



AVG Internet Security 2012

Priručnik za korisnike

Revizija dokumenta 2012.20 (3/29/2012)

Copyright AVG Technologies CZ, s.r.o. Sva prava zadržana.
Svi ostali žigovi su vlasništvo njihovih dotičnih vlasnika.

Ovaj proizvod koristi RSA Data Security, Inc. MD5 Message-Digest algoritam, Copyright (C) 1991-2, RSA Data Security, Inc., kreirano 1991. godine.

Ovaj proizvod koristi kôd iz C-SaCzech biblioteke, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Ovaj proizvod koristi biblioteku kompresije zlib, Copyright (c) 1995-2002 Jean-loup Gailly i Mark Adler.

Ovaj proizvod koristi biblioteku kompresije libbzip2, Copyright (c) 1996-2002 Julian R. Seward.



Sadržaj

1. Uvod	7
2. Zahtevi za instalaciju programa AVG	8
2.1 Podržani operativni sistemi	8
2.2 Minimalni i preporučeni hardverski zahtevi	8
3. Proces instalacije programa AVG	9
3.1 Dobro došli: izbor jezika	9
3.2 Dobro došli: Ugovor o licenciranju	10
3.3 Aktivirajte licencu	11
3.4 Izaberite tip instalacije	12
3.5 Prilagođene opcije	14
3.6 Instalirajte AVG bezbednosnu traku sa alatima	15
3.7 Tok instalacije	16
3.8 Instalacija je uspešno obavljena	17
4. Nakon instalacije	18
4.1 Registracija proizvoda	18
4.2 Pristup korisničkom interfejsu	18
4.3 Skeniranje celog računara	18
4.4 Eicar test	18
4.5 Podrazumevana AVG konfiguracija	19
5. AVG korisnički interfejs	20
5.1 Sistemski meni	21
5.1.1 Datoteka	21
5.1.2 Komponente	21
5.1.3 Istorija	21
5.1.4 Alati	21
5.1.5 Pomoć	21
5.1.6 Podrška	21
5.2 Informacije o bezbednosnom statusu	29
5.3 Brze veze	30
5.4 Pregled komponenti	30
5.5 Ikona sistemske palete	32
5.6 AVG Savetnik	34
5.7 AVG gadžet	34

6. Komponente programa AVG	37
6.1 Antivirusni program	37
6.1.1 Mašina za skeniranje	37
6.1.2 Stalna zaštita	37
6.1.3 Zaštita od špijunskog softvera	37
6.1.4 Interfejs antivirusnog programa	37
6.1.5 Detekcije stalnog štita	37
6.2 LinkScanner	43
6.2.1 Interfejs komponente LinkScanner	43
6.2.2 Detekcije štita za pretraživanje	43
6.2.3 Detekcije štita za pregledanje Interneta	43
6.2.4 Online Shield detekcije	43
6.3 Zaštita e-pošte	48
6.3.1 Skener e-pošte	48
6.3.2 Odbrana od bezvredne pošte	48
6.3.3 Interfejs zaštite e-pošte	48
6.3.4 Detekcija od strane skenera e-pošte	48
6.4 Zaštitni zid	52
6.4.1 Principi funkcionisanja zaštitnog zida	52
6.4.2 Profili zaštitnog zida	52
6.4.3 Interfejs zaštitnog zida	52
6.5 Anti-Rootkit	56
6.5.1 Interfejs komponente Anti-Rootkit	56
6.6 Sistemske alatke	58
6.6.1 Procesi	58
6.6.2 Mrežne veze	58
6.6.3 Automatsko pokretanje	58
6.6.4 Proširenja pregledača	58
6.6.5 LSP prikazivač	58
6.7 PC Analyzer	64
6.8 Identity Protection	65
6.8.1 Interfejs zaštite identiteta	65
6.9 Daljinska administracija	67
7. Moje aplikacije	69
7.1 AVG Family Safety	69
7.2 AVG LiveKive	70
7.3 AVG Mobilation	70



7.4 AVG PC Tuneup	71
8. AVG Security Toolbar	73
9. AVG Do Not Track	75
9.1 AVG Do Not Track interfejs	76
9.2 Informacije o procesima praćenja	77
9.3 Blokiranje procesa praćenja	78
9.4 AVG Do Not Track postavke	78
10. AVG napredna podešavanja	81
10.1 Izgled	81
10.2 Zvuci	84
10.3 Privremeno onemogućiti AVG zaštitu	85
10.4 Anti-Virus	86
10.4.1 Stalni štiti	86
10.4.2 Keš server	86
10.5 Zaštita e-pošte	92
10.5.1 Skener e-pošte	92
10.5.2 Odbrana od bezvredne pošte	92
10.6 LinkScanner	109
10.6.1 Postavke Skenera linkova	109
10.6.2 Online Shield	109
10.7 Skeniranja	113
10.7.1 Skeniranje celog računara	113
10.7.2 Skeniranje proširenja ljske	113
10.7.3 Skeniranje datoteka ili fascikli	113
10.7.4 Skeniranje prenosnog uređaja	113
10.8 Planovi	119
10.8.1 Planirano skeniranje	119
10.8.2 Plan ažuriranja definicija	119
10.8.3 Plan ažuriranja programa	119
10.8.4 Plan ažuriranja Anti-Spam komponente	119
10.9 Ažuriranje	130
10.9.1 Proxy	130
10.9.2 Pozivna veza	130
10.9.3 URL adresa	130
10.9.4 Upravljanje	130
10.10 Anti-Rootkit	136

10.10.1 Izuzeci	136
10.11 Identity Protection	138
10.11.1 Postavke zaštite identiteta	138
10.11.2 Lista „Dozvoljeno“	138
10.12 Potencijalno neželjeni programi	142
10.13 Skladište za viruse	145
10.14 Program za poboljšanje proizvoda	145
10.15 Zanemari status greške	148
10.16 Savetnik - poznate mreže	149
11. Podešavanja zaštitnog zida	150
11.1 Opšte postavke	150
11.2 Bezbednost	151
11.3 Profili za oblasti i adaptere	152
11.4 IDS	153
11.5 Datoteke evidencije	155
11.6 Profili	156
11.6.1 Informacije o profilu	156
11.6.2 Definisane mreže	156
11.6.3 Aplikacije	156
11.6.4 Sistemske usluge	156
12. Skeniranje programom AVG	167
12.1 Interfejs za skeniranje	167
12.2 Unapred definisana skeniranja	168
12.2.1 Skeniranje celog računara	168
12.2.2 Skeniraj određene datoteke ili fascikle	168
12.3 Skeniranje u programu Windows Explorer	177
12.4 Skeniranje komandne linije	177
12.4.1 Parametri za skeniranje iz komandne linije	177
12.5 Planiranje skeniranja	180
12.5.1 Postavke planiranja	180
12.5.2 Kako skenirati	180
12.5.3 Šta skenirati	180
12.6 Pregled rezultata skeniranja	190
12.7 Detalji rezultata skeniranja	191
12.7.1 Kartica Pregled rezultata	191
12.7.2 Kartica Zaraze	191
12.7.3 Kartica Špijunski softver	191



12.7.4 Kartica Upozorenja	191
12.7.5 Kartica Rootkit programi	191
12.7.6 Kartica Informacije	191
12.8 Skladište za viruse	198
13. Ažuriranje programa AVG	201
13.1 Pokretanje ažuriranja	201
13.2 Tok ažuriranja	201
13.3 Nivoi ažuriranja	202
14. Istorija događaja	203
15. Najčešća pitanja i tehnička podrška	205



1. Uvod

Ovo korisničko uputstvo sadrži sveobuhvatnu dokumentaciju za **AVG Internet Security 2012**.

AVG Internet Security 2012 pruža više slojeva zaštite za sve što radite na mreži, što znači da ne morate brinuti oko krađe identiteta, virusa ili posećivanja štetnih lokacija. AVG zaštitna tehnologija u oblaku i AVG mreža za zaštitu zajednice su uključene, što znači da prikupljamo najnovije informacije o pretnjama i delimo ih sa zajednicom da bismo se uverili da dobijate najbolju zaštitu:

- Kupujte i obavljajte bankarske poslove na mreži bezbedno uz AVG zaštitni zid, odbranu od bezvredne pošte i zaštitu identiteta
- Ostanite bezbedni na društvenim mrežama pomoću AVG zaštite društvenog umrežavanja
- Pregledajte i pretražujte Internet pouzdano uz LinkScanner zaštitu u realnom vremenu



2. Zahtevi za instalaciju programa AVG

2.1. Podržani operativni sistemi

AVG Internet Security 2012 je namenjen zaštiti radnih stanica na kojima se koriste sledeći operativni sistemi:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 i x64, sva izdanja)
- Windows 7 (x86 i x64, sva izdanja)

(i eventualno noviji servisni paketi za određene operativne sisteme)

Napomena: komponenta [Identity Protection](#) nije podržana u operativnom sistemu Windows XP x64. Na ovom operativnom sistemu možete da instalirate AVG Internet Security 2012, ali bez komponente Identity Protection.

2.2. Minimalni i preporučeni hardverski zahtevi

Minimalni hardverski zahtevi za **AVG Internet Security 2012**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM memorije
- 1000 MB slobodnog prostora na čvrstom disku (za potrebe instalacije)

Preporučeni hardverski zahtevi za **AVG Internet Security 2012**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM memorije
- 1550 MB slobodnog prostora na čvrstom disku (za potrebe instalacije)



3. Proces instalacije programa AVG

Gde mogu da preuzmem instalacionu datoteku?

Da biste instalirali **AVG Internet Security 2012** na svoj računar, potrebna vam je najnovija instalaciona datoteka. Da biste se uverili da instalirate najnoviju verziju programa **AVG Internet Security 2012**, preporučuje se da instalacionu datoteku preuzmete sa AVG Web lokacije (<http://www.avg.com/>). Odeljak **Centar za podršku / preuzimanje** pruža strukturisani pregled instalacionih datoteka za svako AVG izdanje.

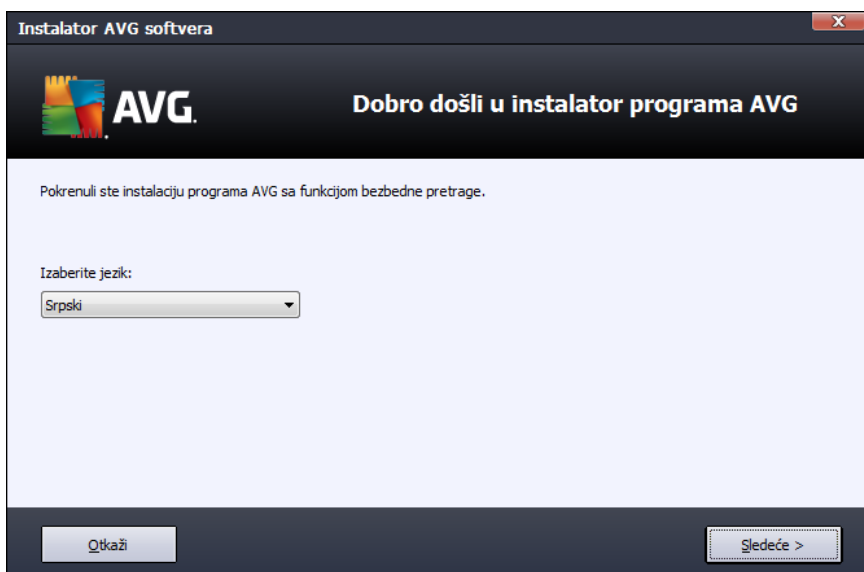
Ako niste sigurni koje datoteke treba da preuzmete i instalirate, možete koristiti uslugu **Izbor proizvođa** na dnu Web stranice. Kada odgovorite na tri jednostavna pitanja, ova usluga definiše tačne datoteke koje su vam potrebne. Kliknite na dugme **Nastavi** da biste bili preusmereni na kompletnu listu datoteka za preuzimanje, koje su prilagođene za vaše lične potrebe.

Kako izgleda proces instalacije?

Nakon što preuzmete instalacionu datoteku i sačuvate je na čvrstom disku, možete pokrenuti proces instalacije. Instalacija predstavlja sekvencu jednostavnih dijaloga lakih za razumevanje. Svaki dijalog ukratko opisuje šta treba raditi u svakom koraku procesa instalacije. Zatim pružamo detaljno objašnjenje svakog dijaloga:

3.1. Dobro došli: izbor jezika

Proces instalacije započinje dijalogom **Dobro došli u AVG program za instalaciju**:



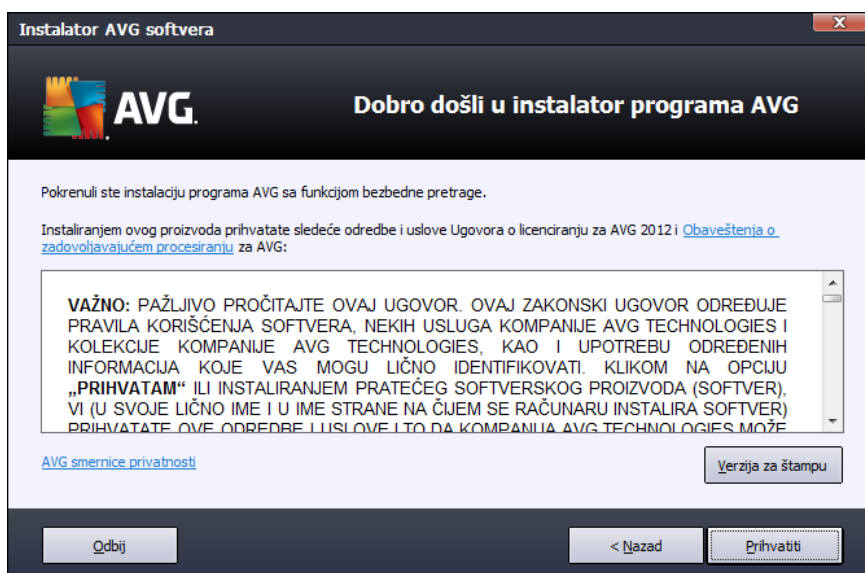
U ovom dijalogu možete izabrati jezik koji će se koristiti za proces instalacije. U desnom uglu dijaloga kliknite na kombinovani okvir da biste došli do padajućeg menija sa jezicima. Izaberite željeni jezik i proces instalacije će se nastaviti na izabranom jeziku.



Pažnja: trenutno birate samo jezik procesa instalacije. AVG Internet Security 2012 aplikacija će se instalirati na izabranom jeziku i na engleskom jeziku koji je uvek automatski instaliran. Međutim, moguće je instalirati više jezika i raditi sa programom AVG Internet Security 2012 na svakom od njih. Od vas će se tražiti da potvrdite pun izbor alternativnih jezika u jednom od sledećih dijaloga za instalaciju pod imenom [Prilagođene opcije](#).

3.2. Dobro došli: Ugovor o licenciranju

U sledećem koraku, dijalog **Dobro došli u AVG program za instalaciju** obezbeđuje kompletan tekst AVG ugovora o licenciranju:



Pažljivo pročitajte ceo tekst. Da biste potvrdili da ste pročitali, razumeli i prihvatili ugovor pritisnite dugme **Prihvati**. Ako se ne slažete sa uslovima ugovora o licenciranju kliknite na dugme **Odbij**, čime ćete odmah prekinuti proces instalacije.

AVG smernice privatnosti

Pored ugovora o licenciranju, ovaj dijalog za instalaciju pruža i opciju da saznate više o AVG smernicama privatnost. U levom uglu dijaloga možete videti vezu **AVG smernice privatnosti**. Kliknite na nju da biste bili preusmereni na AVG Web lokaciju (<http://www.avg.com/>) gde možete videti kompletne principe smernica za privatnost preduzeća AVG Technologies.

Kontrolna dugmad

U prvom dijalogu za instalaciju dostupna su samo dva kontrolna dugmeta:

- **Verzija za štampanje** - kliknite da biste odštampli ceo tekst AVG ugovora o licenciranju.
- **Odbij** - kliknite da biste odbili ugovor o licenciranju. Proces instalacije će se odmah

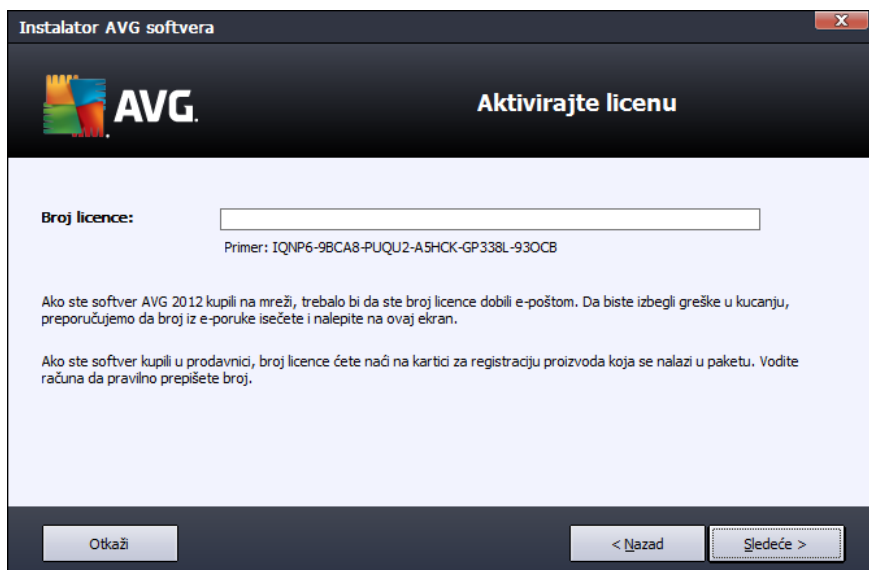


obustaviti. **AVG Internet Security 2012** neće biti instaliran!

- **Nazad** - kliknite da biste se vratili za jedan korak unazad na prethodni dijalog za instalaciju.
- **Prihvati** - kliknite da biste potvrdili da ste pročitali, razumeli i prihvatili ugovor o licenciranju. Instalacija će se nastaviti i preći ćete na sledeći korak u narednom dijalogu za instalaciju.

3.3. Aktivirajte licencu

U dijalogu **Aktivirajte vašu licencu** pozivate se da unesete broj vaše licence u ponuđeno tekstualno polje:



Gde se nalazi broj licence

Prodajni broj se može pronaći na pakovanju CD-a u kutiji programa **AVG Internet Security 2012**. Broj licence će se nalaziti u potvrdnoj e-poruci koju ste dobili nakon kupovine programa **AVG Internet Security 2012** na Internetu. Morate uneti broj tačno onako kao što je prikazan. Ako je broj licence dostupan u digitalnom obliku (*u e-poruci*), preporučujemo da ga umetnete metodom kopiranja i nalepljivanja.

Kako se koristi metod „Kopiranje i lepljenje“

Korišćenje metoda **Kopiranje i lepljenje** za unos **AVG Internet Security 2012** broja licence u program obezbeđuje pravilan unos broja. Pratite sledeće korake:

- Otvorite e-poruku koja sadrži broj licence.
- Kliknite levim tasterom miša na početak broja licence, zadržite i prevucite miš do kraja broja, a zatim otpustite dugme. Broj bi sada trebalo da bude markiran.



- Pritisnite i zadržite taster **Ctrl**, a zatim pritisnite taster **C**. Ovo će kopirati broj.
- Postavite pokazivač i kliknite na mesto na kojem želite da nalepite kopirani broj.
- Pritisnite i zadržite taster **Ctrl**, a zatim pritisnite taster **V**. Ovo će nalepiti broj na lokaciju koju ste izabrali.

Kontrolna dugmad

Kao i u većini dijaloga za instalaciju, dostupna su tri kontrolna dugmeta:

- **Otkazi** - kliknite da biste odmah napustili proces instalacije; **AVG Internet Security 2012** neće biti instaliran!
- **Nazad** - kliknite da biste se vratili za jedan korak unazad na prethodni dijalog za instalaciju.
- **Dalje** - kliknite da biste nastavili sa instalacijom i prešli na sledeći korak.

3.4. Izaberite tip instalacije

Dijalog **Izaberite tip instalacije** nudi izbor od dve opcije za instalaciju: **Brza** i **Prilagođena instalacija**:



Brza instalacija

Za većinu korisnika se preporučuje da se drže standardne **Brze** instalacije koja instalira **AVG Internet Security 2012** u potpuno automatizovanom režimu sa podešavanjima koje je prodavac programa unapred definisao, uključujući [AVG gadžet](#). Ova konfiguracija obezbeđuje maksimalnu



bezbednost i optimalnu zauzetost resursa. Ako kasnije bude potrebno da promenite konfiguraciju, to ćete uvek moći da uradite direktno u aplikaciji **AVG Internet Security 2012**.

U okviru ove opcije možete videti dva unapred označena polja i preporučuje se da ostavite obe opcije označene:

- **Želeo/želela bih da podesim AVG Bezbednu pretragu kao moj podrazumevani pretraživač** - ostavite označeno ako želite da koristite pretraživač „AVG bezbedna pretraga“ koji je u bliskoj saradnji sa komponentom [Link Scanner](#) radi vaše maksimalne bezbednosti na mreži.
- **Želeo/želela bih da instaliram AVG bezbednosnu traku sa alatkama** - ostavite označeno da biste instalirali [AVG bezbednosnu traku sa alatkama](#) koja vam obezbeđuje maksimalnu bezbednost dok pregledate Internet.

Kliknite na dugme **Dalje** da biste prešli u sledeći dijalog [Instaliranje AVG bezbednosne trake sa alatkama](#).

Prilagođena instalacija

Prilagođenu instalaciju treba da koriste isključivo iskusni korisnici koji imaju dobar razlog da **AVG Internet Security 2012** instaliraju sa nestandardnim postavkama, npr. u skladu sa specijalnim zahtevima sistema.

Ako se odlučite za ovu opciju, u dijalogu će se pojaviti novi odeljak pod imenom **Odredišna fascikla**. Ovde treba da navedete lokaciju na kojoj će se **AVG Internet Security 2012** instalirati. Podrazumevano, **AVG Internet Security 2012** će se instalirati u fascikli sa programskim datotekama koja se nalazi na disk jedinici C:, kao što je navedeno u tekstualnom polju u dijalogu. Ako želite da promenite ovu lokaciju, kliknite na dugme **Potraži** da biste videli strukturu disk jedinice i izaberite odgovarajuću fasciklu. Da biste se vratili na podrazumevano odredište unapred podešeno od strane prodavca programa, koristite dugme **Podrazumevano**.

Zatim kliknite na dugme **Dalje** da biste nastavili ka dijalogu [Prilagođene opcije](#).

Kontrolna dugmad

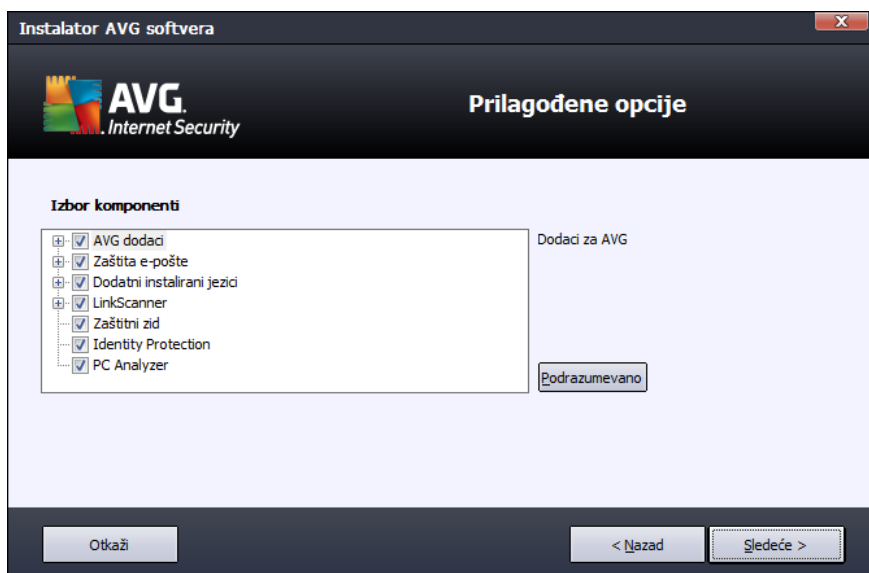
Kao i u većini dijaloga za instalaciju, dostupna su tri kontrolna dugmeta:

- **Otkazi** - kliknite da biste odmah napustili proces instalacije; **AVG Internet Security 2012** neće biti instaliran!
- **Nazad** - kliknite da biste se vratili za jedan korak unazad na prethodni dijalog za instalaciju.
- **Dalje** - kliknite da biste nastavili sa instalacijom i prešli na sledeći korak.



3.5. Prilagođene opcije

Dijalog **Prilagođene opcije** omogućava vam da podesite dva parametra instalacije:



Odeljak **Izbor komponenti** omogućava pregled svih **AVG Internet Security 2012** komponenti koje mogu biti instalirane. Ako vam podrazumevane postavke ne odgovaraju, možete ukloniti/dodati određene komponente.

