

Antivirusni i *content security* softver

# eScan i MailScan

*eScan i MailScan sličnih su mogućnosti: oba mogu skenirati sve e-mail poruke koje dolaze ili odlaze s računala te ukloniti viruse, trojanske konje i crve, kao i poruke koje sadrže neželjene sadržaje ili ključne riječi. eScan je namijenjen korištenju na klijentskim računalima i radnim stanicama, dok je MailScan softver koji ćete instalirati na središnji e-mail poslužitelj u tvrtki kako biste dobili zaštitu za cijeli e-mail sustav*

piše: **Dario Sušanj** • dario@pcchip.hr

**V**irusne prijetnje ne jenjavaju, a borba protiv crva, virusa i održavanje "čiste" okoline može biti itekako velik problem u tvrtkama. Na računala vrlo često nisu instalirane odgovarajuće nadogradnje koje "krpaju" sigurnosne rupe u e-mail klijentima, što stvara plodno tlo za širenje crva i virusa. Nepotrebno je naglašavati kakvu štetu crvi i virusi nanose svakoj kompaniji: ne radi se samo o potencijalnom gubitku podataka, već i negativnim utjecajima na e-mail poslužitelj (koji se, pod navalom crva, može jednostavno srušiti), a o srušenom ugledu kod klijenata i poslovnih partnera da niti ne govorimo. Korištenje antivirusnog softvera koji pregledava svaku datoteku u realnom vremenu (prilikom pokretanja aplikacija ili otvaranja dokumenata) može, dakako, znatno pomoći u uklanjanju virusne prijetnje, no u posljednje je vrijeme - s obzirom na to da se većina crva širi putem elektroničke pošte - korištenje e-mail skenera gotovo neophodno.

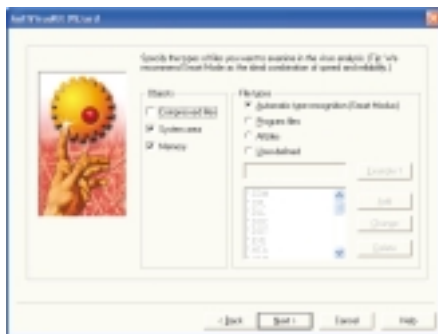
eScan, proizvod tvrtke Microworld Technologies, jedan je od takvih proizvoda na tržištu. Korištenjem MWL tehnologije - Microworld Winsock Layer - ovaj se proizvod zapravo "uvlači" vrlo duboko u operativni sustav, na razinu samog Winsocka, sučelja koje osigurava TCP/IP komunikaciju. To eScanu omogućava da skenira i očisti viruse ili crve u elektroničkim porukama prije nego što poruke uopće stignu do mail klijenta, poput Outlooka, Outlook Expressa, Eudora ili Netscapea. Prednosti ovakvog načina rada ima mnogo: sustav je neovisan o e-mail klijentu koji se koristi, a nijedna poruka ne može otići van ili stići na računalo a da pritom ne bude pregledana. Jedino što će korisnici primijetiti jest naznaka na svakoj e-mail poruci da je i ona pregledana, te to da poruke iz e-mail klijenta odlaze trenutačno, a potom ih eScan pregledava i u pozadini šalje. Rad eScana potpuno je transparentan te ga, osim kratke poruke na kraju svakog e-maila koja potvrđuje da je poruka pregledana, gotovo nećete niti primijetiti.

eScan, dakako, nudi i standardne mogućnosti antivirusnog softvera: pregledavanje diskova, memorije, datoteka i samih sektora na disku, te sistemskih područja diska (boot sektor, *master boot*

*record*, tablica particija). eScan, dakako, otkriva razne vrste virusa, uključujući i polimorfne te *stealth* viruse, kao i makro viruse koji se šire kroz Office aplikacije. No, ono što je zanimljivo jest da eScan također koristi heuristički analizator koda koji, prema tvrdnjama Microworld Technologies, proizvođača ovog softvera, može analiziranjem koda otkriti oko 80 posto nepoznatih virusa. Popis poznatih virusa nadopunjuje se svaki dan, a eScan ga preuzima automatski, no uvjete spajanja na Internet možemo sami definirati (eScan prepoznaje dostupnost internetske veze, te aktivira *update* kada je veza na raspolaganju). Budući da je dnevni *update* malen, rijetko kada ćete "skinuti" više od 10-15 kilobajta.

