Antivirusni i firewall programi

U rečnicima računarskih termina, pored reči virus obično piše - virus (zlonamerni kod) je računarski program, koji je napisan sa namerom da se nanese šteta tj. da se poremeti ili uništi naš rad kao i rad samog računara.

Iz tih razloga za sigurnost pri razmeni podataka i komunikaciji sa drugim korisnicima, neophodno je razumevanje pojave **računarskih virusa, trojanaca i Internet "crva" (worm).** Najveća opasnost od virusa je to što mnogi virusi ostaju neprimećeni sve dok ne naprave štetu.

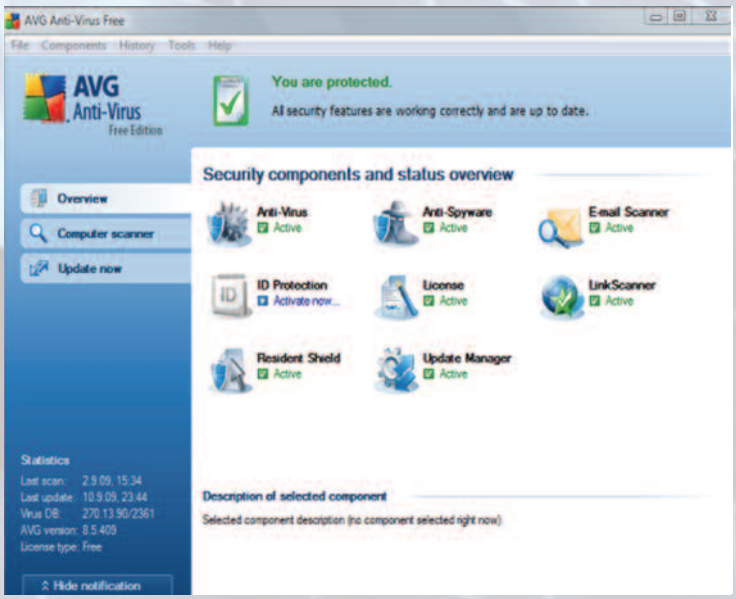
Viruse današnje generacije u odnosu na predhodnike karakteriše veća moć i veća brzina širenja. Prvi virusi, krajem osamdesetih godina širili su se deljenjem disketa. Sledeća generacija virusa, koja se pojavila krajem devedesetih su makro virusi. Oni su se najčešće prenosili preko Word dokumenata, i širili putem elektronske pošte.

Virusi koji se prenose preko velikog broja elektronskih poruka poznati pod imenom crvi su virusi savremene generacije. Oni se "razmnožavaju" (kopiraju) i šalju sve adrese iz imenika sa adresama elektronske pošete. Jedan od najpoznatijih crva, pre svega zbog štete koju je izazvao je Sasser. On je u 2004. dominirao Internetom punih pet dana i zarazio milione računara. Broj računara koje je Sasser napadao svakog sata bio je 200.000. Procenjuje se da je do septembra 2004. ovaj crv zarazio milion računara a šteta koju je izazvao je približno 979 miliona dolara.

Naravno, na računarskim sistemima su prisutne sve generacije virusa.

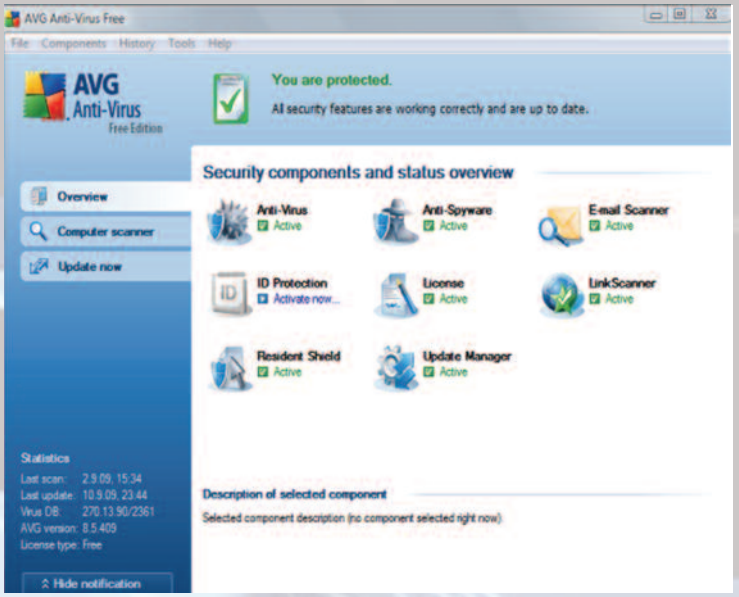
Analitičari računarske bezbednosti tvrde da najveća opasanost za većinu računara ne dolazi direktno spolja, nego iznutra. Pre svega to su tzv. trojanci tj, programi sa sporednim ulazom koje smo instalirali jer su izgledali kao korisni alati koje smo preuzeli sa Intreneta ili bezopasni prilozi (attachments) elektronske pošte.

Protiv virusa se borimo antivirus programom. Antivirus program mora biti temeljan, brz i precizan. Na softverskom tržištu prisutan je veliki broj antivirus programa. Po rezultatima ispitivanja analitičara bezbednosti antivirus programi, koji automatski nude ažuriranje definicija i koji dobro reaguju na pretnje su: **Kaspersky, ETrust, Trend Micro, Norton, McAfree, AVG - anti-virus.**



Slika 1. AVG antivirus program

Antivirus programi nas štite od velikog broja računarskih virusa ali nemogu da spreče sve napade na računarski sistem, kao što je npr. pokušaj hakera da uđe u naš sistem i sazna lozinke. Za zaštitu mreže od nedozvoljenog pristupa u organizacijama je zadužen administrator sistema. On postavlja **tzv. zaštitni zid (firewall)** koji zloamernim korisnicima ne dozvoljava pristup mreži. Osnovini zadatak zaštitnog zida je da prati svaku od 65.536 mogućih adresa TCP I UDP priključaka koje sistem koristi za komunikaciju sa drugim računarima. Firewal programi koji se danas najčešće koriste su: **ZoneAlarm, Cleaner, BlackIce, McAfee Firefall i Norton Personal Firewall.**



Slika 2. Firewall program

Korisnik može da isključi zaštitu Firewall ili da odobri pristup softverima za koje smatra da su iz pouzdanih izvora. Potuno isključivanje Firewall programa nije preporučljivo, jer računar ostaje bez standardne antivirusne zaštite.