Međutim, možete izabrati samo neku od komponenata koje se nalaze u izdanju programa AVG koje ste kupili!

Markirajte bilo koju stavku na listi **Izbor komponenti**, i kratak opis odgovarajuće komponente će se prikazati na desnoj strani ovog odeljka. Za detaljne informacije o funkcionalnosti svake komponente pročitajte poglavlje [Pregled komponenti](#) iz ove dokumentacije. Da biste se vratili na podrazumevanu konfiguraciju, unapred podešenu od strane proizvođača programa, koristite dugme **Podrazumevano**.

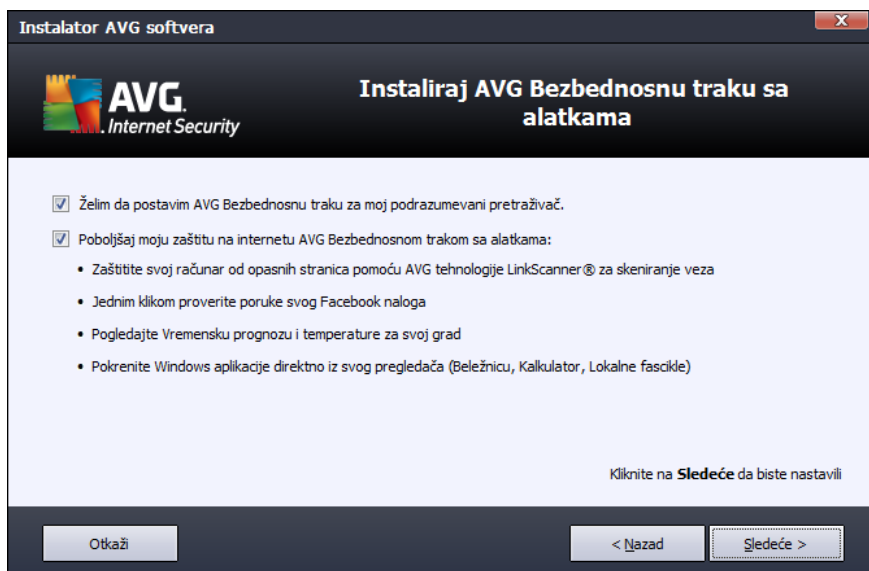
Kontrolna dugmad

Kao i u većini dijaloga za instalaciju, dostupna su tri kontrolna dugmeta:

- **Otkazi** - kliknite da biste odmah napustili proces instalacije; **AVG Internet Security 2012** neće biti instaliran!
- **Nazad** - kliknite da biste se vratili za jedan korak unazad na prethodni dijalog za instalaciju.
- **Dalje** - kliknite da biste nastavili sa instalacijom i prešli na sledeći korak.



3.6. Instalirajte AVG bezbednosnu traku sa alatkama



U dijalogu **Instaliraj AVG bezbednosnu traku sa alatkama** možete izabrati da li želite da instalirate [AVG bezbednosnu traku sa alatkama](#). Ako ne promenite podrazumevana podešavanja, ova komponenta će biti automatski instalirana u vaš Internet pregledač (*trenutno su podržani sledeći pregledači: Microsoft Internet Explorer v. 6.0 ili novije verzije i Mozilla Firefox v. 3.0 i novije verzije*) kako bi se omogućila sveobuhvatna zaštita dok pregledate Internet.

Takođe možete da odlučite da li želite da izaberete *AVG Secure Search (powered by Google)* kao podrazumevani pretraživač. Ukoliko želite, označite odgovarajuće polje.

Kontrolna dugmad

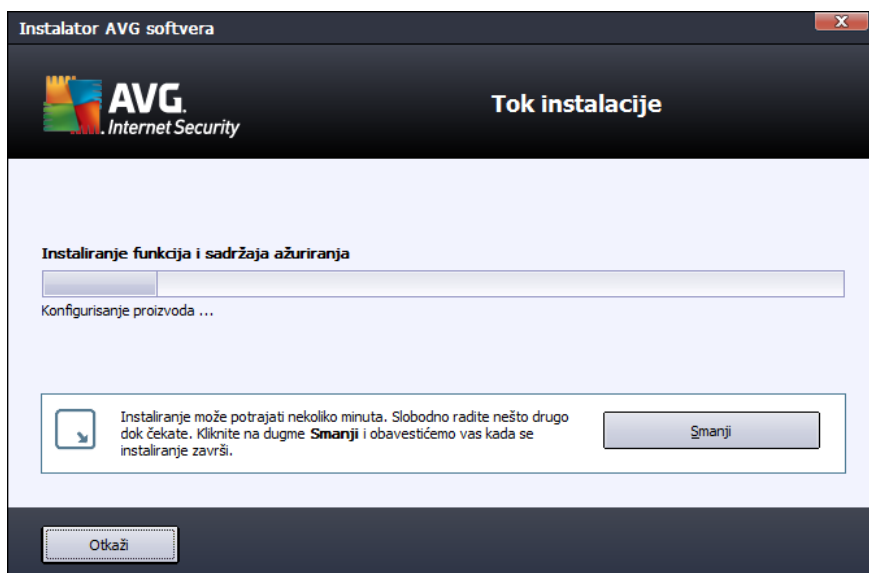
Kao i u većini dijaloga za instalaciju, dostupna su tri kontrolna dugmeta:

- **Otkazi** - kliknite da biste odmah napustili proces instalacije; **AVG Internet Security 2012** neće biti instaliran!
- **Nazad** - kliknite da biste se vratili za jedan korak unazad na prethodni dijalog za instalaciju.
- **Dalje** - kliknite da biste nastavili sa instalacijom i prešli na sledeći korak.



3.7. Tok instalacije

Dijalog **Tok instalacije** prikazuje tok instalacionog procesa i ne zahteva angažovanje korisnika:



Kada se proces instalacije završi, automatski ćete biti preusmereni na sledeći dijalog.

Kontrolna dugmad

U ovom dijalogu je dostupno samo jedno kontrolno dugme - **Otkazi**. Ovo dugme treba koristiti samo ako želite da zaustavite pokrenuti proces instalacije. Imajte u vidu da u tom slučaju **AVG Internet Security 2012** neće biti instaliran!



3.8. Instalacija je uspešno obavljena

Dijalog Instalacija je uspešno obavljena potvrđuje da je vaš **AVG Internet Security 2012** u potpunosti instaliran i konfigurisan:



Program za unapređenje proizvoda

Ovde možete odlučiti da li želite da učestvujete u programu za poboljšanje proizvoda (*detalje potražite u poglavlju [AVG napredna podešavanja / program za poboljšanje proizvoda](#)*) koji prikuplja anonimne informacije o otkrivenim pretnjama da bi se povećao ukupni nivo Internet bezbednosti. Ako pristajete na ovu izjavu, ostavite izabranu opciju **Pristajem da učestvujem u AVG 2012 programu za Web bezbednost i poboljšanje proizvoda ...** (opcija je podrazumevano izabrana).

Ponovno pokretanje računara

Da biste završili proces instalacije morate da restartujete vaš računar: odaberite da li želite da **Restartujete sada**, ili želite da odložite ovu radnju - **Restartuj kasnije**.



4. Nakon instalacije

4.1. Registracija proizvoda

Kada završite sa instalacijom programa **AVG Internet Security 2012**, registrujte proizvod na mreži na AVG Web lokaciji (<http://www.avg.com/>). Nakon registracije, imaćete pun pristup AVG korisničkom nalogu, AVG informativnom biltenu i drugim uslugama koje su dostupne isključivo registrovanim korisnicima.

Najlakši način da ga registrujete jeste direktno iz **AVG Internet Security 2012** korisničkog interfejsa. U glavnom meniju izaberite stavku [Pomoć/Registruj odmah](#). Bićete preusmereni na stranicu **Registracija** na AVG Web lokaciji (<http://www.avg.com/>). Pratite uputstva na toj stranici.

4.2. Pristup korisničkom interfejsu

[Glavnom dijalogu AV](#) možete pristupiti na nekoliko načina:

- dvaput kliknite na [AVG ikonu u sistemskoj traci](#)
- dvaput kliknite na AVG ikonu na radnoj površini
- iz menija **Start / Svi programi / AVG 2012**

4.3. Skeniranje celog računara

Postoji potencijalni rizik da je vaš računar zaražen virusom pre instalacije programa **AVG Internet Security 2012**. Zato je potrebno da pokrenete [Skeniranje celog računara](#), kako biste bili sigurni da računar nije zaražen. Prvo skeniranje može potrajati dugo (*oko sat vremena*), ali preporučuje se da njegovo pokretanje da biste se uverili da neka pretnja nije ugrozila računar. Uputstva za [Skeniranje celog računara](#) potražite u poglavlju [Skeniranje programom AVG](#).

4.4. Eicar test

Da biste potvrdili da je **AVG Internet Security 2012** pravilno instaliran, možete obaviti EICAR test.

EICAR test je standardan i potpuno bezbedan metod koji se koristi za testiranje funkcionisanja antivirusnog sistema. Bezbedno ga je širiti zato što nije pravi virus i ne sadrži nijedan deo virusnog koda. Većina proizvoda reaguje na njega kao na virus (*iako najčešće izveštavaju o njemu sa očiglednim imenom, kao što je „EICAR-AV-Test“*). Virus EICAR možete da preuzmete sa EICAR Web lokacije na adresi www.eicar.com gde takođe možete pronaći sve neophodne informacije o EICAR testu.

Pokušajte da preuzmete datoteku **eicar.com** i sačuvajte je na lokalnom disku. Odmah kada potvrdite preuzimanje probne datoteke, [Online Shield](#) (deo komponente [Link Scanner](#)) će na njega reagovati upozorenjem. Ovo obaveštenje pokazuje da je AVG ispravno instaliran na računaru.



Na Web lokaciji <http://www.eicar.com> takođe možete da preuzmete komprimovanu verziju EICAR „virusa“ (npr. u obliku *eicar_com.zip*). [Online Shield](#) vam omogućava da preuzmete ovu datoteku i da je sačuvate na lokalnom disku, ali će u tom slučaju [Stalni štit](#) (u okviru [antivirusne](#) komponente) otkriti „virus“ kada pokušate da je otpakujete.

Ako AVG ne identifikuje probnu datoteku EICAR kao virus, trebalo bi da ponovo proverite konfiguraciju programa!

4.5. Podrazumevana AVG konfiguracija

Podrazumevanu konfiguraciju (tj. način na koji je aplikacija podešena odmah nakon instalacije) programa **AVG Internet Security 2012** podesio je proizvođač softvera kako bi sve komponente i funkcije bile podešene tako da se postignu optimalne performanse.

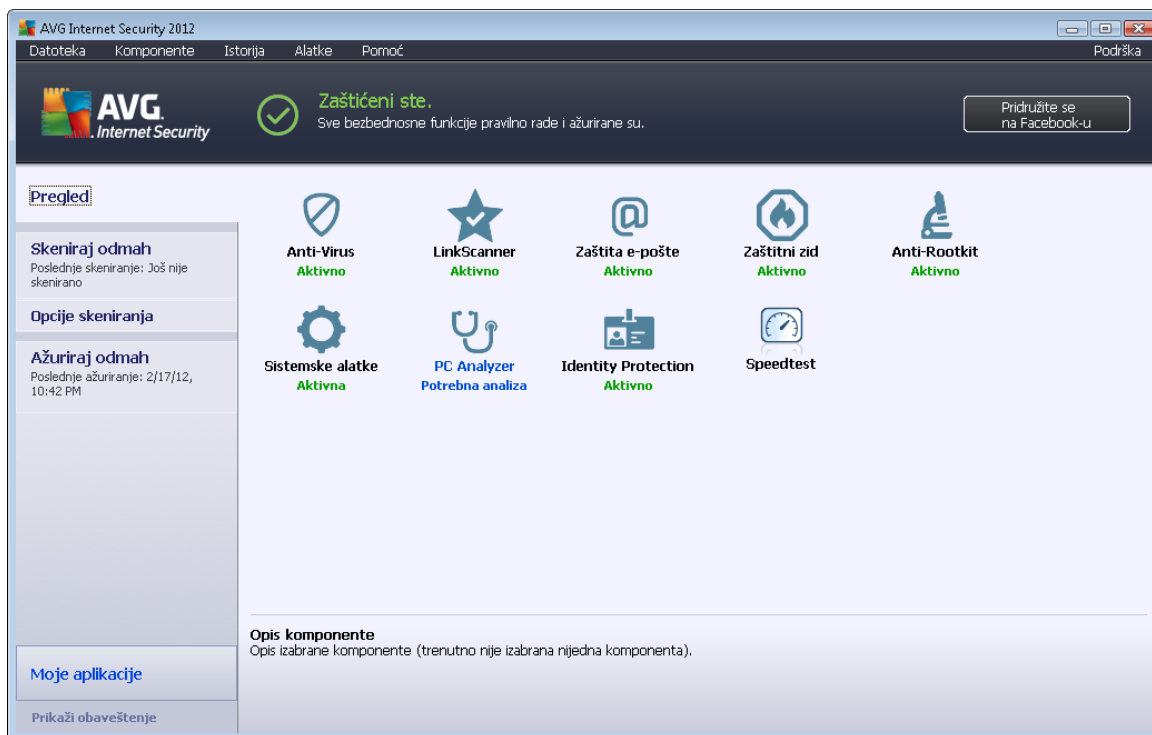
Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to! Podešavanja bi trebalo da menjaju samo iskusni korisnici.

Manje izmene [AVG komponenti](#) mogu se obavljati direktno iz korisničkog interfejsa te komponente. Ako bude potrebno da prilagodite konfiguraciju programa AVG svojim potrebama, idite na [AVG napredna podešavanja](#): izaberite stavku iz sistemskog menija **Alatke/Napredna podešavanja** i uredite konfiguraciju programa AVG u dijalogu [AVG napredna podešavanja](#) koji će se otvoriti.



5. AVG korisnički interfejs

AVG Internet Security 2012 se otvara sa glavnim prozorom:



Glavni prozor je podeljen na nekoliko odeljaka:

- **Sistemska meni** (gornja sistemska linija u prozoru) je standardna navigacija koja vam omogućava da pristupite svim komponentama, uslugama i funkcijama programa **AVG Internet Security 2012** - [detalji>>](#)
- **Informacije o bezbednosnom statusu** (gornji deo prozora) sadrži informacije o trenutnom statusu programa **AVG Internet Security 2012** - [detalji>>](#)
- **Dugme Pridružite nam se na lokaciji Facebook** (gornji desni odeljak prozora) omogućava vam da se pridružite [AVG zajednici na lokaciji Facebook](#). Međutim, dugme se pojavljuje samo u slučaju kada su sve komponente potpuno funkcionalne i rade ispravno (detalje o tome kako da prepoznate status AVG komponenti potražite u poglavlju [Informacije o bezbednosnom statusu](#))
- **Brze veze** (leva strana prozora) omogućavaju vam da brzo pristupite najvažnijim zadacima i onima koji se najčešće koriste u programu **AVG Internet Security 2012** - [detalji>>](#)
- **Moje aplikacije** (donji levi deo prozora) otvaraju pregled dodatnih aplikacija dostupnih za **AVG Internet Security 2012**: [LiveKive](#), [Family Safety](#) i [PC Tuneup](#)
- **Pregled komponenti** (središnji deo prozora) sadrži pregled svih komponenti instaliranih u programu **AVG Internet Security 2012** - [detalji>>](#)



- **Ikona sistemske palete** (donji desni ugao monitora, na sistemskoj paleti) označava trenutni status programa - **AVG Internet Security 2012** - [detalji>>](#)
- **AVG gadžet** (Windows bočna traka, podržano u OS Windows Vista/7) omogućava brzi pristup skeniranju i ažuriranju programa **AVG Internet Security 2012** - [detalji>>](#)

5.1. Sistemski meni

Sistemski meni je standardni oblik navigacije koji se koristi u svim Windows aplikacijama. Postavljen je horizontalno, na samom vrhu glavnog prozora programa **AVG Internet Security 2012**. Pomoću sistemskog menija možete pristupiti određenim AVG komponentama, funkcijama i uslugama.

Sistemski meni ima pet glavnih odeljaka:

5.1.1. Datoteka

- **Izadi** - zatvaranje **AVG Internet Security 2012** korisničkog interfejsa. Međutim, aplikacija AVG će i dalje raditi u pozadini, pa će vaš računar biti zaštićen!

5.1.2. Komponente

Stavka [Komponente](#) u sistemskom meniju sadrži veze ka svim instaliranim AVG komponentama koje služe za otvaranje podrazumevanih dijaloga u korisničkom interfejsu:

- **Pregled sistema** - pređite na podrazumevani dijalog korisničkog interfejsa sa [pregledom svih instaliranih komponenti i njihovim statusom](#)
- **Antivirusni program** otkriva viruse, špijunski softver, crve, trojanske konje, neželjene izvršne datoteke ili biblioteke u sistemu i štiti vas od zlonamernog advera - [detalji >>](#)
- **LinkScanner** vas štiti od napada zasnovanih na Webu dok pretražujete ili pregledate Internet - [detalji >>](#)
- **Zaštita e-pošte** proverava dolazne e-poruke u potrazi za bezvrednim porukama i blokira viruse, phishing napade ili druge pretnje - [detalji >>](#)
- **Zaštitni zid** kontroliše svu komunikaciju na svakom mrežnom portu, štiteći vas od zlonamernih napada i blokirajući sve pokušaje upada - [detalji >>](#)
- **Anti-Rootkit** skenira opasne rootkit programe skrivene u aplikacijama, upravljačkim programima ili bibliotekama - [detalji >>](#)
- **Sistemski alati** nudi detaljan pregled AVG okruženja i informacije o operativnom sistemu - [detalji >>](#)
- **PC Analyzer** analizator pruža informacije o statusu vašeg računara - [detalji >>](#)
- **Identity Protection** neprekidno štiti vaše digitalne resurse od novih i nepoznatih pretnji - [detalji >>](#)
- **Daljinska administracija** prikazuje se samo u okviru verzija iz serije AVG Business



Edition, u slučaju da ste tokom [procesa instalacije](#) označili da želite da instalirate ovu komponentu

5.1.3. Istorija

- [Rezultati skeniranja](#) - prelazak u AVG interfejs za testiranje, tj. u dijalog [Pregled rezultata skeniranja](#)
- [Detekcija od strane stalnog štita](#) – otvara se dijalog sa pregledom pretnji koje je detektovala komponenta [Stalni štit](#)
- [Otkrivanje skenera e-pošte](#) - otvara dijalog sa priložima e-poruka koje je komponenta [Zaštite e-pošte](#) otkrila kao opasne
- [Online Shield pronalazačenja](#) - otvara dijalog sa pregledom pretnji koje je usluga [Online Shield](#) otkrila u komponenti [LinkScanner](#)
- [Skladište za viruse](#) - otvaranje interfejsa karantina ([Skladište za viruse](#)) u koji AVG premešta sve detektovane slučajeve zaraze koji se iz nekog razloga ne mogu automatski izlečiti. Zaražene datoteke su izolovane u karantinu, pa je bezbednost vašeg računara zagarantovana; istovremeno, zaražene datoteke se čuvaju radi potencijalnog oporavka u budućnosti
- [Evidencija istorije događaja](#) - otvaranje interfejsa evidencije istorije sa pregledom svih evidentiranih **AVG Internet Security 2012** radnji
- [Evidencija zaštitnog zida](#) - otvara interfejs za podešavanje zaštitnog zida na kartici [Datoteke evidencije](#) sa detaljnim pregledom svih radnji komponente Zaštitni zid.

5.1.4. Alatke

- [Skeniraj računar](#) - pokreće skeniranje celog računara.
- [Skeniraj izabranu fasciklu...](#) - prebacuje se na [AVG interfejs za skeniranje](#) i dozvoljava vam da u strukturi stabla računara definišete koje datoteke i fascikle treba da se skeniraju.
- [Skeniraj datoteku...](#) - omogućava vam da pokrenete testiranje jedne određene datoteke na zahtev. Izaberite ovu opciju da biste otvorili novi prozor sa strukturom stabla vašeg diska. Izaberite željenu datoteku i potvrdite pokretanje skeniranja.
- [Ažuriraj](#) – automatsko pokretanje procesa ažuriranja za **AVG Internet Security 2012**.
- [Ažuriraj iz direktorijuma...](#) - pokreće proces ažuriranja iz datoteka za ažuriranje koje se nalaze u navedenoj fascikli na lokalnom disku. Međutim, korišćenje ove opcije preporučuje se isključivo u hitnim slučajevima, npr. ako nije dostupna veza sa Internetom (*na primer, vaš računar je zaražen i nije povezan sa Internetom; vaš računar je povezan na mrežu koja nema pristup Internetu, itd.*). U prozoru koji će se otvoriti, izaberite fasciklu u koju ste prethodno smestili datoteku za ažuriranje, pa pokrenite proces ažuriranja.
- [Napredna podešavanja...](#) - otvara dijalog [AVG napredna podešavanja](#) u kojem možete urediti AVG Internet Security 2012 konfiguraciju. Uglavnom se preporučuje da zadržite podrazumevana podešavanja ove aplikacije koje je definisao proizvođač softvera.



- [Podešavanja zaštitnog zida...](#) - otvara samostalni dijalog za naprednu konfiguraciju komponente [zaštitnog zida](#).

5.1.5. Pomoć

- **Sadržaj** - otvaranje AVG datoteka pomoći
- **Pronalaženje podrške** - otvara AVG Web lokaciju (<http://www.avg.com/>) na stranici centra za korisničku podršku
- **Vaš AVG Web** - otvara AVG Web lokaciju (<http://www.avg.com/>)
- **Više informacija o virusima i pretnjama** - otvaranje [Enciklopedije virusa](#) na mreži u kojoj možete pronaći detaljne informacije o identifikovanom virusu
- **Ponovo aktiviraj** – otvaranje dijaloga **Aktivacija AVG programa** sa podacima koje ste uneli u dijalogu [Prilagođavanje programa AVG](#) u toku [procesa instalacije](#). U ovom dijalogu možete uneti svoj broj licence kako biste zamenili prodajni broj (*broj sa kojim ste instalirali AVG*) ili zamenili stari broj licence (*npr. prilikom nadogradnje na nov AVG proizvod*).
- **Registruj odmah** - vrši povezivanje sa stranicom za registraciju na AVG Web lokaciji (<http://www.avg.com/>). Popunite svoje podatke o registraciji; samo klijenti koji registruju svoj AVG proizvod mogu primati besplatnu tehničku podršku.

Napomena: ako koristite probnu verziju programa **AVG Internet Security 2012**, poslednje dve stavke se pojavljuju kao **Kupi odmah i Aktiviraj**, što vam omogućava da odmah kupite punu verziju programa. Ako je **AVG Internet Security 2012** instaliran sa prodajnim brojem, prikazuju se stavke **Registracija i Aktivacija**.

- **O programu AVG** - otvara dijalog **Informacije** koji sadrži šest kartica sa podacima o imenu programa, verziji programa i baze podataka o virusima, sistemskim informacijama, ugovorom o licenciranju i kontakt podacima kompanije **AVG Technologies CZ**.

5.1.6. Podrška

Veza **Podrška** otvara novi dijalog **Informacije** sa svim tipovima informacija koji će vam možda biti potrebni prilikom pokušaja pronalaženja pomoći. Dijalog uključuje osnovne podatke o instaliranom AVG programu (*verziju programa/baze podataka*), detalje o licenci i listu brzih veza za podršku.