eScan također može skenirati sažete datoteke (arhive), može automatski provjeravati sve datoteke preuzete s weba te, ako to želimo, automatski blokira izvršavanje svih VBS skriptata koji su glavni način aktivacije crva koji stižu s e-mail porukama. Ako se unutar neke poruke nalazio privitak neželjenog tipa (primjerice, izvršiva EXE datoteka), eScan će je, ako je ta opcija uključena, automatski ukloniti iz poruke. Postoji također i eScan Enterprise Edition, koji olakšava distribuciju nadogradnji diljem cijele računalne mreže, a uz Corporate Edition dolaze i Content-Monitor i Content-Administrator koji omogućavaju detaljno stvaranje pravila za pregledavanje elektroničke pošte te definiranje elektroničkih poruka koje se šalju kao upozorenje kada bude pronađen virus ili crv. eScan također posjeduje lokalni filtar za sadržaje koji omogućava filtriranje neželjenih poruka.

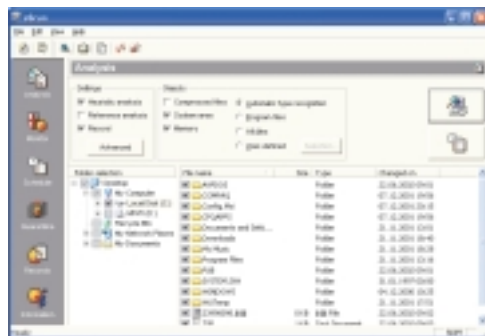
U okruženjima većih mreža uz antivirusni softver dobro je imati i *content security* softver, dakle program koji će pregledavati sav promet putem e-maila te automatski otklanjati svaki sigurnosnu



**AntiVirus Wizard:** Određivanje vrsta datoteka koje program ispituje



**eScan Monitor:** Odredite kako će program postupati ako nađe virus



**Analiza:** Način na koji program određuje što je virus, a što nije

prijetnju ili prenošenje neželjenih sadržaja. MailScan je također rješenje tvrtke Microworld Technologies, a postoji u desetak verzija za različite e-mail poslužitelje. Osim MailScana za MDAEMON, VPOP3, WinRoute i PostMaster, MailScan postoji i za komercijalne poslužitelje poput Microsoft Exchangea i Lotus Notusa, te one poput MailGatea, WinGatea, CMaila i sličnih. Iako je MailScan primarno namijenjen e-mail poslužiteljima za Windowse, čak i ako kao e-mail poslužitelj koristite Linux, Unix ili Novell Groupwise, postoji odgovarajuća verzija softvera, MailScan for SMTP Servers, rješenje koje će raditi s bilo kojim standardnim SMTP poslužiteljem. Dakle, bez obzira na to za koju se verziju odlučili, dovoljno je MailScan instalirati na središnji e-mail poslužitelj u tvrtki, kako bi mogao pregledati cjelokupnu komunikaciju između lokalnih korisnika, te poštu koja ide prema Internetu ili s njega dolazi. Radi na način sličan eScanu: integrira se u sustav na razini Winsocka te pregledava sve poruke prije nego što one uopće budu isporučene. Zahvaljujući takvom načinu rada, na samom e-mail poslužitelju nisu potrebne nikakve modifikacije postavki, a nije potrebno niti posjedovati dedikirani, specijalizirani poslužitelj (*gateway*) na kojemu bi se MailScan koristio: on se može nalaziti na istom poslužitelju koji služi i kao e-mail server. ☑

## eScan i MailScan

Antivirusni i *content security* paketi

Microworld Technologies

Cijena: Na upit

Pardus, (01) 2344-042, www.pardus.hr

www.mwti.net