuje). Preostale opcije omogućuju spremanje kopija poruka, statističkih podataka te cjelokupne mrežne komunikacije između e-mail klijenta, alata K9 i POP3 poslužitelja u, za to predviđene, datoteke.

4.3. Interface sekcija

Interface sekcija sadrži opcije čije podešavanje utječe na ponašanje alata, a čine ju:

1. Minimize to system tray icon (minimiziranje alata u *system tray*),
2. Minimize on startup (minimiziranje alata prilikom startanja),
3. Use system date/time format (korištenje sistemskog formata datuma i vremena),
4. Always show Recent E-mail when restoring window (prikazivanje poruka elektroničke pošte prilikom otvaranja sučelja alata),
5. Ask when deleting messages (potvrda prilikom brisanja poruka),
6. Monitor statistics (nadgledanje statistike),
7. Flash tray icon when mail is being processed (vizualizacija ikone alata prilikom filtriranje poruka),
8. Change tray icon when Good email has arrived (promjena izgleda ikone alata kada je primljena "dobra" poruka (Good),
9. Play sound when Good email has arrived (zvučna obavijest o primitku "dobre" poruke (Good).

4.4. Mark emails as Spam by… sekcija

Sekcija za označavanje poruka kao neželjenih poruka (spam) sastoji se od opcija koje utječu na izgled predmeta poruke koja je označena kao spam. Opcije koje se mogu podesiti su:

1. Adding marker to the END of the Subject line (dodavanje oznake na kraju predmeta poruke),
2. Adding marker to the START of the Subject line (dodavanje oznake na početku predmeta poruke),
3. Adding the following email header line (dodavanje korisnički definiranog zaglavlja poruke),
4. Include Spam percentage (prikaz postotka neželjene poruke).

4.5. Cleanup and Storage sekcija

Ova sekcija sadrži opcije kojima se izvodi podešavanje brisanja poruka te njihovo spremanje. Spremanje poruka može se izvoditi tako da se one enkriptiraju prilikom spremanja na disk (opcija *Encrypt emails stored on disk*) ili se organiziraju unutar mapa `Good i Spam`, nakon određenog broja dana (*When Recent Emails are older than*). Ista vrijednost za određivanje starosti poruke koristi se i prilikom definiranja brisanja poruka. Ostale mogućnosti brisanja podešavaju se definiranjem uvjeta za broj poruka unutar svake mape.

4.6. Napredno podešavanje

Kartica za napredno podešavanje nudi mogućnost podešavanja naprednih opcija koje su podijeljene na pet područja. To su:

1. Filter list,
2. POP3 Server Check,
3. Compatibility/Tweaks,
4. Blackhole List,
5. Automatic Email Program Configuration.

`Filter list` omogućuje korištenje korisnički definirane liste "dobrih" poruka (*whitelist*) te spam poruka (b*lacklist*). Korištenje ovih listi predefinirano je isključeno, no njihovim uključivanjem omogućuje se jednostavno kreiranje liste tako da se desnom tipkom miša označi poruka te se doda ili u crnu ili u bijelu listu. Svaka poruka se dodaje u željenu listu prema nekoliko kriterija. Kompletan opis kreiranja bijele i crne liste može se pročitati na stranci http://keir.net/k9_lists.html. Područje `POP3 Server Check` definira se ukoliko se želi koristiti mogućnost pregleda poruka na `POP3` poslužitelju, prije pristupa porukama e-mail klijentom. Podešavanje ovog područja identično je podešavanju `POP3` korisničkog računa u bilo kojem e-mail klijentu. Potrebno je upisati naziv korisničkog računa, `POP3` poslužitelj, korisničko ime i lozinku. Maksimalan broj korisničkih računa ovdje definiranih je 16. `Compatibility/Tweaks` područje nudi nekoliko opcija koje utječu na način primanja poruka elektroničke pošte, definiranje naredbi kojima će e-mail klijent pristupati POP3 poslužitelju te na koji način će one biti ocjenjivane i spremane. `Blackhole List` omogućuje korištenje `DNSBL` (*DNS Blackhole List*) koja predstavlja listu računala identificiranih po IP adresi kao računala koja aktivno sudjeluju u slanju spam poruka, namjerno ili slučajno. Uključivanjem ove opcije alat K9 sudjeluje u identifikaciji takvih računala šaljući IP adrese identificirani u zaglavlju poruke. `Automatic Email Program Configuration` omogućuje automatsko podešavanje s e-mail klijentom u slučaju promjene korisničkih računa ili dodavanja novih te povratak postavki e-mail klijenta na prethodne.

Alat omogućuje dodatnu prilagodbu o kojoj se više može pročitati na referentnoj adresi http://keir.net/k9_advanced.html.