Dijalog **Informacije** podeljen je u šest kartica:



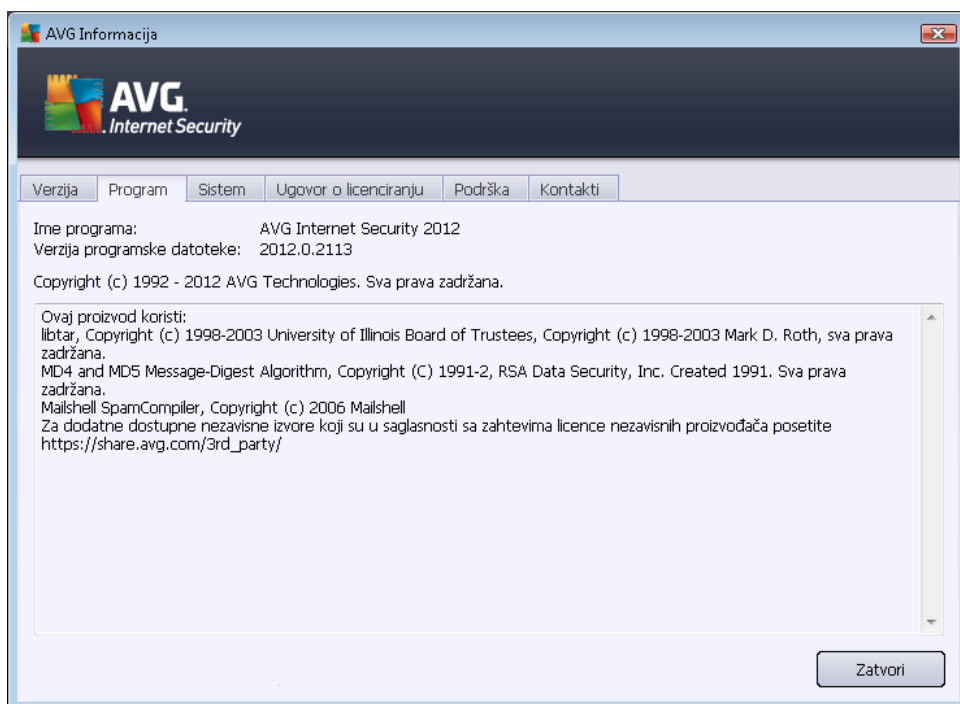
Kartica **Verzija** je podeljena u tri odeljka:



- **Informacije o podršci** - obezbeđuje informacije o **AVG Internet Security 2012** verziji, verziji baze podataka o virusima, verziji baze podataka [odbrane od bezvredne pošte](#) i [LinkScanner](#) verziji.
- **Informacije o korisniku** - obezbeđuje informacije o licenciranom korisniku i preduzeću.
- **Detalji o licenci** - obezbeđuje informacije o licenci (*ime proizvoda, tip licence, broj licence, datum isteka i broj računara*). U ovom odeljku takođe možete koristiti vezu **Registracija** da biste registrovali **AVG Internet Security 2012** na mreži; ovo vam dozvoljava da u potpunosti koristite [AVG tehničku podršku](#). Isto tako, koristite vezu **Ponovna aktivacija** da biste otvorili dijalog **Aktivacija AVG proizvoda**: unesite broj licence u odgovarajuće polje da biste zamenili prodajni broj (*koji koristite tokom AVG Internet Security 2012 instalacije*) ili da biste zamenili trenutni broj licence nekim drugim (*npr. prilikom nadogradnje na noviji AVG proizvod*).

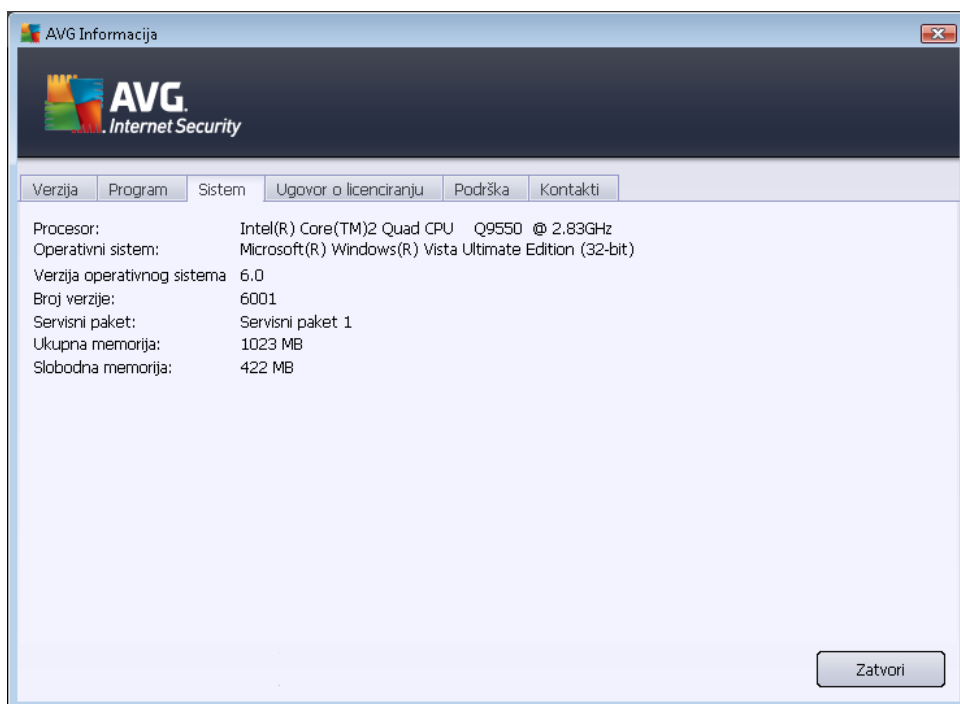


Na kartici **Program** možete pronaći informacije o **AVG Internet Security 2012** verziji programske datoteke i o kodu trećih strana u proizvodu:



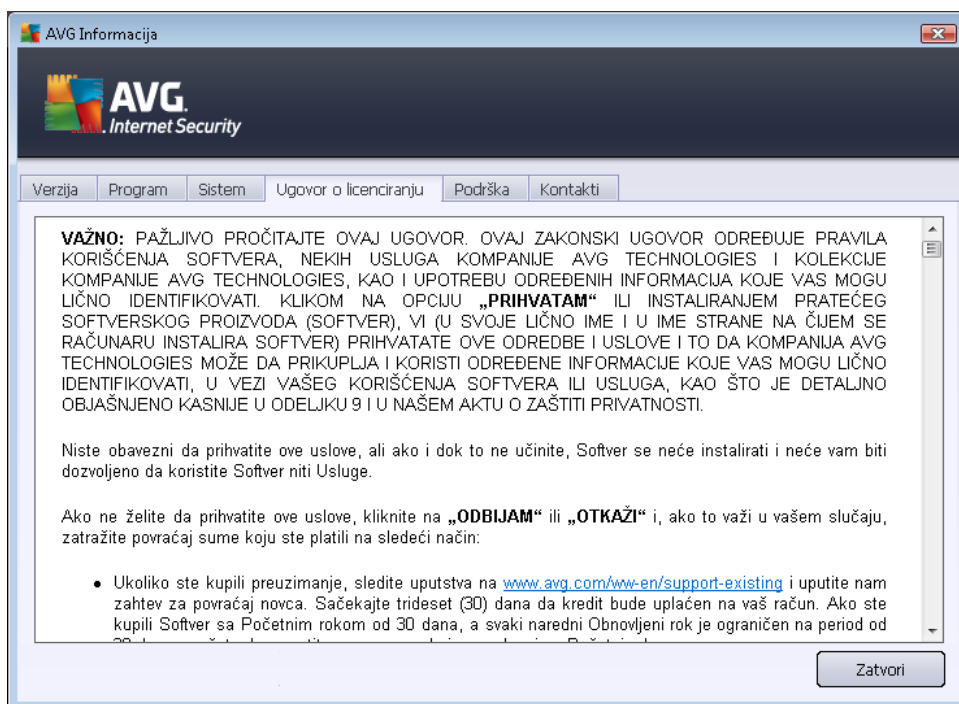


Kartica **Sistem** nudi listu parametara operativnog sistema (*tip procesora, operativni sistem i verzija, broj verzije, korišćeni servisni paketi, ukupna veličina memorije i veličina slobodne memorije*):





Na kartici **Ugovor o licenciranju** možete pročitati kompletan tekst ugovora o licenciranju između vas i preduzeća AVG Technologies:



Kartica **Podrška** prikazuje listu svih mogućnosti kontaktiranja korisničke podrške. Ona takođe obezbeđuje veze ka AVG Web lokaciji (<http://www.avg.com/>), AVG forumima, najčešćim pitanjima... Pored toga, možete pronaći informacije koje možete koristiti prilikom kontaktiranja tima korisničke podrške:



Kartica **Kontakti** obezbeđuje listu svih kontakata preduzeća AVG Technologies, kao i kontakata AVG lokalnih predstavnika i prodavaca:



5.2. Informacije o bezbednosnom statusu

Odeljak **Informacije o bezbednosnom statusu** se nalazi u gornjem delu glavnog prozora programa **AVG Internet Security 2012**. U ovom odeljku uvek možete pronaći informacije o trenutnom bezbednosnom statusu programa **AVG Internet Security 2012**. Pogledajte opise ikona iz ovog odeljka i njihovo značenje:



- Zelena ikona ukazuje na to da je **AVG Internet Security 2012 u potpunosti funkcionalan**. Računar je u potpunosti zaštićen i ažuriran, i sve instalirane komponente ispravno rade.



- Žuta ikona upozorava na to da su **neke komponente nepravilno konfigurisane** i da bi trebalo da obratite pažnju na njihova svojstva/podešavanja. Nema kritičnih problema u programu **AVG Internet Security 2012**, ali ste verovatno odlučili da isključite neku komponentu. I dalje ste zaštićeni! Međutim, obratite pažnju na podešavanja problematične komponente! Njeno ime će biti prikazano u odeljku **Informacije o bezbednosnom statusu**.

Žuta ikona se takođe pojavljuje ako iz nekog razloga odlučite da zanemarite status greške komponente. Opcija **Zanemari status komponente** dostupna je iz kontekstualnog menija (koji se otvara klikom desnim tasterom miša) iznad ikone odgovarajuće komponente u [pregledu komponenti](#) glavnog prozora programa **AVG Internet Security 2012**. Izaberite ovu opciju da biste naveli da ste svesni statusa greške komponente, ali iz nekog razloga želite da zadržite **AVG Internet Security 2012** na taj način i ne želite da vas [ikona na sistemskoj paleti](#) upozorava. Možda treba da koristite ovu opciju u određenoj situaciji, ali se preporučuje da isključite opciju **Zanemari status komponente** što je pre moguće.

Isto tako, žuta ikona će se prikazati i ako **AVG Internet Security 2012** zahteva ponovno pokretanje računara (**Potrebno je ponovno pokretanje**). Obratite pažnju na ovo upozorenje i ponovo pokrenite računar pomoću dugmeta **Ponovo pokreni odmah**.



- Žuta ikona ukazuje na to da je **AVG Internet Security 2012 u kritičnom stanju!** Jedna ili više komponenti ne radi ispravno, pa **AVG Internet Security 2012** ne može da zaštititi vaš računar. Odmah pokušajte da rešite prijavljeni problem. Ako ne možete sami da rešite problem, obratite se [AVG timu za tehničku podršku](#).

U slučaju da AVG Internet Security 2012 nije postavljen na optimalnu performansu, pojaviće se novo dugme pod imenom „Popravi“ (odnosno „Popravi sve“ ako problem uključuje više komponenti) pored informacija o bezbednosnom statusu. Pritisnite dugme da pokrenete automatski proces provere i konfiguracije programa. Ovo je jednostavan način da postavite AVG Internet Security 2012 na optimalnu performansu i dostignete maksimalni nivo bezbednosti!

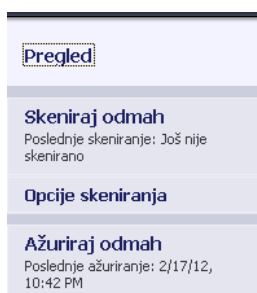
Preporučuje se da obratite pažnju na Informacije o bezbednosnom statusu, a u slučaju da izveštaj ukazuje na neki problem, odmah pokušajte da ga rešite. U suprotnom vaš računar će biti izložen riziku!



Napomena: informacije o statusu programa AVG Internet Security 2012 takođe možete dobiti u bilo kojem trenutku preko [ikone sistemske palete](#).

5.3. Brze veze

Brze veze se nalaze sa leve strane **AVG Internet Security 2012** [korisničkog interfejsa](#). Ove veze vam dozvoljavaju da odmah pristupite najvažnijim i najčešće korišćenim funkcijama aplikacije, tj. skeniranju i ažuriranju. Brze veze su dostupne iz svih dijaloga korisničkog interfejsa:



Brze veze su grafički podeljene u tri odeljka:

- **Skeniraj odmah** - ovo dugme podrazumevano pruža informacije o poslednjem pokrenutom skeniranju (tj. *tip skeniranja i datum poslednjeg pokretanja*). Kliknite na komandu **Skeniraj odmah** da biste ponovo pokrenuli isto skeniranje. Ako želite da pokrenete drugo skeniranje, kliknite na vezu **Opcije skeniranja**. Na ovaj način ćete otvoriti [AVG interfejs za skeniranje](#) odakle možete pokrenuti skeniranja, planirati skeniranja ili uređivati njihove parametre. (Detalje potražite u poglavlju [AVG skeniranje](#))
- **Opcije skeniranja** - koristite ovu vezu da biste iz bilo kog trenutno otvorenog AVG dijaloga prešli u podrazumevani prozor sa [pregledom svih instaliranih komponenti](#). (Detalje potražite u poglavlju [Pregled komponenti](#))
- **Ažuriraj odmah** - ova veza obezbeđuje datum i vreme poslednjeg pokretanja [ažuriranja](#). Kliknite na ovo dugme da biste odmah pokrenuli proces ažuriranja i da biste pratili njegov tok. (Detalje potražite u poglavlju [AVG ažuriranja](#))

Brze veze su u svakom trenutku dostupne iz [AVG korisničkog interfejsa](#). Kada upotrebite brzu vezu za pokretanje određenog procesa, skeniranja ili ažuriranja, aplikacija će se prebaciti na novi dijalog, ali brze veze će i dalje biti dostupne. Pored toga, pokrenuti proces se dodatno grafički prikazuje u navigaciji kako biste imali punu kontrolu nad svim trenutno pokrenutim procesima u programu **AVG Internet Security 2012**.

5.4. Pregled komponenti

Odeljci „Pregled komponenti“

Odeljak **Pregled komponenti** se nalazi u centralnom delu vašeg **AVG Internet Security 2012** [korisničkog interfejsa](#). Ovaj odeljak ima dva dela:



- **Pregled svih instaliranih komponenti** koji se sastoji od grafičkih tabli za sve instalirane komponente. Svaka tabla je označena ikonom komponente i pruža informacije o tome da li je odgovarajuća komponenta trenutno aktivna ili neaktivna.
- **Opis komponente** se nalazi u donjem delu ovog dijaloga. Opis ukratko objašnjava osnovnu funkcionalnost komponente. On takođe pruža informacije o trenutnom statusu izabrane komponente.

Lista instaliranih komponenti

U okviru programa **AVG Internet Security 2012**, odeljak **Pregled komponenti** sadrži informacije o sledećim komponentama:

- **Antivirusni program** otkriva viruse, špijunski softver, crve, trojanske konje, neželjene izvršne datoteke ili biblioteke u sistemu i štiti vas od zlonamernog advera - [detalji >>](#)
- **LinkScanner** vas štiti od napada zasnovanih na Webu dok pretražujete ili pregledate Internet - [detalji >>](#)
- **Zaštita e-pošte** proverava dolazne e-poruke u potrazi za bezvrednom poštom i blokira viruse, phishing napade ili druge pretnje - [detalji >>](#)
- **Zaštitni zid** kontroliše svu komunikaciju na svakom mrežnom portu, štiteći vas od zlonamernih napada i blokirajući sve pokušaje upada - [detalji >>](#)
- **Anti-Rootkit** skenira opasne rootkit programe skrivene u aplikacijama, upravljačkim programima ili bibliotekama - [detalji >>](#)
- **Sistemski alati** nudi detaljan pregled AVG okruženja i informacije o operativnom sistemu - [detalji >>](#)
- **PC Analyzer** analizator pruža informacije o statusu vašeg računara - [detalji >>](#)
- **Identity Protection** neprekidno štiti vaše digitalne resurse od novih i nepoznatih pretnji - [detalji >>](#)
- **Daljinska administracija** prikazuje se samo u okviru verzija iz serije AVG Business Edition, u slučaju da ste tokom [procesa instalacije](#) označili da želite da instalirate ovu komponentu

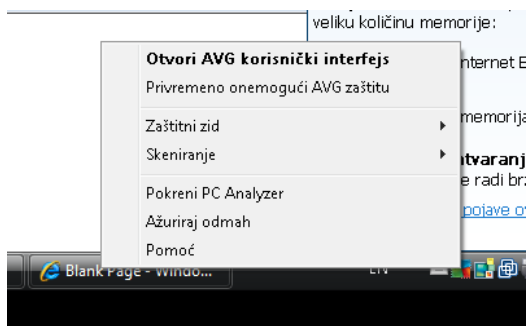
Dostupne radnje

- **Postavite miš iznad ikone bilo koje komponente** da biste je označili u pregledu komponenti. Istovremeno se pojavljuje opis osnovne funkcionalnosti komponente u donjem delu [korisničkog interfejsa](#).
- **Kliknite na ikonu komponente** da biste otvorili njen interfejs sa listom osnovnih statističkih podataka.

- **Kliknite desnim tasterom miša na ikonu komponente** da biste razvili kontekstualni meni sa nekoliko opcija:
 - **Otvori** - izaberite ovu opciju da biste otvorili dijalog komponente (*kao što radite klikom na ikonu komponente*).
 - **Zanemari status ove komponente** - izaberite ovu opciju da biste stavili do znanja da ste svesni [stanja greške komponente](#), ali iz nekog razloga želite da zadržite ovaj status i ne želite da dobijate upozorenja od [ikone u sistemskoj paleti](#).
 - **Otvori u naprednim podešavanjima...** - ova opcija je dostupna samo za neke komponente; tj. one koje pružaju mogućnost [naprednih podešavanja](#).

5.5. Ikona sistemske palete

AVG ikona sistemske palete (na traci zadataka operativnog sistema Windows, donji desni ugao monitora) ukazuje na trenutni status programa **AVG Internet Security 2012**. Vidljiva je u svakom trenutku na sistemskoj paleti, bez obzira na to da li je [korisnički interfejs](#) programa **AVG Internet Security 2012** otvoren ili zatvoren:



Prikaz AVG ikone sistemske palete

-  U punoj boji bez dodatnih elemenata, ikona ukazuje na to da su sve **AVG Internet Security 2012** komponente aktivne i u potpunosti funkcionalne. Međutim, ikona se može prikazati na ovaj način i u situaciji kada neka komponenta nije u potpunosti funkcionalna, ali korisnik je odlučio da [zanemari status komponente](#). (*Ako potvrdite opciju „Zanemari status komponente“, vi navodite da ste svesni [statusa greške komponente](#), ali iz nekog razloga želite da je ostavite tako i ne želite da primete obaveštenja o situaciji.*)
-  Ikona sa znakom uzvika ukazuje na to da je komponenta (*ili čak više komponenti*) u [stanju greške](#). Uvek obratite pažnju na takvo upozorenje i pokušajte da uklonite problem sa konfiguracijom komponente koja nije ispravno podešena. Da biste mogli da izvršite promene u konfiguraciji komponente, dvaput kliknite na ikonu sistemske palete da biste otvorili [korisnički interfejs aplikacije](#). Detaljne informacije o komponentama koje su u [stanju greške](#) potražite u odeljku [Informacije o bezbednosnom statusu](#).
-  Ikona sistemske palete se može dodatno prikazati u punoj boji sa treperavim i rotirajućim zrakom svetlosti. Ova grafička verzija signalizira trenutno pokrenuti proces

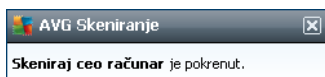


ažuriranja.

-  Alternativni prikaz ikone u punoj boji sa strelicom znači da je neko **AVG Internet Security 2012** skeniranje upravo pokrenuto.

Informacije o AVG ikoni sistemske palete

AVG ikona sistemske palete dodatno pruža informacije o trenutnim aktivnostima u programu **AVG Internet Security 2012**, kao i o mogućim promenama statusa u programu (*npr. automatsko pokretanje planiranog skeniranja ili ažuriranja, promena profila zaštitnog zida, promena statusa komponente, instanca statusa greške, ...*) putem iskačućeg prozora koji se otvara pomoću ikone na sistemskoj traci poslova:



Radnje dostupne putem AVG ikone sistemske palete

AVG ikona sistemske palete može se koristiti i kao brza veza za pristup [korisničkom interfejsu](#) programa **AVG Internet Security 2012**, jednostavno kliknite dvaput na ikonu. Klikom desnim tasterom miša na ikonu otvarate kratki kontekstualni meni sa sledećim opcijama:

- **Otvori AVG korisnički interfejs** - kliknite da biste otvorili [korisnički interfejs](#) programa **AVG Internet Security 2012**.
- **Privremeno onemogućiti AVG zaštitu** - ova opcija vam omogućava da isključite celu zaštitu koju vam obezbeđuje **AVG Internet Security 2012** odjednom. Imajte u vidu da ovu opciju ne treba da koristite, osim ako to nije apsolutno neophodno! U većini slučajeva, neće biti neophodno da onemogućite **AVG Internet Security 2012** pre instalacije novog softvera ili upravljačkih programa, čak i ako instalator ili čarobnjak softvera predlažu da isključite pokrenute programe i aplikacije da ne bi ometale proces instalacije. Ako se ukaže potreba da privremeno onemogućite program **AVG Internet Security 2012**, preporučujemo da ga što pre ponovo omogućite. Ukoliko ste povezani na Internet ili mrežu tokom vremena u kojem je vaš antivirusni softver onemogućen, vaš računar je podložan napadima.
- **Zaštitni zid** - kliknite da biste otvorili kontekstualni meni opcija podešavanja [zaštitnog zida](#), odakle možete urediti glavne parametre: [Status zaštitnog zida](#) (*Zaštitni zid omogućen/Zaštitni zid onemogućen/Hitni režim*), [prebacivanje režima za igre](#) i [Profili zaštitnog zida](#).
- **Skeniranja** - kliknite da biste otvorili kontekstualni meni [unapred definisanih skeniranja](#) ([Skeniranje celog računara](#) i [Skeniranje određenih datoteka ili fascikli](#)) i izaberite potrebno skeniranje, ono će se odmah pokrenuti.
- **Pokretanje skeniranja...** - ova stavka se prikazuje samo u slučaju kada je skeniranje trenutno pokrenuto na računaru. Za ovo skeniranje tada možete postaviti prioritet, odnosno zaustaviti ili pauzirati tekuće skeniranje. Dalje, sledeće radnje su dostupne: *Postavi prioritet za sva skeniranja, Pauziraj sva skeniranja ili Zaustavi sva skeniranja*.



- **Pokreni PC Analyzer** - kliknite da biste pokrenuli komponentu [PC Analyzer](#).
- **Ažuriraj odmah** - odmah pokreće [ažuriranje](#).
- **Pomoć** - otvara datoteku pomoći na početnoj stranici.

5.6. AVG Savetnik

AVG Savetnik je funkcija za performanse koja nadgleda sve pokrenute procese na računaru u potrazi za mogućim problemima i nudi savete o tome kako da se izbegne problem. **AVG Savetnik** je vidljiv u obliku klizećeg iskačućeg prozora iznad systemske palete.



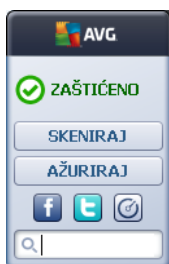
AVG Savetnik se može pojaviti u sledećim situacijama:

- Internet pregledaču koji koristite ponestaje memorije, što može usporiti vaš rad (**AVG Savetnik podržava samo Internet Explorer, Chrome, Firefox, Opera i Safari pregledače**);
- Proces pokrenut na računaru koristi preveliku količinu memorije i usporava performanse računara;
- Vaš računar će se automatski povezati sa nepoznatom WiFi mrežom.

U svakoj od ovih situacija, **AVG Savetnik** vas upozorava o mogućem problemu koji se može desiti i obezbeđuje ime i ikonu neusaglašenog procesa odnosno aplikacije. Isto tako, **AVG Savetnik** predlaže korake koje treba preduzeti da bi se izbegao mogući problem.

5.7. AVG gadžet

AVG gadžet se prikazuje na Windows radnoj površini (*Windows pomoćna traka*). Ova aplikacija je podržana samo kod operativnih sistema Windows Vista i Windows 7. **AVG gadžet** nudi trenutni pristup najvažnijim **AVG Internet Security 2012** funkcijama, npr. [skeniranju](#) i [ažuriranju](#):



Brzi pristup skeniranju i ažuriranju

Ukoliko je potrebno, **AVG gadžet** vam omogućava da odmah pokrenete skeniranje ili ažuriranje:

- **Skeniraj sada** - kliknite na vezu **Skeniraj sada** da direktno započnete [skeniranje celog računara](#). Možete posmatrati napredak procesa skeniranja u naizmeničnom korisničkom interfejsu gadžeta. Kratak pregled statističkih podataka pruža informacije o broju skeniranih objekata, otkrivenim pretnjama i saniranim pretnjama. Tokom skeniranja uvek možete pauzirati  ili zaustaviti  proces skeniranja. Za detaljne podatke u vezi sa rezultatima skeniranja, pogledajte standardni dijalog [Pregled rezultata skeniranja](#) koji se može otvoriti direktno iz gadžeta putem opcije **Prikaži detalje** (rezultati odgovarajućeg skeniranja biće navedeni u okviru stavke Skeniranje pomoću gadžeta iz bočne trake).



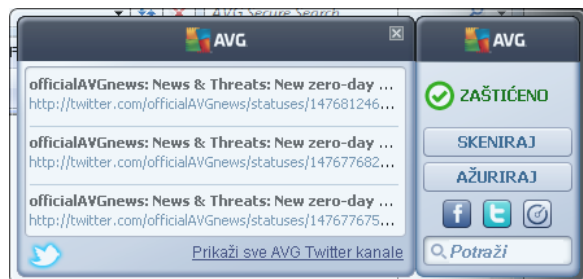
- **Ažuriraj odmah** - kliknite na vezu **Ažuriraj odmah AVG Internet Security 2012** da pokrenete ažuriranje programa direktno unutar gadžeta:



Pristup društvenim mrežama

AVG gadžet takođe obezbeđuje brzu vezu koja vas povezuje sa glavnim društvenim mrežama. Koristite odgovarajuće dugme da biste se povezali sa AVG zajednicama u uslugama Twitter, Facebook ili LinkedIn:

- **Twitter veza**  - otvara novi interfejs **AVG gadžet** koji pruža pregled poslednjih AVG napomena postavljenih na Twitter-u. Sledite vezu **Pogledaj sve AVG Twitter vesti** da otvorite vaš Web pregledač u novom prozoru, i bićete preusmereni direktno na Twitter Web lokaciju, posebno na stranicu posvećenu vestima vezanim za AVG:



- **Facebook veza**  - otvara vaš Web pregledač na Facebook Web lokaciji, posebno na stranici AVG zajednica
- **LinkedIn**  – ova opcija je dostupna samo u okviru mrežne instalacije (tj. pod uslovom da ste instalirali AVG, koristeći neku od licenci za AVG Business Edition, i otvara vaš Internet pregledač na Web lokaciji **AVG SMB zajednice** na društvenoj mreži LinkedIn.

Ostale funkcije dostupne putem gadžeta

- **PC Analyzer**  - otvara korisnički interfejs u komponenti [PC Analyzer](#) i odmah pokreće analizu.
- **Polje za pretragu** - unesite ključnu reč i odmah ćete dobiti rezultate pretrage u novom prozoru podrazumevanog Web pregledača.



6. Komponente programa AVG

6.1. Antivirusni program

Antivirusna komponenta predstavlja osnovu programa **AVG Internet Security 2012** i ona kombinuje nekoliko fundamentalnih funkcija bezbednosnog programa:

- [Mašina za skeniranje](#)
- [Stalna zaštita](#)
- [Zaštita od špijunskog softvera](#)

6.1.1. Mašina za skeniranje

Mašina za skeniranje, koja predstavlja osnovu komponente **Antivirusni program** skenira sve datoteke i aktivnosti datoteka (*otvaranje/zatvaranje datoteka itd.*) kako bi se proverilo da li sadrže poznate viruse. Svim otkrivenim virusima će biti blokirano izvršavanje radnji, a oni će zatim biti očišćeni ili stavljeni u karantin u [skladište za viruse](#).

Važna funkcija AVG Internet Security 2012 zaštite je to što nijedan poznati virus ne može da se pokrene na računaru!

Metodi otkrivanja

Većina antivirusnih softvera koristi i heurističko skeniranje, kod kojeg se u datotekama traže tipične karakteristike virusa, takozvani viralni potpisi. To znači da će antivirusni softver biti u stanju da detektuje nov, nepoznat virus ako taj virus ima neke od tipičnih karakteristika postojećih virusa.

Antivirusni program koristi sledeće metode otkrivanja:

- Skeniranje - traženje niski znakova koje su karakteristične za dati virus
- *Heuristička analiza* - dinamička emulacija uputstava skeniranog objekta u okruženju virtuelnog računara
- Generičko otkrivanje - otkrivanje uputstava karakterističnih za dati virus/grupu virusa

Pošto samo jedna tehnologija može biti nedovoljna za otkrivanje ili identifikaciju virusa, **Antivirusni program** kombinuje nekoliko tehnologija da bi obezbedio zaštitu računara. **AVG Internet Security 2012** takođe može da analizira i otkrije izvršne aplikacije ili DLL biblioteke koje su potencijalno neželjene u sistemu. Takve pretnje nazivamo „potencijalno neželjeni programi“ (*različiti tipovi špijunskog softvera, advera itd.*). Pored toga, **AVG Internet Security 2012** skenira registrator sistema u potrazi za sumnjivim unosima, privremenim Internet datotekama i kolačićima za praćenje i dozvoljava vam da sve potencijalno štetne stavke tretirate na isti način kao i svaku drugu zarazu.

AVG Internet Security 2012 obezbeđuje neprekidnu zaštitu za vaš računar!



6.1.2. Stalna zaštita

AVG Internet Security 2012 vam pruža neprekidnu zaštitu u obliku takozvane „stalne zaštite“. Komponenta **Antivirusni program** skenira svaku datoteku (sa određenim oznakama tipa datoteka ili bez ikakvih oznaka tipa datoteka) koja se otvara, čuva ili kopira. Ona štiti oblasti sistema računara i prenosive medijume (fleš disk itd.). U slučaju da se otkrije virus u datoteci kojoj se pristupa, ona zaustavlja operaciju koja se trenutno izvršava i ne dozvoljava virusu da se aktivira. Vi nećete čak ni primetiti taj proces zato što se stalna zaštita pokreće „u pozadini“. Bićete obavešteni samo kada se pronađu pretnje; **Antivirusni program** istovremeno blokira aktiviranje pretnje i uklanja je.

Stalna zaštita se učitava u memoriju računara tokom pokretanja sistema i veoma je važno da uvek bude uključena!

6.1.3. Zaštita od špijunskog softvera

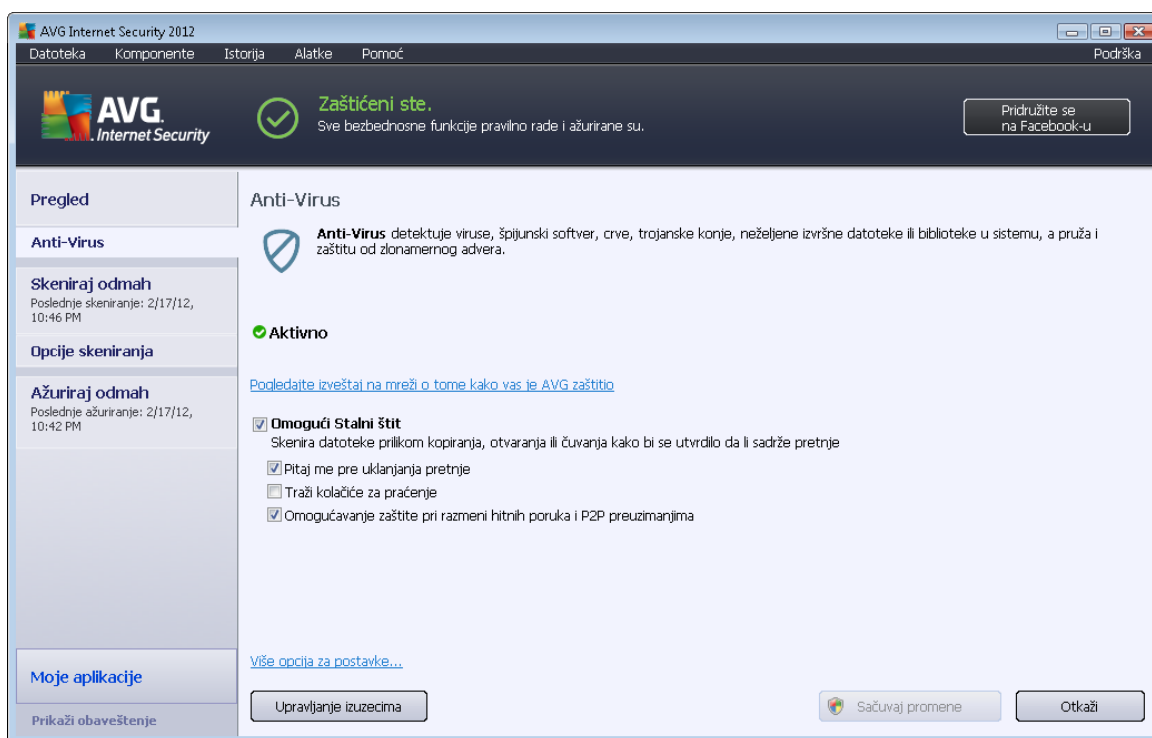
Odbrana od špijunskog softvera se sastoji od baze podataka o špijunskom softveru koja se koristi za identifikovanje poznatih tipova definicija špijunskog softvera. AVG stručnjaci za špijunski softver vredno rade na identifikaciji i opisivanju najnovijih oblika špijunskog softvera čim se pojave, a definicije se zatim dodaju u bazu podataka o špijunskom softveru. Pomoću procesa ažuriranja, nove definicije se preuzimaju na vaš računar kako biste uvek imali pouzdanu zaštitu, čak i od najnovijih tipova špijunskog softvera. **Odbrana od špijunskog softvera** vam dozvoljava da u potpunosti skenirate računar u potrazi za malverom/špijunskim softverom. Ona takođe otkriva i malver koji je u stanju spavanja i neaktivan je, tj. malver koji je preuzet, ali još nije aktiviran.

Šta je to špijunski softver?

Špijunski softver se obično definiše kao tip malvera, tj. softver koji prikuplja informacije sa računara korisnika bez njegovog znanja ili odobrenja. Neke špijunске aplikacije mogu biti namerno instalirane i često sadrže reklame, iskačuće prozore ili različite vrste neugodnog softvera. Trenutno, najčešći izvor zaraze su Web lokacije sa potencijalno opasnim sadržajem. Rasprostranjene su i druge metode prenosa, npr. putem e-pošte ili prenos crvima i virusima. Najvažnija zaštita jeste da koristite uvek uključeni skener u pozadini, kao što je **Antispajver** komponenta koja radi kao stalni štit i skenira aplikacije u pozadini dok ih pokrećete.

6.1.4. Interfejs antivirusnog programa

Interfejs **antivirusne** komponente pruža kratke informacije o funkcionalnosti komponente, informacije o trenutnom statusu komponente (*Aktivno*) i osnovne opcije konfiguracije komponente:



Opcije konfiguracije

Dijalog obezbeđuje neke osnovne opcije konfiguracije funkcija dostupnih u **antivirusnoj** komponenti. Njihov kratak opis sledi u nastavku:

- **Prikažite izveštaj na mreži o tome kako vas je AVG zaštitio** - veza vas preusmerava na određenu stranicu na AVG Web lokaciji (<http://www.avg.com/>). Na stranici možete pronaći detaljan statistički pregled svih **AVG Internet Security 2012** aktivnosti izvršenih na računaru u određenom vremenskom periodu i ukupno.
- **Omogući stalni štit** - ova opcija vam omogućava da jednostavno uključite/isključite stalnu zaštitu. Stalni štit skenira datoteke prilikom njihovog kopiranja, otvaranja ili čuvanja. Odmah ćete biti upozoreni kada je detektovan virus ili bilo kakva pretnja. Ova funkcija je podrazumevano uključena i preporučuje se da ostane tako! Ako je stalna zaštita uključena, možete odlučiti kako da se postupi sa eventualnim detektovanim zarazama:
 - **Pitaj me pre uklanjanja pretnji** - ostavite opciju izabranu da biste potvrdili da želite da budete upitani svaki put kada se pretnja otkrije pre nego što se ona ukloni u [skladište za viruse](#). Ovaj izbor ne utiče na nivo bezbednosti, već samo zavisi od vaših želja.

- **Skeniranje u potrazi za kolačićima za praćenje** - nezavisno od prethodnih opcija, možete odlučiti da li želite da skenirate u potrazi za kolačićima za praćenje. (Kolačići su paketi teksta koje server šalje Web pregledaču, a zatim mu ih pregledač nepromenjene šalje pri svakom sledećem pristupanju serveru. HTTP kolačići služe za proveru identiteta, praćenje i održavanje određenih informacija o korisnicima, kao što su željene opcije za lokaciju ili sadržaj elektronskih kolica za kupovinu.) U određenim slučajevima, možete uključiti ovu opciju da biste postigli najviši nivo bezbednosti, ali je ona podrazumevano isključena.
- **Omogući zaštitu razmene hitnih poruka i P2P preuzimanja** - označite ovu stavku ako želite da potvrdite da je komunikacija razmenom hitnih poruka (npr. ICQ, MSN Messenger...) bezbedna od virusa.
- **Napredna podešavanja...** - kliknite na vezu da biste bili preusmereni na odgovarajući dijalog u okviru [Napredna podešavanja](#) programa **AVG Internet Security 2012**. Odatle možete detaljno urediti konfiguraciju komponente. Međutim, imajte u vidu da je podrazumevana konfiguracija svih komponenti podešena tako da **AVG Internet Security 2012** obezbeđuje optimalnu performansu i maksimalnu bezbednost. Preporučuje se da zadržite podrazumevanu konfiguraciju, osim ako nemate opravdan razlog da to ne uradite!

Kontrolna dugmad

U okviru dijaloga možete koristiti sledeću kontrolnu dugmad:

- **Upravljač izuzecima** - otvorite novi dijalog pod imenom **Stalni štit - izuzeci**. Konfiguraciji izuzetaka iz skeniranja stalnog štita možete pristupiti i iz glavnog menija, prateći redosled [Napredna podešavanja / Anti-Virus / Stalni štit / Izuzeci](#) (detaljan opis potražite u odgovarajućem poglavlju). U okviru dijaloga možete navesti datoteke i fascikle koje treba izuzeti iz skeniranja stalnog štita. Preporučujemo vam da ne izuzimate nijednu stavku ako to nije neophodno! Ovaj dijalog sadrži sledeću kontrolnu dugmad:
 - **Dodaj putanju** – navedite direktorijum (ili direktorijume) koji treba izuzeti iz skeniranja, tako što ćete sa navigacionog stabla lokalnog diska izabrati jedan po jedan.
 - **Dodaj datoteku** – navedite datoteke koje treba izuzeti iz skeniranja, tako što ćete sa navigacionog stabla lokalnog diska izabrati jednu po jednu.
 - **Uredi stavku** – omogućava vam da uređujete navedenu putanju do izabrane datoteke ili fascikle.
 - **Ukloni stavku** – omogućava vam da sa liste izbrišete putanju do izabrane stavke.
 - **Uredi listu** – omogućava vam da uredite čitavu listu definisanih izuzetaka u novom dijalogu koji se ponaša kao standardni uređivač teksta.
- **Primeni** - sačuvajte sve promene podešavanja komponente izvršene u ovom dijalogu i vratite se u glavni [korisnički interfejs](#) programa **AVG Internet Security 2012** (pregled komponenti).

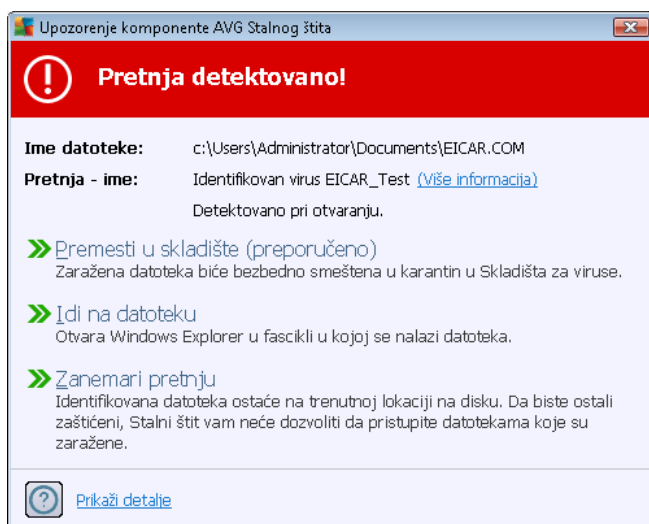


- **Otkazi** - otkazite sve promene podešavanja komponente izvršene u ovom dijalogu. Neće biti sačuvana nijedna izmena. Vratite se u glavni [korisnički interfejs](#) programa **AVG Internet Security 2012** (*pregled komponenti*).

6.1.5. Detekcije stalnog štita

Detektovana je pretnja!

Stalni štit skenira datoteke prilikom njihovog kopiranja, otvaranja ili čuvanja. Kad bude detektovan virus ili bilo kakva pretnja, o tome će vas odmah upozoriti sledeći dijalog.



U okviru ovog dijaloga upozorenja naći ćete podatke o datoteci koja je detektovana i obeležena kao zaražena (*Naziv datoteke*), naziv prepoznate infekcije (*Naziv pretnje*) i vezu ka [Enciklopediji virusa](#) gde možete naći detaljne informacije o detektovanoj infekciji, ukoliko je poznata (*Više informacija*).

Pored toga, treba da odlučite koja radnja sada treba da se izvrši. Dostupno je nekoliko alternativnih opcija. **Imajte u vidu da, zavisno od posebnih uslova (koja vrsta datoteke je zaražena i gde je locirana), nisu uvek sve opcije dostupne!**

- **Izleči** - ovo dugme se pojavljuje samo ako detektovana infekcija može biti izlečena. Zatim, uklanja se infekcija iz datoteke, i datoteka se vraća u prvobitno stanje. Ukoliko je sama datoteka virus, koristite ovu funkciju da je izbrišete (tj. premestite u [Skladište za viruse](#))
- **Premesti u Skladište (preporučuje se)** - virus će biti premešten u [Skladište za viruse](#)
- **Idi do datoteke** - ova opcija vas preusmerava do tačne lokacije sumnjivog objekta (otvara novi prozor programa *Windows Explorer*)
- **Zanemari pretnju** - savetujemo vam da NE koristite ovu opciju ako za to nemate dobar razlog!

Napomena: Može se desiti da veličina otkrivenog objekta prelazi ograničenje za slobodan prostor u skladištu za viruse. Ako se to desi, prikazaće se poruka upozorenja koja će vas obavestiti o

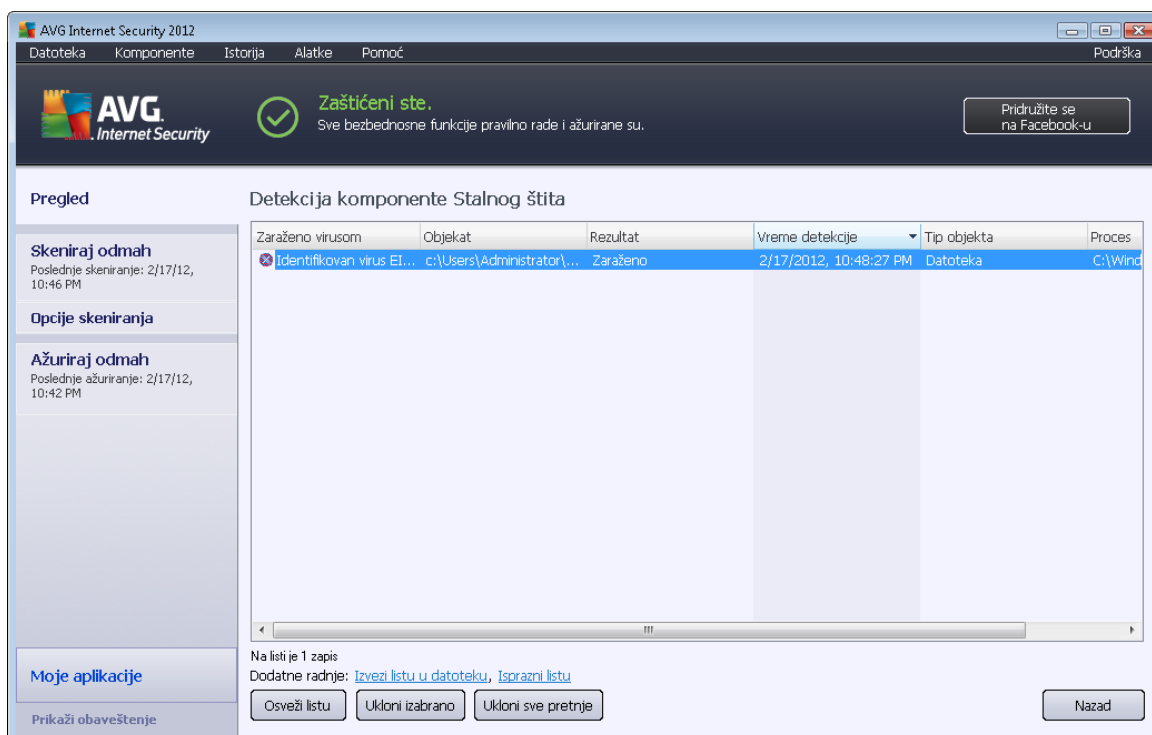


problemu kada pokušate da premestite zaraženi objekat u skladište za viruse. Međutim, veličinu skladišta za viruse možete da promenite. Ona se definiše kao procenat stvarne veličine čvrstog diska koji možete da podesite. Da biste povećali veličinu skladišta za viruse, otvorite dijalog [Skladište za viruse](#) u okviru odeljka [Napredna podešavanja programa AVG](#) tako što ćete izabrati opciju „Ograniči veličinu skladišta za viruse“.

U donjem odeljku dijaloga možete naći vezu **Prikaži detalje** - kliknite da otvorite iskačući prozor sa detaljnim informacijama o tekućim procesima tokom detekcije infekcije, i identifikacijom procesa.

Pregled detekcija od strane stalnog štita

Celokupan pregled pretnji koje je detektovao [Stalni štiti](#) možete videti u dijalogu **Detekcija od strane stalnog štita**, kojem možete pristupiti iz sistemskog menija izborom opcije [Istorija / Detekcija od strane stalnog štita](#):



Detekcija od strane stalnog štita sadrži pregled objekata koje je detektovala komponenta [Stalni štiti](#), ocenila ih kao opasne i izlečila ili premestila u fasciklu [Skladište za viruse](#). Za svaki detektovan objekat, date su sledeće informacije:

- **Infekcija** - opis (a moguće i ime) otkrivenog objekta
- **Objekat** - lokacija objekta
- **Rezultat** - radnja obavljena nad detektovanim objektom
- **Vreme otkrivanja** - datum i vreme otkrivanja objekta



- **Tip objekta** - tip detektovanog objekta
- **Proces** - radnja koja je obavljena da bi potencijalno opasan objekat mogao da se detektuje

U donjem delu dijaloga, ispod liste, pronaći ćete informacije o ukupnom broju gore navedenih detektovanih objekata. Osim toga, možete izvesti celu listu detektovanih objekata u datoteku (**Izvezi listu u datoteku**) i izbrisati sve stavke o detektovanim objektima (**Isprazni listu**). Dugme **Osveži listu** ažuriraće listu pretnji koje je pronašao **Stalni štit**. Dugme **Nazad** vas vraća u podrazumevani [glavni dijalog AVG](#) (*pregled komponenti*).

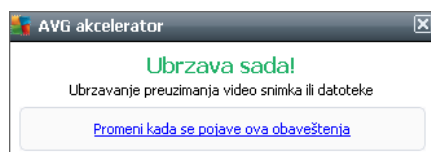
6.2. LinkScanner

LinkScanner vas štiti od rastućeg broja "danas ovde, sutra nije" pretnji na Internetu. Ove pretnje mogu biti sakrivene na bilo kom tipu Web lokacije, od vlada preko velikih, poznatih robnih marki do malih firmi, i retko se zadržavaju na tim lokacijama duže od 24 sata. **LinkScanner** vas štiti analiziranjem Web stranica iza svih veza na bilo kojoj Web stranici koju gledate i utvrđivanjem da su bezbedne u trenutku koji je najbitniji - kada kliknete na tu vezu.

LinkScanner nije namenjen za zaštitu na serverskim platformama!