5. Funkcionalnost

Nakon opisa sučelja te mogućih podešavanja alata, većina mogućnosti alata već je došla do izražaja. Osnova podešavanja predstavlja podešavanje e-mail klijenta koji će pristupati porukama preko K9 alata. Alat omogućuje kompletnu zaštitu od spam poruka na dva osnovna načina. Prvi način je pristup porukama na samom `POP3` poslužitelju gdje se označavanjem poruka kao dobrih ili spam izvodi kategorizacija. Prednost ovog načina jest što korisnik odmah na poslužitelju može obrisati poruke kojima ne želi pristupiti e-mail klijentom te će na taj način smanjiti troškove pristupa nepoželjnim porukama. Drugi, osnovni, način je pristup porukama istovremeno kada im pristupa i e-mail klijent. Preporučljivo je korištenje bijele i crne korisničke liste čime se mogućnost prepoznavanja nepoželjnih poruka povećava. Ova dva načina rade potpuno neovisno. Osnovni način rada predstavlja pregled poruka prilikom pristupa e-mail klijenta, a ukoliko se poruke žele provjeravati na poslužitelju, tu opciju korisnik mora posebno podesiti te ju koristiti manualno. K9 alat će, prilikom filtriranja, poruku definiranu kao neželjenu, označiti kao spam prema zadanim pravilima filtriranja. Akcije koje se poduzimaju za spam poruke su ili njihovo smještanje u, za to, kreiranu mapu ili njihovo brisanje.

Kreiranje mape izvodi se unutar e-mail klijenta nakon čega se mora definirati pravilo koje će svaku poruku koja zadovoljava zadani kriterij automatski smještati u predviđenu mapu. Postupak kreiranja mape za spam poruke za Outlook Express e-mail klijent je slijedeći:

1. Desnom tipkom miša kliknuti na mapu `Inbox` i odabrati `New folder`... naredbu.
2. Upisati ime nove mape "`Spam`" (ime mape je proizvoljno) i kliknuti `OK`.
3. Odabrati izbornik Tools | Message Rules | Mail... kako bi se otvori dijaloški okvir `Message Rules window`.
4. Kliknuti dugme New.
5. U prikazanom okviru označiti opciju `Where the Subject line contains specific words`.

6. U polju za definiranje pravila kliknuti plavim slovima ispisane riječi `specific words`.
7. U dijaloškom okviru koji se pojavio upisati riječ `[Spam]` i kliknuti dugme `Add` pa `OK`.
8. U okviru `Select the Actions for your rule section` odabrati opciju `Move it to the specified folder`.
9. U polju za definiranje pravila kliknuti plavim slovima ispisane riječi `specified folder`.
10. Odabrati mapu `Spam` i kliknuti `OK`.
11. Pravilo imenovati proizvoljno i kliknuti `OK`.
12. Kliknuti dugme `OK` za zatvaranje dijaloškog okvira `Message Rules window`.

Mogućnost programa da samostalno organizira poruke, na temelju korisničke kategorizacije, vrlo je jednostavna za korištenje pomoću naredbe `Organize`. Ova organizacija odnosi se samo na poruke koje su prošle filtriranje alatom i nikako ne utječe na organizaciju poruka unutar e-mail klijenta. Ukoliko je alat instaliran putem .exe datoteke, onda se poruke organiziraju unutar mape `C:\Program Files\KeirNet\K9\Emails`, a ukoliko se koristila .zip datoteka s alatom koji se starta bez prethodne instalacije, poruke su organizirane unutar mape `C:\Documents and Settings\<user>\Application Data\K9\Emails`.

Osim prethodno navedenih podešavanja, alat nudi i kartice za pregled aktivnosti alata. Kartica `Statistics` omogućuje pregled statističkih podataka o filtriranim porukama. `Log` kartica nudi pregled svih aktivnosti alata prema POP3 poslužitelju.

Nedostatak programa je taj što podržava isključivo POP3 protokol dok IMAP, Webmail i ostali servisi u trenutnoj inačici nisu podržani.

6. Zaključak

K9 je jednostavan alat za filtriranje nepoželjnih poruka elektroničke pošte, a nakon detaljnog podešavanja alata, korisniku omogućuje neometan rad.

Obzirom na činjenicu da spam poruke predstavljaju ozbiljan sigurnosni problem, korištenje antispam alata postaje neizbježno. Svojim mogućnostima K9 predstavlja ozbiljnog kandidata među ovom grupom alata te je svakako preporučljiv za implementaciju, naročito kućnim korisnicima i manjim tvrtkama koje nemaju nadzor nad e-mail poslužiteljima putem kojih primaju elektroničku poštu. Za sva dodatna pitanja preporučljivo je pogledati listu najčešće postavljenih pitanja na referentnoj adresi http://keir.net/k9_faq.html gdje se, između ostalog, mogu pronaći i brojni napuci za podešavanje alata za rad s Eudora ili Netscape Navigator klijentima.