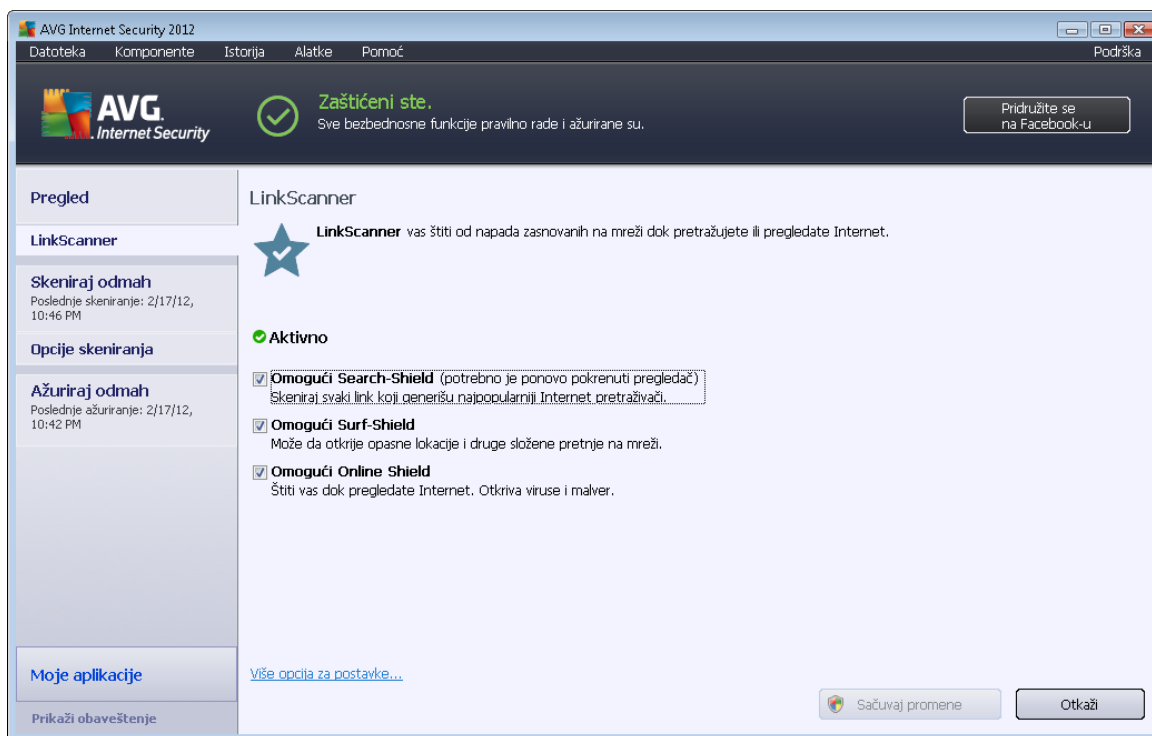
LinkScanner tehnologija se sastoji od sledećih glavnih funkcija:

- [Štit za pretraživanje](#) sadrži listu Web lokacija (*URL adresa*) za koje se zna da su opasne. Kada pretražujete koristeći Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask i Seznam, svi rezultati pretrage se proveravaju u skladu sa ovom listom i prikazuje se ikona sa ocenom (za Yahoo! rezultate pretrage prikazuju se samo ikone sa ocenom „opasna Web lokacija“).
- [Štit za pregledanje Interneta](#) skenira sadržaj Web lokacija koje posećujete, bez obzira na njihovu adresu. Čak i ako neku Web lokaciju ne otkrije [Štit za pregledanje Interneta](#) (*npr. kada se kreira nova zlonamerna Web lokacija ili kada prethodno čista Web lokacija sada sadrži neki malver*), nju će otkriti i blokirati [Štiti za pregledanje Interneta](#) čim pokušate da je posetite.
- [Online Shield](#) funkcioniše kao zaštita u realnom vremenu prilikom pregledanja Interneta. On skenira sadržaj posećenih Web stranica i moguće datoteke uključene u njih, čak i pre nego što se one prikažu u Web pregledaču ili preuzmu na računar. [Online Shield](#) otkriva viruse i špijunski softver koji se nalazi na stranici koju ćete posetiti i zaustavlja preuzimanje odmah kako nijedna pretnja ne bi došla do računara.
- **AVG akcelerator** omogućava jednostavniju reprodukciju video zapisa na mreži i olakšava dodatna preuzimanja. Kada je proces video akceleracije u toku, bićete obavešteni putem iskaćućeg prozora na sistemskoj paleti.



6.2.1. Interfejs komponente LinkScanner

Glavni dijalog komponente [LinkScanner](#) pruža kratak opis funkcionalnosti komponente i informacije o njenom trenutnom statusu (*Aktivno*):



U donjem delu dijaloga je dostupna osnovna konfiguracija komponente:

- **Omogući Štiti za pretraživanje** - (*podrazumevano uključeno*): opozovite izbor u ovom polju za potvrdu ako imate dobar razlog da isključite funkcionalnost štita za pretraživanje.
- **Omogući Štit za pregledanje Interneta** - (*podrazumevano uključeno*): aktivna zaštita (*u realnom vremenu*) od lokacija koje služe za iskorišćavanje kada im se pristupa. Veze do poznatih zlonamernih Web lokacija i njihov opasan sadržaj se blokiraju dok im korisnik pristupa pomoću Web pregledača (*ili neke druge aplikacije koja koristi HTTP*).
- **Omogući Online Shield** - (*podrazumevano uključeno*): skeniranje Web stranica koje ćete posetiti u realnom vremenu u potrazi za mogućim virusima ili špijunskim softverom. Ako se oni otkriju, preuzimanje se odmah zaustavlja kako nijedna pretnja ne bi došla do računara.

6.2.2. Detekcije štita za pretraživanje

Kada pretražujete Internet dok je funkcija **štit za pretraživanje** uključena, svi rezultati pretrage pomoću najpopularnijih pretraživača (*Google, Yahoo!, JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg i SlashDot*) biće procenjeni kako bi se proverilo da li sadrže opasne ili sumnjive linkove. Proverom veza i označavanjem onih opasnih, [LinkScanner](#) vas upozorava pre nego što kliknete na opasnu ili sumnjivu vezu, kako biste bili sigurni da ćete posećivati isključivo bezbedne lokacije.



Dok se veza proverava na stranici sa rezultatima pretrage, pored veze će se prikazivati ikona koja označava da je provera veze u toku. Po završetku procene, pojaviće se odgovarajuća informativna ikona:

Stranica na koju veza upućuje je bezbedna.

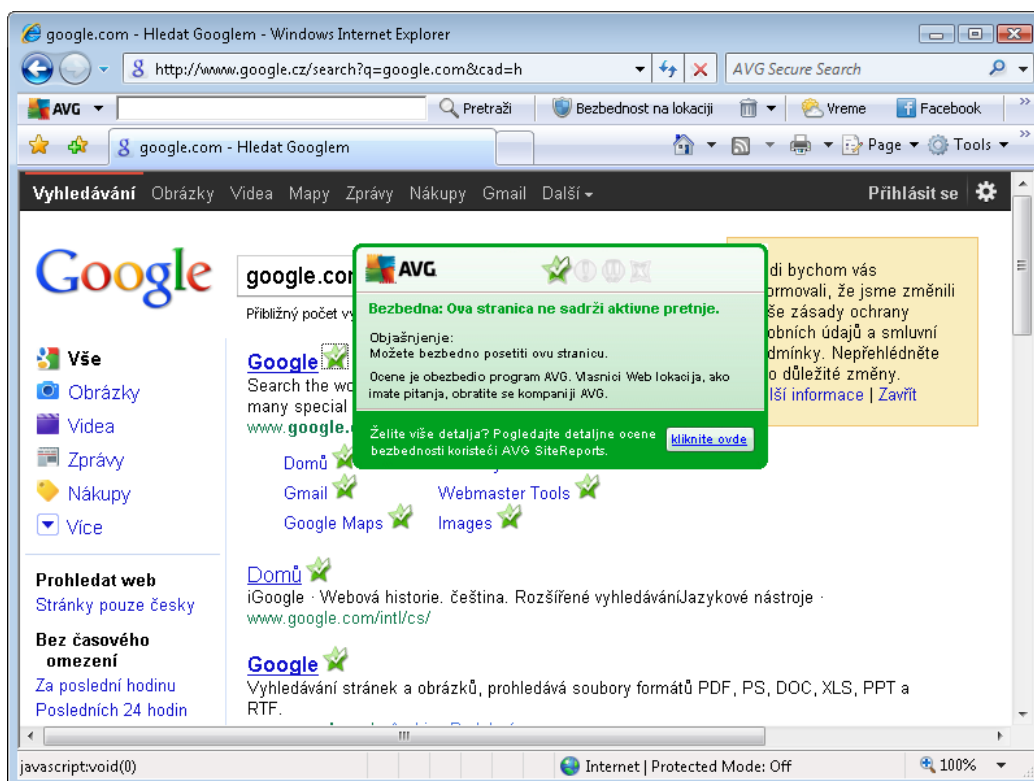
Stranica na koju link upućuje ne sadrži pretnje, ali je donekle sumnjiva (*nesigurnog porekla ili motiva, zbog čega se ne preporučuje za kupovinu na mreži itd.*).

Stranica na koju link upućuje je bezbedna, ali sadrži linkove ka stranicama koje su definitivno opasne, ili je njen kôd sumnjiv iako trenutno ne predstavlja pretnju.

Stranica na koju link upućuje sadrži aktivne pretnje! Radi vaše sopstvene bezbednosti, neće vam biti dozvoljeno da posetite ovu stranicu.

Stranica na koju link upućuje nije pristupačna, pa se ne može skenirati.

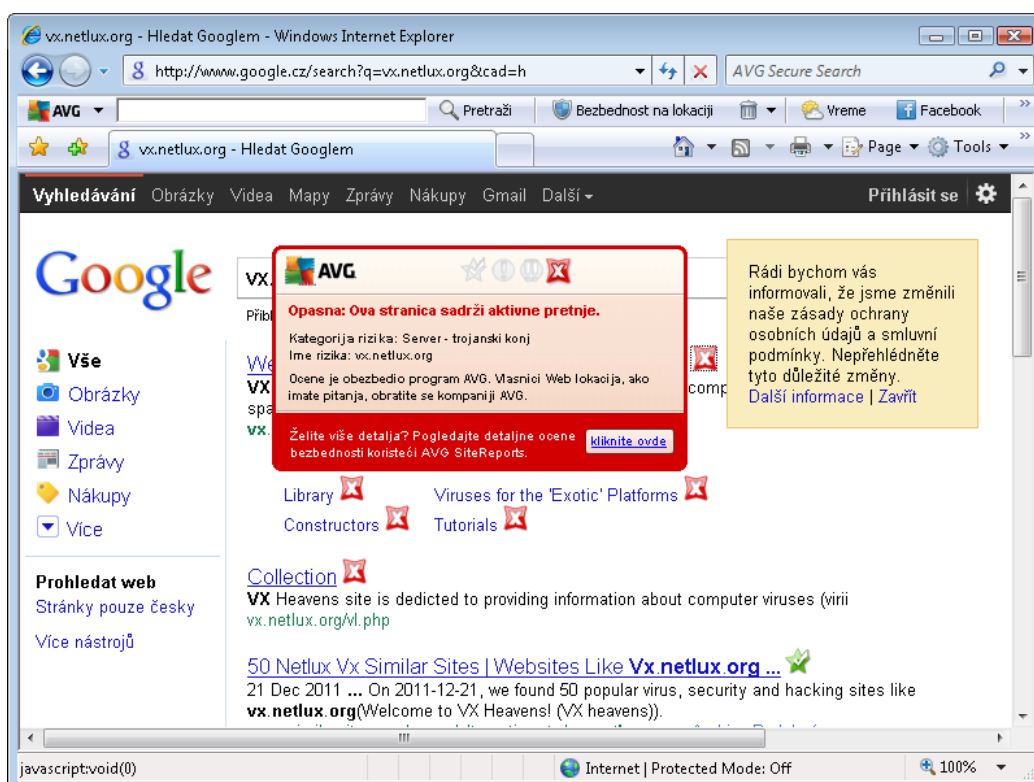
Ako postavite pokazivač iznad pojedinačnih ikona ocene, prikazaće se više informacija o tom linku. U informacije spadaju dodatne informacije o pretnji (*ako ih ima*):



6.2.3. Detekcije štita za pregledanje Interneta

Ovaj snažan vid zaštite blokira sve zlonamerne sadržaje na stranici koju pokušate da otvorite i sprečiće njegovo preuzimanje na računar. Ako je ova funkcija omogućena, a vi kliknete na link ili unesete URL adresu opasne lokacije, njeno otvaranje biće automatski blokirano kako biste bili zaštićeni od slučajne zaraze. Važno je imati u vidu da je dovoljno da posetite opasnu Web lokaciju da bi došlo do zaraze računara. Zato [LinkScanner](#) neće dozvoliti pregledaču da prikaže opasnu Web stranicu sa „exploit“ programima i drugim opasnim pretnjama kada pokušate da joj pristupite.

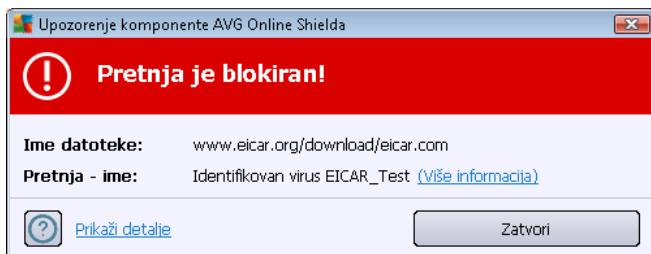
Ako naiđete na zlonamernu Web lokaciju, [LinkScanner](#) će prikazati ekran upozorenja u Web pregledaču nalik sledećem:



Ulazak na ovakvu Web lokaciju je veoma rizičan i ne preporučuje se!

6.2.4. Online Shield detekcije

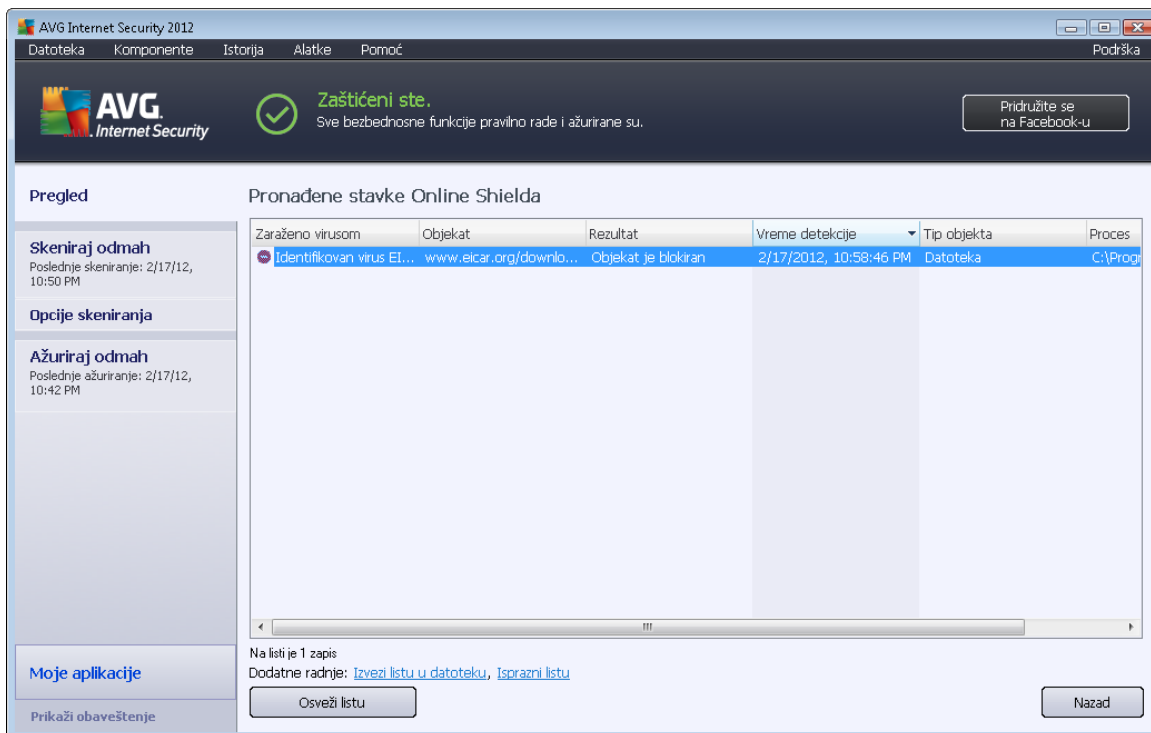
Online Shield skenira sadržaj Web stranica koje posećujete i potencijalne datoteke koje se na njima nalaze pre nego što se prikažu u vašem Web pregledaču ili preuzmu na vaš računar. Ako se detektuje pretnja, o tome ćete odmah biti obavešteni sledećim dijalogom:



U okviru ovog dijaloga upozorenja naći ćete podatke o datoteci koja je detektovana i obeležena kao zaražena (*Naziv datoteke*), naziv prepoznate infekcije (*Naziv pretnje*), i vezu ka [Enciklopediji virusa](#) gde možete naći detaljne informacije o detektovanoj infekciji (*ukoliko je poznata*). Ovaj dijalog sadrži sledeću dugmad:

- **Prikaži detalje** - kliknite na **Prikaži detalje** dugme da otvorite novi iskačući prozor gde možete naći informacije o procesima koji su se odvijali kada je infekcija detektovana, i identifikacije procesa.
- **Zatvori** - kliknite na dugme da zatvorite dijalog upozorenja.

Sumnjiva Web stranica neće biti otvorena, a otkrivena pretnja biće evidentirana na listi **Detekcije komponente Online Shield** - ovom pregledu otkrivenih pretnji možete da pristupite putem sistemskog menija [Istorija / Detekcije komponente Online Shield](#).



Za svaki detektovan objekat, date su sledeće informacije:

- **Infekcija**- opis (*a moguće i ime*) otkrivenog objekta



- **Objekat** - izvor objekta (*Web stranica*)
- **Rezultat** - radnja obavljena nad detektovanim objektom
- **Vreme otkrivanja** - datum i vreme otkrivanja i blokiranja pretnje
- **Tip objekta** - tip detektovanog objekta
- **Proces** - radnja koja je obavljena da bi potencijalno opasan objekat mogao da se detektuje

U donjem delu dijaloga, ispod liste, pronaći ćete informacije o ukupnom broju gore navedenih detektovanih objekata. Osim toga, možete izvesti celu listu detektovanih objekata u datoteku (**Izvezi listu u datoteku**) i izbrisati sve stavke o detektovanim objektima (**Isprazni listu**).

Kontrolna dugmad

- **Osveži listu** - ažurirajte listu pronađenih stavki koje je otkrio **Online Shield**
- **Nazad** - vraća vas nazad u podrazumevani [glavni dijalog AVG](#) (*pregled komponenti*)

6.3. Zaštita e-pošte

E-pošta predstavlja jedan od najčešćih izvora virusa i trojanskih konja. Phishing i bezvredna pošta čine e-poštu još većim izvorom rizika. Besplatni nalozi za e-poštu češće dobijaju takve zlonamerne e-poruke (*pošto najčešće ne primenjuju tehnologiju za zaštitu od neželjene pošte*), a kućni korisnici u velikoj meri koriste takve naloge. Izloženost kućnih korisnika napadima preko e-pošte dodatno povećava pregledanje nepoznatih Web lokacija i unošenje ličnih podataka u obrasce na mreži (*kao što je e-adresa*). Preduzeća obično koriste korporativne naloge za e-poštu i primenjuju filtere za odbranu od bezvredne pošte kako bi se smanjio rizik.

Komponenta **Zaštita e-pošte** odgovorna je za skeniranje svake poslate ili primljene e-poruke; svaki put kada se u e-poruci otkrije virus, on se odmah uklanja u [skladište za viruse](#). Ova komponenta takođe može da filtrira određene tipove priloga iz e-poruka i da dodaje sertifikacioni tekst u poruke koje nisu zaražene. **Zaštita e-pošte** se sastoji od dve glavne funkcije:

- [Skener e-pošte](#)
- [Odbrana od bezvredne pošte](#)

6.3.1. Skener e-pošte

Personalni skener e-pošte automatski skenira dolazne/odlazne poruke. Možete ga koristiti kod klijenata za e-poštu koji nemaju sopstveni dodatak za AVG, (*ali može takođe da se koristi i za skeniranje poruka e-pošte kod klijenata za e-poštu koje AVG podržava pomoću određenih dodataka, npr. Microsoft Outlook, The Bat i Mozilla Thunderbird*). Prvenstveno je namenjen korišćenju sa aplikacijama e-pošte kao što su Outlook Express, Incredimail, itd.

Tokom [instalacije](#) programa kreiraju se automatski serveri za kontrolu e-pošte: jedan za proveravanje dolazne, a drugi za proveravanje odlazne e-pošte. Upotrebom ova dva servera e-pošta se automatski proverava na portovima 110 i 25 (*standardni portovi za slanje/primanje e-pošte*).



Skener e-pošte funkcioniše kao interfejs između klijenta e-pošte i servera e-pošte na Internetu.

- **Dolazna pošta:** kada primete e-poruke sa servera, komponenta **Skener e-pošte** ih testira na viruse, uklanja zaražene priloge i dodaje certifikate. Nakon detekcije, virusi se odmah smeštaju u [Skladište za viruse](#). Poruka se zatim prosleđuje do klijenta e-pošte.
- **Odlazna pošta:** poruka se šalje od klijenta e-pošte do skenera e-pošte; on proverava da li se u poruci i njenim prilogima nalaze virusi, a zatim je šalje na SMTP server (*skeniranje odlazne pošte je podrazumevano onemogućeno i može se ručno podesiti*).

Skener e-pošte nije predviđen za serverske platforme!

6.3.2. Odbrana od bezvredne pošte

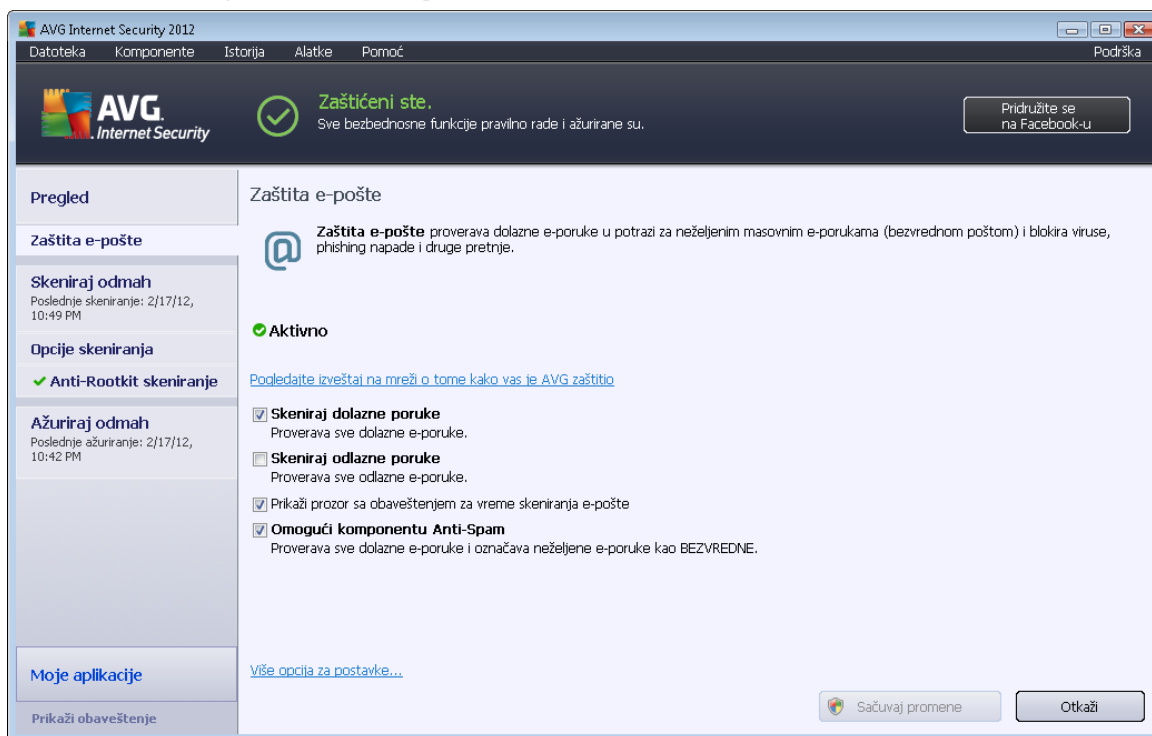
Kako Odbrana od bezvredne pošte funkcioniše?

Komponenta „odbrana od bezvredne pošte“ proverava sve dolazne e-poruke i označava neželjene e-poruke kao bezvredne. **Komponenta odbrana od bezvredne pošte** može da izmeni predmet e-poruke (*koji je identifikovan kao bezvredan*) dodavanjem posebne tekstualne niske. Zatim možete lako filtrirati e-poruke u svom klijentu e-pošte. **Komponenta „odbrana od bezvredne pošte“** koristi nekoliko metoda za analizu kako bi obradila svaku e-poruku i nudi maksimalnu zaštitu od neželjenih e-poruka. **Komponenta „odbrana od bezvredne pošte“** za otkrivanje neželjene pošte koristi bazu podataka koja se redovno ažurira. Takođe možete da koristite [RBL servere](#) (*javnu bazu podataka e-adresa „poznatih pošiljalaca“ bezvredne pošte*) i da ručno dodate e-adrese na [Belu listu](#) (*nikad ne označavaj kao neželjeno*) i [crnu listu](#) (*uvek označi kao neželjeno*).

Šta je to bezvredna pošta?

Bezvredna pošta se odnosi na neželjenu e-poštu, uglavnom reklame proizvoda ili usluga koje se masovno šalju na ogroman broj e-adresa istovremeno, puneći poštanske sandučice primalaca. Bezvredna se ne odnosi na legitimnu neželjenu e-poštu za koju su primaoci dali svoje odobrenje. Bezvredna pošta nije samo dosadna, već često može predstavljati izvor prevara, virusa ili uvredljivih sadržaja.

6.3.3. Interfejs zaštite e-pošte



U dijalogu **Zaštita e-pošte** možete pronaći kratak tekst koji opisuje funkcionalnost komponente, kao i informacije o njenom trenutnom statusu (*Aktivno*). Koristite vezu **Prikaži izveštaj na mreži o tome kako vas je AVG zaštitio** da biste pregledali detaljnu statistiku **AVG Internet Security 2012** aktivnosti i detekcija na namenjenoj stranici na AVG Web lokaciji (<http://www.avg.com/>).

Osnovna podešavanja zaštite e-pošte

U dijalogu **Zaštita e-pošte** možete dodatno urediti neke osnovne funkcije funkcionalnosti komponente:

- **Skeniraj dolazne poruke** (*podrazumevano uključeno*) - označite ovo polje da biste naveli da se sve e-poruke koje stižu na vaš nalog skeniraju kako bi se proverilo da li sadrže viruse.
- **Skeniraj odlazne poruke** (*podrazumevano isključeno*) - označite ovo polje da biste potvrdili da sve e-poruke poslate sa vašeg naloga treba da se skeniraju kako bi se proverilo da li sadrže viruse.
- **Prikaži prozor obaveštenja u toku skeniranja e-pošte** (*podrazumevano uključeno*) - označite ovu stavku da potvrdite da želite da budete obaveštavani putem dijaloga za obaveštavanje koji se prikazuje iznad [AVG ikone u sistemskoj paleti](#) tokom skeniranja e-pošte.
- **Omogući odbranu od bezzvredne pošte** (*podrazumevano uključeno*) - označite ovu stavku da biste naveli da li želite da se dolazna pošta filtrira u potrazi za neželjenom e-poštom.



Prodavac softvera je podesio sve AVG komponente, tako da se postignu optimalnu performansu. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku Alatk / Napredna podešavanja, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu [AVG napredna podešavanja](#).

Kontrolna dugmad

U dijalogu **Zaštita e-pošte** dostupna su sledeća kontrolna dugmad:

- **Sačuvaj promene** - kliknite na ovo dugme da biste sačuvali i primenili promene koje ste napravili u ovom dijalogu
- **Otkazi** - kliknite na ovo dugme da biste se vratili u podrazumevani [glavni dijalog AVG](#) (pregled komponenti)

6.3.4. Detekcija od strane skenera e-pošte

The screenshot shows the AVG Internet Security 2012 interface. The main window is titled 'Detekcija od strane Zaštita e-pošte'. It features a table with the following columns: 'Zaraženo virusom' (Infected by virus), 'Objekat' (Object), 'Rezultat' (Result), 'Vreme detekcije' (Detection time), and 'Tip objekta' (Object type). The table contains two entries, both identified as 'Identifikovan virus Eicar' (Identified Eicar virus) and 'eicar_com.zip', with the result 'Premešteno u Skladište' (Moved to storage). The detection times are '2/17/2012, 10:46:06 PM' and '2/17/2012, 10:45:57 PM', both for 'Datoteka' (File) objects. The interface also includes a sidebar with options like 'Skeniraj odmah' (Scan now), 'Opcije skeniranja' (Scan options), and 'Ažuriraj odmah' (Update now). At the bottom, there are buttons for 'Moje aplikacije' (My applications), 'Prikaži obaveštenje' (Show notification), 'Osveži listu' (Refresh list), and 'Nazad' (Back).

Zaraženo virusom	Objekat	Rezultat	Vreme detekcije	Tip objekta
Identifikovan virus Eicar	eicar_com.zip	Premešteno u Skladište	2/17/2012, 10:46:06 PM	Datoteka
Identifikovan virus Eicar	eicar_com.zip	Premešteno u Skladište	2/17/2012, 10:45:57 PM	Datoteka

U dijalogu **Detekcija e-pošte skenerom** (kojem možete pristupiti putem opcije iz sistemskog menija *Istorija / Detekcija e-pošte skenerom*), moći ćete da vidite listu svih nalaza koje je otkrila komponenta [Zaštita e-pošte](#). Za svaki detektovan objekat, date su sledeće informacije:

- **Infekcija** - opis (a moguće i ime) otkrivenog objekta
- **Objekat** - lokacija objekta



- **Rezultat** - radnja obavljena nad detektovanim objektom
- **Vreme otkrivanja** - datum i vreme otkrivanja sumnjivog objekta
- **Tip objekta** - tip detektovanog objekta

U donjem delu dijaloga, ispod liste, pronaći ćete informacije o ukupnom broju gore navedenih detektovanih objekata. Osim toga, možete izvesti celu listu detektovanih objekata u datoteku (**Izvezi listu u datoteku**) i izbrisati sve stavke o detektovanim objektima (**Isprazni listu**).

Kontrolna dugmad

U interfejsu za **detekciju od strane skenera e-pošte** dostupna su sledeća kontrolna dugmad:

- **Osveži listu** - ažurira listu otkrivenih pretnji.
- **Nazad** - prebacuje vas nazad na prethodno prikazani dijalog.

6.4. Zaštitni zid

Zaštitni zid je sistem koji nameće smernice za kontrolu pristupa između dve ili više mreža, tako što blokira/dozvoljava saobraćaj. **Zaštitni zid** sadrži skup pravila koja štite internu mrežu od napada koji potiču spolja (*obično sa Interneta*) i kontroliše kompletnu komunikaciju na svakom pojedinačnom mrežnom portu. Komunikacija se procenjuje u skladu sa definisanim pravilima, a zatim se dozvoljava ili zabranjuje. Ako **Zaštitni zid** prepozna pokušaje upada, on „blokira“ pokušaj i ne dozvoljava uljezu da pristupi računaru.

Zaštitni zid je konfigurisan da omogući ili odbije unutrašnju/spoljnu komunikaciju (obosmernu, ka unutra ili ka spolja) kroz definisane portove, kao i za definisane softverske aplikacije. Na primer, zaštitni zid se može konfigurisati tako da dozvoljava da podaci sa Interneta mogu da ulaze i izlaze samo kroz Microsoft Explorer. Svaki pokušaj prenosa podataka kroz neki drugi pregledač biće blokiran.

Zaštitni zid štiti lične informacije od slanja sa računara bez vaše dozvole. On kontroliše način na koji računar razmenjuje podatke sa drugim računarima na Internetu ili lokalnoj mreži. U okviru organizacije, **Zaštitni zid** takođe štiti pojedinačne računare od napada koje pokrenu interni korisnici na drugim računarima na mreži.

Računari koje ne štiti Zaštitni zid postaju laka meta za računarske hakere i krađu podataka.

Preporuka: ne preporučuje se upotreba više zaštitnih zidova na jednom računaru. Bezbednost računara se ne poboljšava ako instalirate više zaštitnih zidova. Verovatno će doći do neusaglašenosti između ove dve aplikacije. Zbog toga vam preporučujemo da koristite samo jedan zaštitni zid na računaru i da deaktivirate ostale čime ćete eliminisati rizik od mogućih neusaglašenosti i problema.



6.4.1. Principi funkcionisanja zaštitnog zida

U aplikaciji **AVG Internet Security 2012**, **Zaštitni zid** kontroliše saobraćaj na svakom mrežnom portu računara. Na osnovu definisanih pravila, **Zaštitni zid** procenjuje aplikacije koje su pokrenute na računaru (*i žele da se povežu sa Internetom/lokalnom mrežom*) ili aplikacije koje spolja pristupaju računaru pokušavajući da se povežu sa njim. Za svaku od ovih aplikacija **Zaštitni zid** zatim dozvoljava ili zabranjuje komunikaciju na mrežnim portovima. Podrazumevano, ako je aplikacija nepoznata (*tj. nema definisana pravila Zaštitnog zida*), **Zaštitni zid** će vas pitati da li želite da dozvolite ili blokirate pokušaj komunikacije.

AVG zaštitni zid nije predviđen za serverske platforme!

Mogućnosti koje nudi AVG zaštitni zid:

- Dozvoljavanje ili blokiranje pokušaja komunikacije poznatih [aplikacija](#) automatski ili uz vašu potvrdu
- Korišćenje čitavih [profila](#) sa unapred definisanim pravilima u skladu sa vašim potrebama
- [Menjanje profila](#) automatski prilikom povezivanja na različite mreže ili upotrebe različitih mrežnih adaptera

6.4.2. Profili zaštitnog zida

[Zaštitni zid](#) vam omogućava da definišete određena bezbednosna pravila na osnovu toga da li se vaš računar nalazi u domenu, da li je u pitanju samostalan računar ili prenosni računar. Svaka od tih opcija zahteva različit nivo zaštite, a te nivoe pokrivaju odgovarajući profili. Dakle, profil [Zaštitnog zida](#) je određena konfiguracija komponente [Zaštitni zid](#), a možete koristiti nekoliko unapred definisanih konfiguracija.

Dostupni profili

- **Dozvoli sve** – sistemski profil komponente [Zaštitni zid](#), unapred podešen od strane proizvođača i uvek dostupan. Kada se ovaj profil aktivira, svaki vid komunikacije preko mreže je dozvoljen i ne primenjuju se nikakve bezbednosne smernice, kao da je [Zaštitni zid](#) isključen (tj. sve aplikacije su dozvoljene, ali se paketi ipak proveravaju – da bi se filtriranje u potpunosti onemogućilo, potrebno je da onemogućite Zaštitni zid). Ovaj sistemski profil se ne može duplicirati, izbrisati i njegove postavke se ne mogu izmeniti.
- **Blokiraj sve** – sistemski profil komponente [Zaštitni zid](#), unapred podešen od strane proizvođača i uvek dostupan. Kada se ovaj profil aktivira, svaki vid komunikacije preko mreže je blokiran i računaru se ne može pristupiti sa spoljnih mreža niti on može da komunicira spolja. Ovaj sistemski profil se ne može duplicirati, izbrisati i njegove postavke izmeniti.
- **Prilagođeni profili** – prilagođeni profili vam omogućavaju da iskoristite prednosti automatske zamene profila koja može biti naročito korisna ako se često povezujete sa različitim mrežama (*npr. sa prenosnog računara*). Prilagođeni profili se generišu automatski nakon instaliranja aplikacije **AVG Internet Security 2012** i pokrivaju sve pojedinačne



potrebe za pravila smernice za [Zaštitni zid](#). Dostupni su sledeći prilagođeni profili:

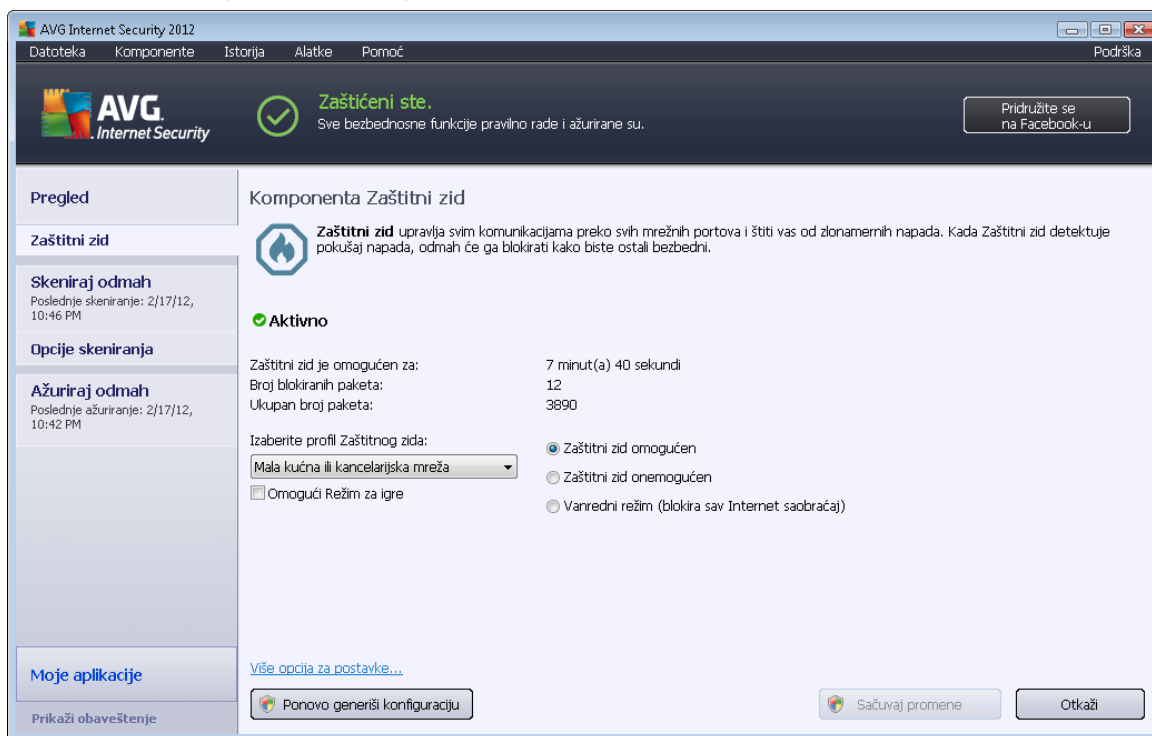
- **Direktno povezano sa Internetom** – pogodan za uobičajene kućne računare ili prenosne računare povezane direktno sa Internetom, bez dodatne zaštite. Ova opcija se preporučuje i kada povezujete prenosni računar sa različitim nepoznatim i verovatno nebezbednim mrežama (*npr. u Internet kafeu, hotelskoj sobi itd.*). Najstroža pravila smernice [Zaštitnog zida](#) iz ovog profila osiguravaju da takvi računari budu odgovarajuće zaštićeni.
- **Računar u okviru domena** – pogodno za računare na lokalnoj mreži, obično u školi ili na poslu. Pretpostavlja se da mreža ima profesionalnog administratora i da je zaštićena dodatnim merama, tako da nivo bezbednosti može biti niži nego u gorenavedenim slučajevima, čime se dozvoljava pristup deljenim fasciklama, jedinicama diska itd.
- **Mala kućna ili kancelarijska mreža** – pogodno za računare na maloj mreži, obično kod kuće ili u malom preduzeću. Ova vrsta mreže obično nema „centralnog“ administratora i sastoji se od svega nekoliko međusobno povezanih računara, koji često dele štampač, skener ili slični uređaj, što moraju da odražavaju pravila [Zaštitnog zida](#).

Zamena profila

Funkcija zamene profila [Zaštitnom zidu](#) omogućava da se automatski prebaci na definisani profil prilikom korišćenja određenog mrežnog adaptera ili prilikom povezivanja sa određenim tipom mreže. Ako nekoj mrežnoj oblasti još nije dodeljen profil, prilikom sledećeg povezivanja sa tom oblašću, [Zaštitni zid](#) će prikazati dijalog kojim se od vas traži da joj dodelite profil. Možete dodeliti profile svim lokalnim mrežnim interfejsima, a dodatne postavke možete podesiti u dijalogu [Profili za oblasti i mrežne kartice](#), u kojem možete i onemogućiti ovu funkciju ako ne želite da je koristite (*u tom slučaju, podrazumevani profil će se koristiti za sve veze*).

Ova funkcija je uglavnom korisna za korisnike prenosnog računara koji koriste različite tipove veza. Ako imate stoni računar, a koristite samo jedan tip veze (*npr. kablovsku vezu sa Internetom*), ne morate da podešavate funkciju zamene profila jer vam verovatno nikada neće biti potrebna.

6.4.3. Interfejs zaštitnog zida



Glavni dijalog pod imenom **Komponenta Zaštitni zid** obezbeđuje osnovne informacije o funkcionalnosti komponente, njenom statusu (*Aktivno*) i kratak pregled statističkih podataka komponente:

- **Zaštitni zid je omogućen u trajanju od** – vremenski period od trenutka kada je [Zaštitni zid](#) poslednji put pokrenut
- **Blokirani paketi** – broj blokiranih paketa u odnosu na sve proverene pakete
- **Ukupan broj paketa** – broj svih proverenih paketa u toku rada komponente [Zaštitni zid](#)

Osnovne postavke Zaštitnog zida

- **Izaberite profil Zaštitnog zida** – iz padajućeg menija izaberite neki od definisanih profila (*detaljan opis svakog profila i preporučenu upotrebu potražite u poglavlju [Profili Zaštitnog zida](#)*)
- **Omogući režim „Igre“** – označite izbor ove opcije da biste osigurali da se prilikom pokretanja aplikacija u režimu celog ekrana (*igre, prezentacije, filmovi itd.*), neće pojavljivati dijalozi u kojima vas [zaštitni zid](#) pita da li želite da dozvolite ili blokirate komunikaciju sa nepoznatim aplikacijama. Ako za to vreme nepoznata aplikacija pokuša da komunicira preko mreže, [Zaštitni zid](#) će automatski dozvoliti ili blokirati pokušaj na osnovu postavki trenutnog profila. **Napomena:** Dok je režim za igre uključen, svi planirani zadaci (skeniranja, ažuriranja) se odlažu dok ne zatvorite aplikaciju.



- Osim toga, u ovom odeljku sa osnovnim postavkama možete da izaberete neku od tri alternativne opcije koje definišu trenutni status komponente [Zaštitni zid](#):
 - **Zaštitni zid je omogućen** (podrazumevano) – izaberite ovu opciju da biste dozvolili komunikaciju sa onim aplikacijama koje su dodeljene kao „dozvoljene“ u skupu pravila definisanih u okviru izabranog profila [zaštitnog zida](#).
 - **Zaštitni zid onemogućen** – ova opcija potpuno isključuje [zaštitni zid](#), pa je sav mrežni saobraćaj dozvoljen, ali se ne proverava!
 - **Hitni režim (blokira sav Internet saobraćaj)** – izaberite ovu opciju da biste blokirali sav saobraćaj na svim mrežnim portovima; [Zaštitni zid](#) je i dalje aktivan, ali je sav mrežni saobraćaj obustavljen.

Imajte u vidu sledeće: Prodavac softvera je podesio sve komponente programa AVG Internet Security 2012 za postizanje optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Postavke smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju zaštitnog zida, iz sistemskog menija izaberite stavku **Alatke / Postavke zaštitnog zida**, pa u dijalogu [Postavke zaštitnog zida](#) uredite konfiguraciju zaštitnog zida.

Kontrolna dugmad

- **Regeneriši konfiguraciju** - pritisnite ovo dugme da zamenite trenutnu konfiguraciju [Zaštitnog zida](#) i vratite se na podrazumevanu konfiguraciju zasnovanu na automatskoj detekciji.
- **Sačuvaj promene** – kliknite na ovo dugme da biste sačuvali i primenili promene koje ste napravili u ovom dijalogu.
- **Otkazi** – kliknite na ovo dugme da biste se vratili u podrazumevani [glavni AVG dijalog](#) (pregled komponenti).

6.5. Anti-Rootkit

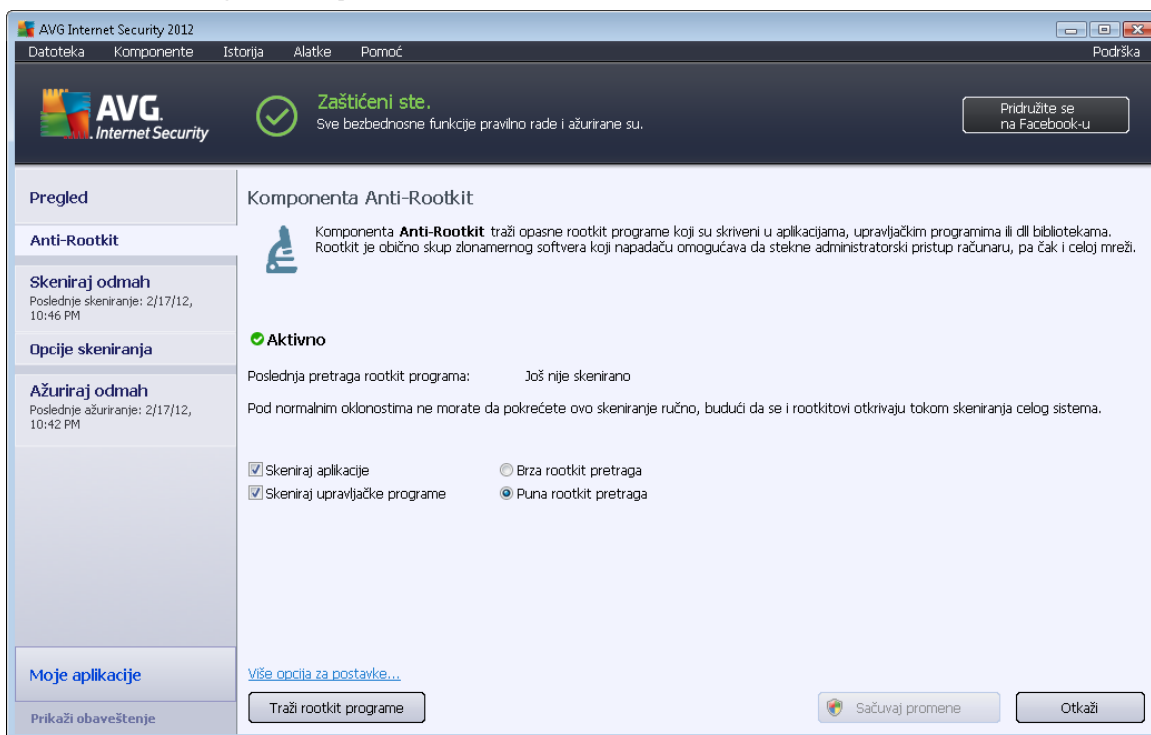
Anti-Rootkit je specijalizovana alatka koja detektuje i efikasno uklanja opasne rootkit programe, tj. programe i tehnologije čiji je cilj da kamufliraju zlonamerni softver na vašem računaru. **Anti-Rootkit** može da otkrije rootkit programe na osnovu unapred definisanog skupa pravila. Imajte u vidu da se otkrivaju svi rootkit programi (ne samo oni koji su zaraženi). Ukoliko **Anti-Rootkit** pronađe rootkit program, to ne mora da znači da je taj rootkit program zaražen. Ponekad se rootkit programi koriste kao upravljački programi ili su deo bezopasnih aplikacija.

Šta je to rootkit?

Rootkit je program osmišljen da preuzme potpunu kontrolu nad računarskim sistemom bez dozvole vlasnika sistema i administratora kojima je dozvoljen pristup. Pristup hardveru nije potreban jer je cilj rootkit programa da preuzme kontrolu nad operativnim sistemom koji je instaliran na hardveru. Rootkit programi najčešće prikrivaju svoje prisustvo na sistemu pomoću subverzije ili izbegavanja standardnih mehanizama za zaštitu operativnog sistema. Ti programi najčešće spadaju u red

trojanskih konja, pa su u stanju da prevare korisnike kako bi poverovali da ih mogu bezbedno pokrenuti na sistemu. Tehnike kojima se to postiže obuhvataju prikrivanje aktivnih procesa kako ih ne bi videli programi za nadgledanje ili sakrivanje datoteka ili sistemskih podataka od operativnog sistema.

6.5.1. Interfejs komponente Anti-Rootkit



Dijalog **Anti-Rootkit** obezbeđuje kratak opis funkcionalnosti komponente, informiše o trenutnom statusu komponente (**Aktivno**) i pruža informacije o poslednjem pokretanju **Anti-Rootkit** testa (*poslednja rootkit pretraga; rootkit test je podrazumevani proces koji se pokreće u okviru [skeniranja celog računara](#)*). Dijalog **Anti-Rootkit** dalje pruža vezu ka opcijama [Alati/Napredna podešavanja](#). Koristite vezu da se preusmerite ka okruženju za napredno konfigurisanje **Anti-Rootkit** komponente.

Prodavac softvera je podesio sve AVG komponente, tako da se postignu optimalna performansa. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja bi trebalo da menjaju samo iskusni korisnici.

Osnovna Anti-Rootkit podešavanja

U donjem delu dijaloga možete podesiti neke osnovne funkcije skeniranja rootkit prisutnosti. Prvo potvrdite izbor u odgovarajućim poljima za potvrdu da biste odredili objekte koje bi trebalo skenirati:

- **Skeniraj aplikacije**
- **Skeniraj upravljačke programe**



Zatim možete izabrati režim rootkit skeniranja:

- **Brzo rootkit skeniranje** - skenira sve aktivne procese, učitane upravljačke programe i sistemsku fasciklu (*obično c:\Windows*).
- **Potpuno rootkit skeniranje** - skenira sve aktivne procese, učitane upravljačke programe, sistemsku fasciklu (*obično c:\Windows*), kao i sve lokalne diskove (*uključujući fleš disk, ali izuzimajući disketnu/CD jedinicu*).

Kontrolna dugmad

- **Traži rootkit programe** - pošto rootkit skeniranje nije podrazumevani deo [Skeniranja celog računara](#), pomoću ovog dugmeta ga možete direktno pokrenuti iz **Anti-Rootkit** interfejsa.
- **Sačuvaj promene** - pritisnite ovo dugme da biste sačuvali sve izmene unete u ovom interfejsu i vratili se u podrazumevani [AVG korisnički interfejs](#) (*pregled komponenti*).
- **Otkazi** - pritisnite ovo dugme da biste se vratili u podrazumevani [glavni dijalog AVG](#) (*pregled komponenti*) bez čuvanja unetih izmena.

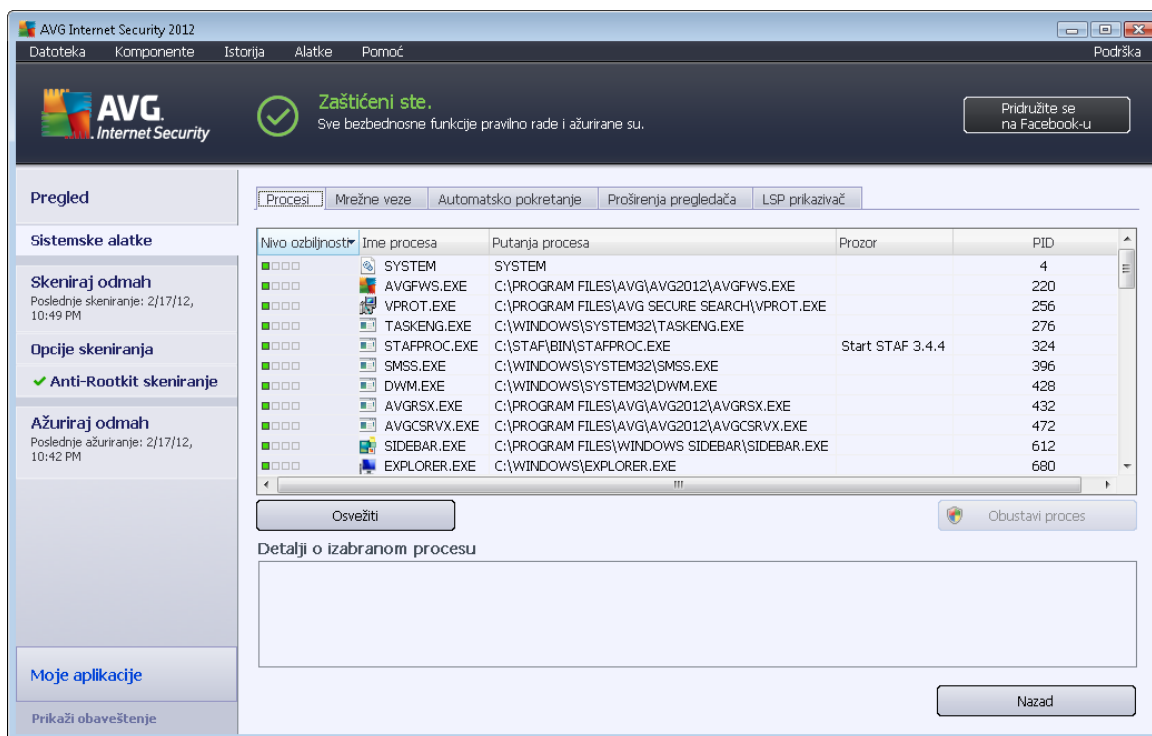
6.6. Sistemske alatke

Sistemske alatke – odnosi se na alatke koje pružaju detaljan pregled **AVG Internet Security 2012** okruženja i operativnog sistema. Komponenta nudi pregled:

- [Procesa](#) - lista procesa (*tj. pokrenutih aplikacija*) koji su trenutno aktivni na vašem računaru
- [Mrežnih veza](#) - lista trenutno aktivnih veza
- [Aplikacija koje se automatski pokreću](#) - lista svih aplikacija koje se izvršavaju tokom pokretanja operativnog sistema Windows
- [Proširenja pregledača](#) - lista dodatnih komponenti (*tj. aplikacija*) koje su instalirane unutar vašeg Internet pregledača
- [LSP pregledač](#) - lista dobavljača slojevitih usluga (LSP)

Određeni pregledi se mogu urediti, ali se to preporučuje samo veoma iskusnim korisnicima!

6.6.1. Procesi



Dijalog **Procesi** sadrži listu procesa (*tj. aktivnih aplikacija*) koji su trenutno aktivni na vašem računaru. Lista je podeljena na više kolona:

- **Nivo ozbiljnosti** – grafički prikaz ozbiljnosti odgovarajućeg procesa na skali od četiri nivoa počevši od manje ozbiljne pretnje (■ □ □ □) pa do veoma ozbiljne (■ ■ ■ ■)
- **Ime procesa** - ime aktivnog procesa.
- **Putanja procesa** - fizička putanja do pokrenutog procesa
- **Prozor** - označava ime prozora aplikacije, ako je primenljivo
- **PID** - identifikacioni broj procesa je jedinstveni interni Windows identifikator procesa

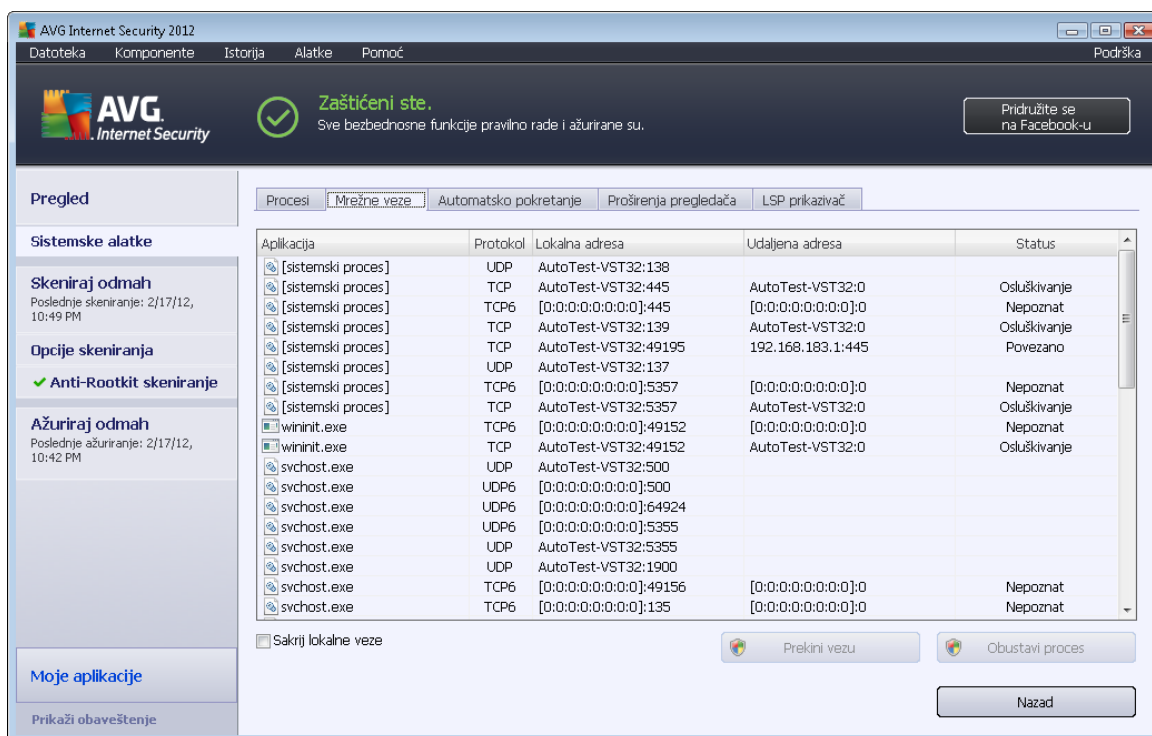
Kontrolna dugmad

Na kartici **Procesi** dostupna su sledeća kontrolna dugmad:

- **Osveži** - ažuriranje liste procesa u skladu sa trenutnim statusom
- **Prekini proces** - možete izabrati jednu ili više aplikacija, a zatim prekinuti njihovo izvršavanje tako što ćete kliknuti na ovo dugme. **Savetujemo da ne zaustavljate nijednu aplikaciju ako niste potpuno sigurni da predstavljaju realnu pretnju!**

- **Nazad** - vraća vas nazad u podrazumevani [glavni dijalog AVG](#) (pregled komponenti).

6.6.2. Mrežne veze



U dijalogu **Mrežne veze** prikazana je lista trenutno aktivnih veza. Ta lista je podeljena na sledeće kolone:

- **Aplikacija** - ime aplikacije koja se odnosi na vezu (izuzev operativnog sistema Windows 2000 gde ove informacije nisu dostupne)
- **Protokol** - tip protokola za prenos koji se koristi za vezu:
 - TCP - protokol koji se koristi zajedno sa Internet protokolom (IP) za prenos informacija preko Interneta
 - UDP - alternativa TCP protokolu
- **Lokalna adresa** - IP adresa lokalnog računara i broj porta koji se koristi
- **Udaljena adresa** - IP adresa udaljenog računara i broj porta koji se koristi Takođe će potražiti ime domaćina na udaljenom računaru, ako je to moguće.
- **Status** - označava najverovatnije trenutno stanje (*Povezano, Server treba da zatvori vezu, Osluškivanje, Aktivno zatvaranje završeno, Pasivno zatvaranje, Aktivno zatvaranje*)

Da biste na listi prikazali samo eksterne veze, potvrdite izbor u polju za potvrdu **Sakrij lokalne veze** u donjem odeljku dijaloga ispod liste.

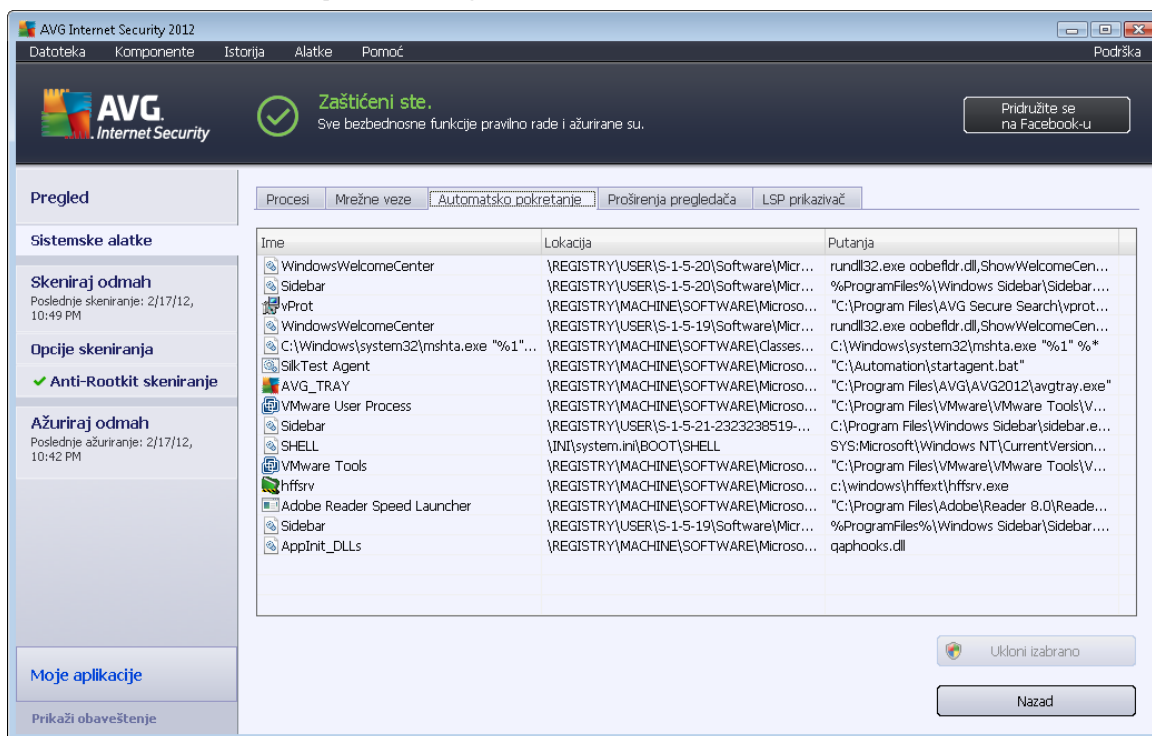
Kontrolna dugmad

Na kartici **Mrežne veze** dostupna su sledeća kontrolna dugmad:

- **Prekini vezu** - prekidanje jedne ili više mreža koje ste izabrali na listi
- **Prekini proces** - zatvaranje jedne ili više aplikacija koje koriste vezu izabranu na listi
- **Nazad** - vraća vas nazad u podrazumevani [glavni dijalog AVG](#) (pregled komponenti).

Ponekad je moguće zaustaviti samo one aplikacije koje su trenutno u stanju uspostavljene veze. Savetujemo da ne prekidate nijednu vezu osim ako niste potpuno sigurni da predstavljaju realnu pretnju!

6.6.3. Automatsko pokretanje



U dijalogu **Automatsko pokretanje** data je lista svih aplikacija koje se pokreću zajedno sa operativnim sistemom Windows. Vrlo često se dešava da se nekoliko malver aplikacija doda u stavku pokretanja u registratoru.

Kontrolna dugmad

Na kartici **Automatsko pokretanje** dostupna su sledeća kontrolna dugmad:

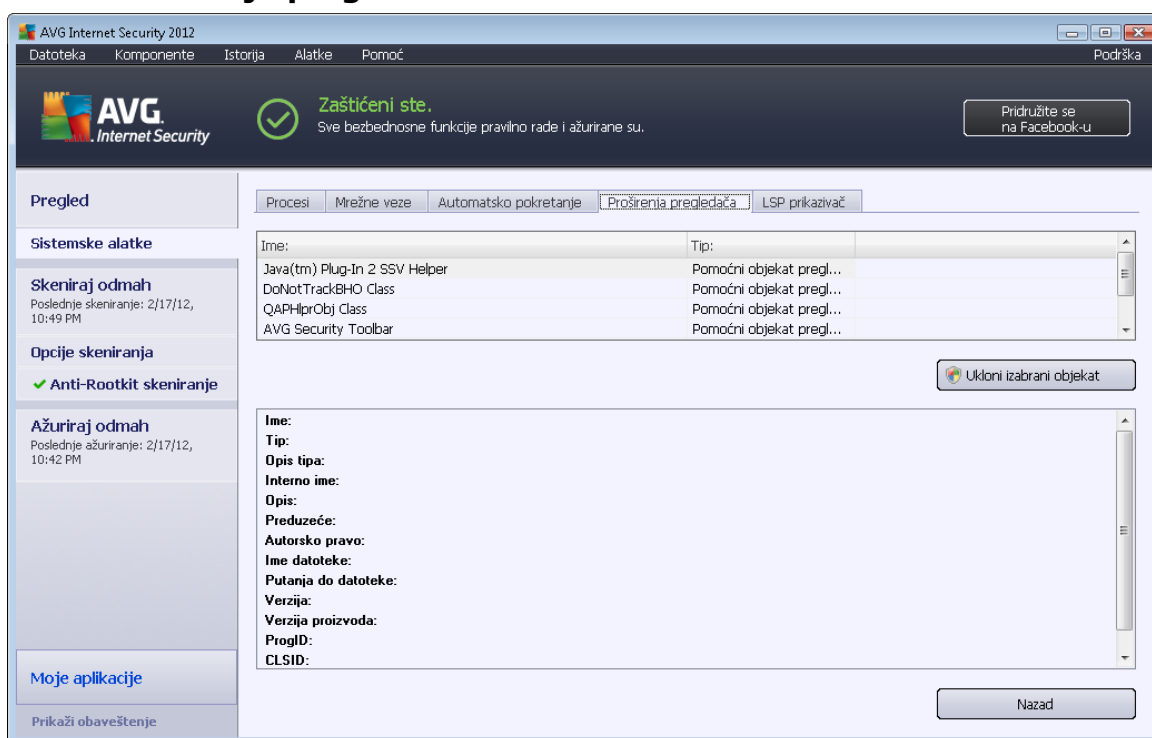
- **Ukloni izabrano** - kliknite na ovo dugme da biste izbrisali neke izabrane stavke.



- **Nazad** - vraća vas nazad u podrazumevani [glavni dijalog AVG](#) (pregled komponenti).

Savetujemo da ne brišete nijednu aplikaciju sa liste, osim ako niste potpuno sigurni da predstavljaju realnu pretnju!

6.6.4. Proširenja pregledača



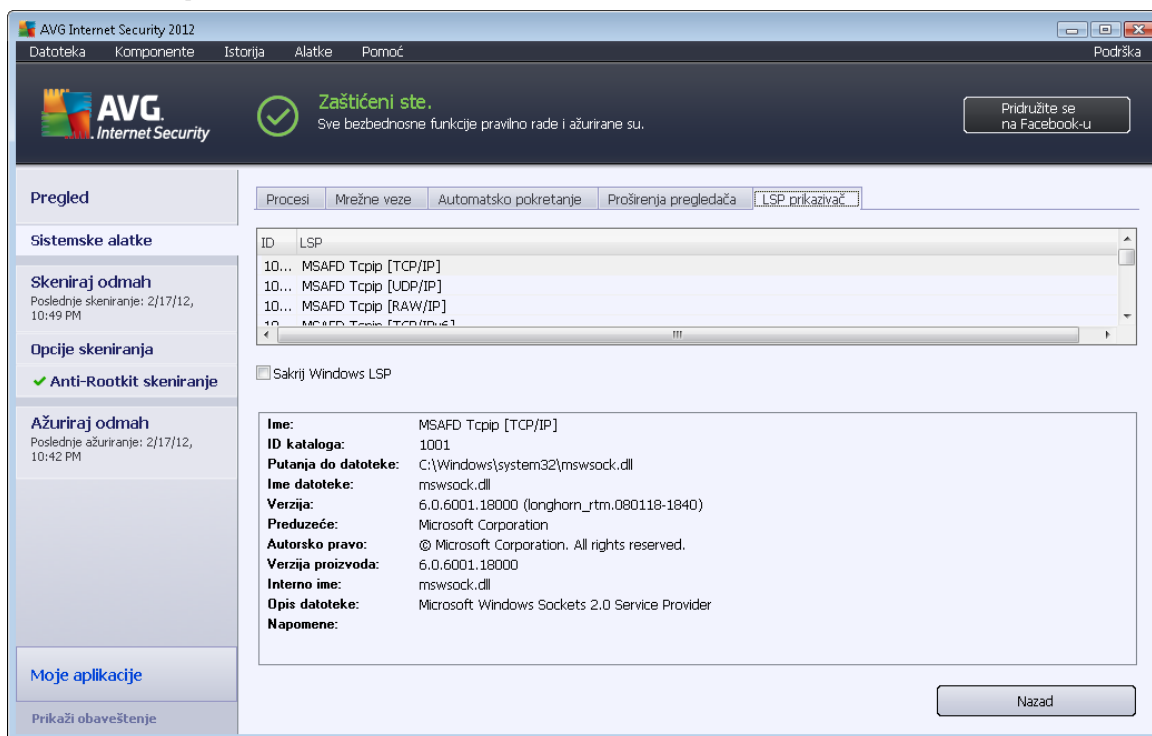
Dijalog **Proširenja pregledača** sadrži listu dodatnih komponenta (*tj. aplikacija*) koje su instalirane u Internet pregledaču. Ova lista može da sadrži standardne dodatne komponente kao i potencijalne malver programe. Kliknite na objekat na listi da biste dobili detaljne informacije o izabranoj dodatnoj komponenti koje će se prikazivati u donjem odeljku dijaloga.

Kontrolna dugmad

Na kartici **Proširenja pregledača** dostupna su sledeća kontrolna dugmad:

- **Ukloni izabrani objekat** - uklanjanje dodatne komponente koja je trenutno označena na listi. **Savetujemo da ne brišete dodatne komponente sa liste, osim ako niste potpuno sigurni da predstavljaju realnu pretnju!**
- **Nazad** - vraća vas nazad u podrazumevani [glavni dijalog AVG](#) (pregled komponenti).

6.6.5. LSP prikazivač



Na kartici **LSP prikazivač** prikazana je lista LSP-ova (Layered Service Providers).

Dobavljač slojevitih usluga (LSP) je sistemski upravljački program povezan sa uslugama umrežavanja operativnog sistema Windows. On ima pristup svim podacima koji se unose na računar, kao i onima koji se šalju sa računara, uključujući i mogućnost izmene ovih podataka. Neki LSP-ovi su neophodni da bi se operativnom sistemu Windows dozvolilo da se poveže sa drugim računarima, uključujući i Internet. Međutim, određene malver aplikacije takođe mogu da se instaliraju kao LSP i na taj način imaju pristup svim podacima koje prenosi računar. Zato vam ovaj pregled može pomoći da proverite sve moguće LSP pretnje.

Takođe, ponekad je moguće popraviti prekinute LSP-ove (*na primer, kada je datoteka uklonjena, ali su stavke registratora ostale netaknute*). Novo dugme za popravku problema prikazuje se kada se otkrije LSP koji se može popraviti.

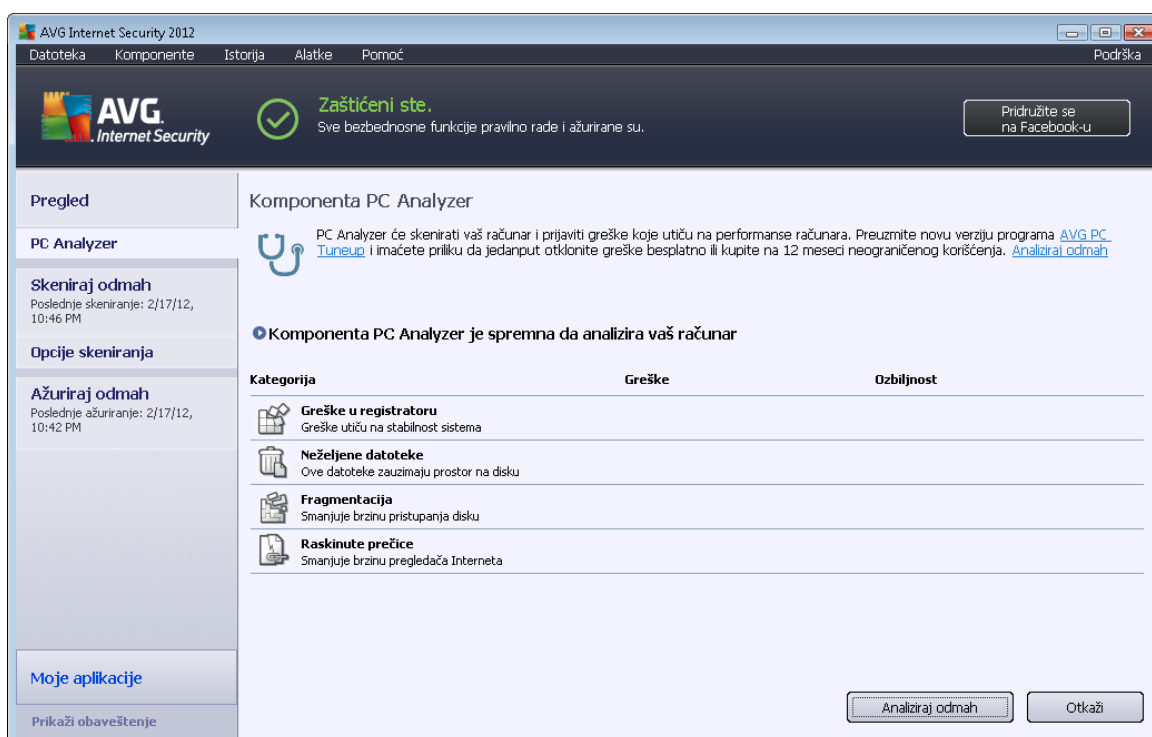
Kontrolna dugmad

Na kartici **LSP prikazivač** dostupna su sledeća kontrolna dugmad:

- **Sakrij Windows LSP** - da biste Windows LSP uključili na listu, opozovite izbor ove stavke.
- **Nazad** - vraća vas nazad u podrazumevani [glavni dijalog AVG](#) (pregled komponenti).

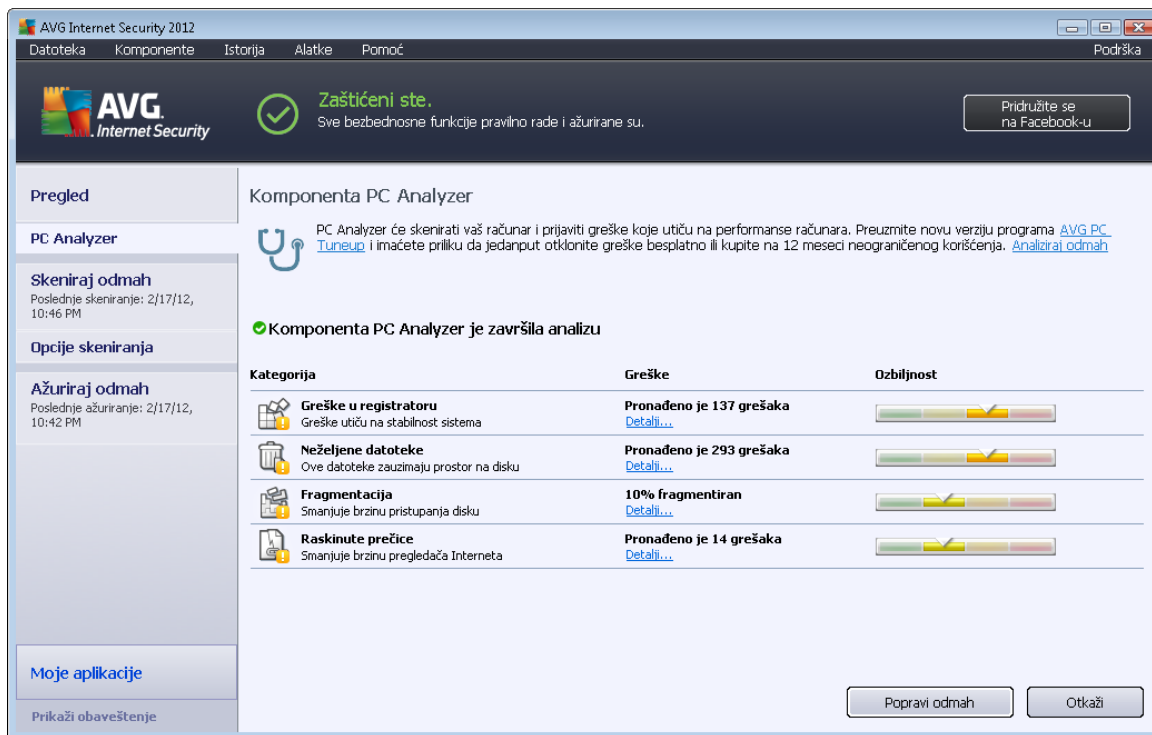
6.7. PC Analyzer

Komponenta **PC Analyzer** može da skenira vaš računar tražeći sistemske probleme i da vam pruži jasan pregled onoga što može da otežava opšte performanse vašeg računara. U korisničkom interfejsu komponente možete videti tabelu podeljenu u četiri reda koji se odnose na odgovarajuće kategorije: greške u registratoru, nepoželjne datoteke, fragmentacija i oštećene prečice:



- **Greške u registratoru** prikazuje broj grešaka u Windows registratoru. Pošto je za popravljavanje registratora potrebno napredno znanje o računarima, ne preporučujemo da ih sami popravljate.
- **Nepoželjne datoteke** prikazuju broj datoteka koje vam verovatno nisu potrebne. Obično su to razne vrste privremenih datoteka, kao i datoteke u korpi za otpatke.
- **Fragmentacija** izračunava koji je procenat čvrstog diska fragmentiran, tj. koji usled dugotrajne upotrebe sadrži rasute datoteke na različitim delovima fizičkog diska. Možete koristiti neke alate za defragmentaciju kako biste ovo popravili.
- **Oštećene prečice** prikazuju prečice koje više ne rade, vode do nepostojećih lokacija, itd.

Da započnete analiziranje vašeg sistema, kliknite na dugme **Analiziraj sada**. Moći ćete da pratite tok analize i njene rezultate direktno u tabeli:



Pregled rezultata pruža broj detektovanih sistemskih problema (**Greške**) podeljene prema odgovarajućim testiranim kategorijama. Rezultati analize će takođe biti prikazani grafički na jednoj osi u koloni **Ozbiljnost**.

Kontrolna dugmad

- **Analiziraj sada** (*prikazano pre nego što analiza počne*) - pritisnite ovo dugme da pokrenete momentalnu analizu vašeg računara
- **Popravi odmah** (*prikazuje se kada se analiza završi*) - kliknite na ovo dugme da biste otišli na AVG Web lokaciju (<http://www.avg.com/>) na stranicu koja pruža detaljne i aktuelne informacije u vezi sa komponentom **PC Analyzer**
- **Otkazi** - kliknite na ovo dugme da biste zaustavili pokrenutu analizu ili da biste se vratili u podrazumevani [glavni dijalog AVG](#) (*pregled komponenti*) kada se analiza dovrši

6.8. Identity Protection

Identity Protection je komponenta odbrane od malvera koja vas štiti od različitih vrsta malvera (špijuskog softvera, botova, krađe identiteta, ...) upotrebom tehnologija za analizu ponašanja i pruža zaštitu od nepoznatih i novih virusa. **Namena zaštite identiteta** jeste da spreči kradljivce identiteta da ukradu vaše lozinke, podatke o bankovnom računu, brojeve kreditnih kartica i zaštita vrednih digitalnih podataka od svih vrsta zlonamernog softvera (*malvera*) usmerenog na vaš računar. On obezbeđuje da svi programi pokrenuti na računaru ili na deljenoj mreži ispravno funkcionišu.

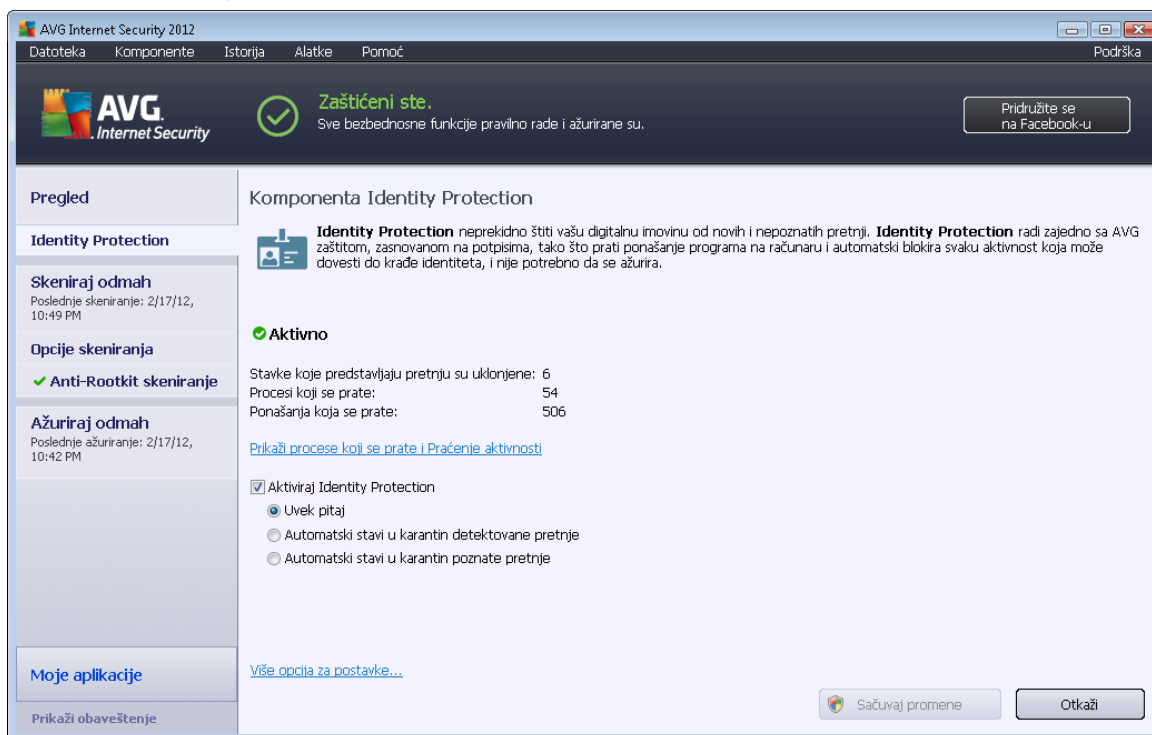
Identity Protection konstantno uočava i blokira sumnjivo ponašanje i štiti vaš računar od svih vrsta novog malvera.



Identity Protection pruža računar zaštitu u realnom vremenu od novih i nepoznatih pretnji. Ona nadgleda sve (*uključujući skrivene*) procese i preko 285 različitih obrazaca ponašanja i može da utvrdi ako se nešto zlonamerno desilo u sistemu. Zato je u stanju da otkrije čak i one pretnje koje još nisu opisane u bazi podataka o virusima. Kada na računar dospe nepoznat kôd, on se posmatra i prati kako bi se proverilo da li pokazuje znake zlonamernog ponašanja. Ako se otkrije da je datoteka zlonamerna, **Identity Protection** će premestiti kôd u [Skladište za viruse](#) i opozvati sve promene koje su izvršene u sistemu (*ubacivanja koda, promene registratora, otvaranje portova itd.*). Nije potrebno da pokrećete skeniranje da biste bili zaštićeni. Ova tehnologija je veoma proaktivna, retko se ažurira i uvek je na oprezu.

Identity Protection predstavlja dodatnu zaštitu [Antivirusnom programu](#). Preporučuje se da imate instalirane obe komponente da biste imali potpunu zaštitu za računar!

6.8.1. Interfejs zaštite identiteta



Dijalog **Identity Protection** pruža kratak opis osnovne funkcionalnosti komponente, njen status (*Aktivno*) i neke statističke podatke:

- **Uklonjene pretnje** - pruža broj aplikacija koje su otkrivene kao malver i uklonjene
- **Praćeni procesi** - broj trenutno pokrenutih aplikacija koje nadgleda komponenta za zaštitu identiteta
- **Ponašanja koja se prate** - broj određenih radnji koje su aktivne unutar praćenih aplikacija

Ispod možete naći vezu [Prikaži nadgledane procese i Pregled aktivnosti](#) koja će vas odvesti na korisnički interfejs komponente [Sistemske alate](#) gde možete naći detaljan pregled svih nadgledanih procesa.



Osnovna podešavanja zaštite identiteta

U donjem delu dijaloga možete urediti neke osnovne funkcije funkcionalnosti komponente:

- **Aktiviraj zaštitu identiteta** - (podrazumevano uključeno): označite radi aktivacije komponente za zaštitu identiteta i otvaranja dodatnih opcija za uređivanje.

U nekim slučajevima, komponenta **Identity Protection** može prijaviti da su neke validne datoteke sumnjive ili opasne. Budući da komponenta **Identity Protection** otkriva pretnje na osnovu njihovog ponašanja, to se obično dešava kada neki program pokuša da nadgleda ključne procese, instalira druge programe ili kada se na računar instalira novi upravljački program. Zbog toga izaberite jednu od sledećih opcija kojima se određuje ponašanje komponente **Identity Protection** u slučaju otkrivanja sumnjive radnje:

- **Uvek pitaj** - ako se aplikacija detektuje kao malver, od vas će se tražiti da li želite da je blokirate (ova opcija je podrazumevano uključena i preporučujemo vam da je ne menjate osim ako nemate dobar razlog za to)
- **Automatski stavi u karantin otkrivene pretnje** - sve aplikacije koje su otkrivene kao malver biće automatski blokirane
- **Automatski stavi u karantin poznate pretnje** - biće blokirane samo one aplikacije za koje je sa sigurnošću utvrđeno da su malver
- **Napredna podešavanja...** - kliknite na vezu da biste bili preusmereni na odgovarajući dijalog u okviru [Napredna podešavanja](#) programa **AVG Internet Security 2012**. Odatle možete detaljno urediti konfiguraciju komponente. Međutim, imajte u vidu da je podrazumevana konfiguracija svih komponenti podešena tako da **AVG Internet Security 2012** obezbeđuje optimalne performanse i maksimalnu bezbednost. Preporučuje se da zadržite podrazumevanu konfiguraciju, osim ako nemate opravdan razlog da to ne uradite!

Kontrolna dugmad

U interfejsu komponente **Identity Protection** dostupna su sledeća kontrolna dugmad:

- **Sačuvaj promene** - kliknite na ovo dugme da biste sačuvali i primenili promene koje ste napravili u ovom dijalogu
- **Otkazi** - kliknite na ovo dugme da biste se vratili u podrazumevani [glavni dijalog AVG](#) (pregled komponenti)

6.9. Daljinska administracija

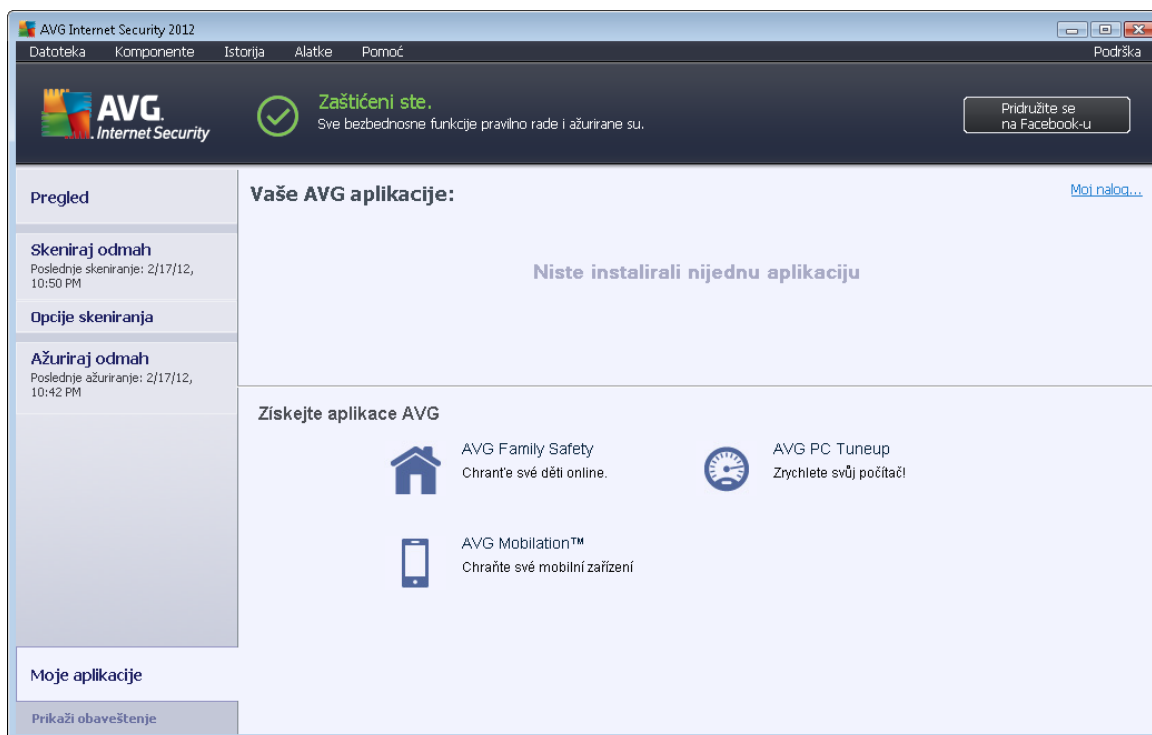
Komponenta **Daljinska administracija** prikazuje se u korisničkom interfejsu programa **AVG Internet Security 2012** samo ako ste instalirali Business Edition proizvoda (*informacije o licenci korišćenju za instalaciju potražite na kartici [Verzija](#) u dijalogu [Informacije](#) koji se može otvoriti putem stavke [Podrška](#) u sistemskom meniju*). Za detaljan opis opcija komponente i funkcija u okviru AVG sistema za daljinsku administraciju pročitajte dokumentaciju koja je posvećena isključivo toj



temi. Ova dokumentacija je dostupna za preuzimanje na AVG Web lokaciji (<http://www.avg.com/>), u odeljku **Centar za podršku / Preuzimanje / Dokumentacija**.

7. Moje aplikacije

Dijalog **Moje aplikacije** (koji je pristupačan putem dugmeta „Moje aplikacije“ direktno iz AVG glavnog dijaloga) obezbeđuje pregled AVG samostalnih aplikacija, onih koje su već instalirane na računaru ili opcionalno onih koje su spremne za instalaciju:



Ovaj dijalog je podeljen na dva odeljka:

- **Vaše AVG aplikacije** - obezbeđuje pregled svih AVG samostalnih aplikacija koje su već instalirane na računaru;
- **Preuzimanje AVG aplikacija** - nudi pregled AVG samostalnih aplikacija koje će vas možda zanimati. Ove aplikacije su spremne za instalaciju. Ponuda se dinamički menja na osnovu vaše licence, lokacije i drugih kriterijuma. Detaljne informacije o ovim aplikacijama potražite na AVG Web lokaciji (<http://www.avg.com/>).

Sledi kratak pregled svih dostupnih aplikacija i kratko objašnjenje njihovih funkcionalnosti:

7.1. AVG Family Safety

AVG Family Safety štiti vašu decu od neprikladnih Web lokacija, medijskih sadržaja i pretraga na mreži i šalje vam izveštaje o njihovoj aktivnosti na mreži. **AVG Family Safety** koristi tehnologiju poteza tasterom za nadgledanje aktivnosti deteta u sobama za časkanje i na lokacijama za društveno umrežavanje. Ako primeti reči, fraze ili jezik za koje je poznato da se koriste za zlostavljanje dece na mreži, on će vas odmah obavestiti putem SMS-a ili e-pošte. Aplikacija vam omogućava da podesite odgovarajući nivo zaštite za svako dete i da zasebno nadgledate svako dete putem jedinstvenih podataka za prijavljivanje.



Za detaljne informacije posetite namensku AVG Web stranicu, gde takođe možete odmah da preuzmete komponentu. Da biste to uradili, možete da koristite vezu „AVG Family Safety“ u okviru dijaloga [Moje aplikacije](#).

7.2. AVG LiveKive

AVG LiveKive je namenjen za pravljenje rezervnih kopija na mreži na bezbednim serverima. **AVG LiveKive** automatski pravi rezervne kopije svih vaših datoteka, fotografija i muzike na jednoj bezbednoj lokaciji i omogućava vam da ih podelite sa porodicom i prijateljima i da im pristupite sa bilo kog uređaja koji ima pristup Internetu, kao što su iPhone i Android uređaji. **AVG LiveKive** funkcije uključuju:

- Sigurnosnu meru u slučaju kvara računara i/ili čvrstog diska
- Pristup podacima sa bilo kog uređaja koji je povezan sa Internetom
- Jednostavnu organizaciju
- Podatke možete da delite sa svim korisnicima kojima date odobrenje

Za detaljne informacije posetite namensku AVG Web stranicu, gde takođe možete odmah da preuzmete komponentu. Da biste to uradili, možete da koristite vezu „AVG LiveKive“ u okviru dijaloga [Moje aplikacije](#).

7.3. AVG Mobilation

AVG Mobilation štiti vaš mobilni telefon od virusa i malvera i pruža vam mogućnost da daljinski pratite svoj pametni telefon ako se odvojite od njega. **AVG Mobilation** funkcije uključuju:

- *Skener datoteka* omogućava bezbednosno skeniranje datoteka na različitim lokacijama za skladištenje;
- *Zaustavljanje zadataka* vam omogućava da zaustavite aplikaciju u slučaju da se uređaj uspori ili zakoči;
- *Zaključavanje aplikacija* vam omogućava da zaključate i od neispravne upotrebe zaštitite jednu ili više aplikacija pomoću lozinke;
- *Tuneup* prikuplja različite parametre sistema (*merač baterije, upotreba skladišta, veličina i lokacija instalacije aplikacija itd.*) u jednom centralizovanom prikazu da biste lakše kontrolisali performanse sistema;
- *Rezervna kopija aplikacija* vam omogućava da napravite rezervnu kopiju aplikacija na SD kartici i da ih kasnije vratite u prethodno stanje;
- *Funkcija Bezvredna pošta i prevare* vam omogućava da označite SMS poruke kao bezvrednu poštu i da prijavite Web lokacije kao prevaru;
- *Brisanje ličnih podataka* daljinski u slučaju krađe telefona;
- *Bezbedno surfovanje Webom* nudi nadgledanje posećenih Web stranica u realnom vremenu.



Za detaljne informacije posetite namensku AVG Web stranicu, gde takođe možete odmah da preuzmete komponentu. Da biste to uradili, možete da koristite vezu AVG Mobilation u okviru dijaloga [Moje aplikacije](#).

7.4. AVG PC Tuneup

AVG PC Tuneup aplikacija je napredna alatka za detaljnu analizu i ispravljanje sistema pomoću koje se utvrđuje na koji se način brzina i celokupna performansa računara mogu poboljšati. **AVG PC Tuneup** funkcije uključuju:

- Čistač diska - uklanja neželjene datoteke koje usporavaju računar.
- Defragmentacija diska - defragmentuje disk jedinice i optimizuje postavljanje sistemskih datoteka.
- Čistač registratora - popravlja greške registratora da bi se povećala stabilnost računara.
- Defragmentacija registratora - sažima registrator da bi se uklonile praznine koje zauzimaju memoriju.
- Doktor za disk - pronalazi oštećene sektore, izgubljene klastere i greške direktorijuma i ispravlja ih.
- Optimizator Interneta - prilagođava univerzalna podešavanja specifičnoj Internet vezi.
- Brisač praćenja - uklanja istoriju upotrebe računara i Interneta.
- Brisač diska - briše slobodan prostor na diskovima da bi se sprečio oporavak osetljivih podataka.
- Brisač datoteka - briše izabrane datoteke bez mogućnosti oporavka na disku ili USB fleš disku.
- Oporavak datoteka - oporavlja slučajno izbrisane datoteke sa diskova, USB fleš diskova ili kamera.
- Pronalaženje dupliranih datoteka - pomaže u pronalaženju i uklanjanju dupliranih datoteka koje troše prostor na disku.
- Upravljač uslugama - onemogućava nepotrebne usluge koje usporavaju računar.
- Upravljač pokretanjem - omogućava korisniku da upravlja programima koji se automatski pokreću pri pokretanju sistema Windows.
- Upravljač deinstaliranjem - u potpunosti deinstalira softverske programe koji vam više nisu potrebni.

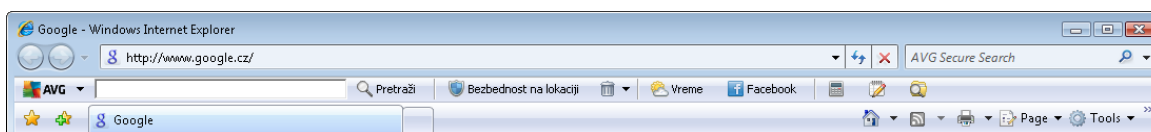


- Upravljač podešavanjima - omogućava korisniku da podesi stotine skrivenih Windows podešavanja.
- Upravljač zadacima - navodi sve pokrenute procese, usluge i zaključane datoteke.
- Istraživač diska - prikazuje koje datoteke zauzimaju najviše prostora na računaru.
- Informacije o sistemu - obezbeđuje detaljne informacije o instaliranom hardveru i softveru.

Za detaljne informacije posetite namensku AVG Web stranicu, gde takođe možete odmah da preuzmete komponentu. Da biste to uradili, možete da koristite vezu „AVG PC Tuneup“ u okviru dijaloga [Moje aplikacije](#).

8. AVG Security Toolbar

AVG Security Toolbar je alatka koja blisko sarađuje sa [LinkScanner](#) komponentom i obezbeđuje maksimalnu bezbednost tokom pregledanja Interneta. U okviru programa **AVG Internet Security 2012**, instalacija **AVG bezbednosne trake sa alatkama** je opcionalna; tokom [procesa instalacije](#) od vas se traži da odlučite da li treba instalirati komponentu. **AVG Security Toolbar** je dostupna direktno u Internet pregledaču. Trenutno podržani Internet pregledači su Internet Explorer (*verzija 6.0 i novije verzije*) i/ili Mozilla Firefox (*verzija 3.0 i novije verzije*). Nije podržan nijedan drugi pregledač (*ako koristite neki alternativni Internet pregledač, npr. Avant Browser, može doći do neočekivanog ponašanja*).



AVG Security Toolbar sastoji se od sledećih stavki:

- **AVG logotip** sa padajućim menijem:
 - **Koristi AVG bezbednu pretragu** - omogućava vam da direktno pretražujete sa **AVG bezbednosne trake sa alatkama** pomoću mašine **AVG bezbedne pretrage**. Sve rezultate pretrage neprekidno proverava usluga [Štit za pretraživanje](#) i možete se osećati potpuno bezbedno na mreži.
 - **Trenutni nivo pretnje** – otvara Web stranicu laboratorije virusa sa grafičkim prikazom trenutnog nivoa pretnje na Webu.
 - **AVG laboratorije pretnji** - otvara određenu Web lokaciju **AVG laboratorije pretnji** (na adresi <http://www.avgthreatlabs.com>) gde možete pronaći informacije o bezbednosti različitih Web lokacija i trenutnom nivou pretnje na mreži.
 - **Pomoć na traci sa alatkama** - otvara pomoć na mreži koja pokriva sve funkcionalnosti **AVG bezbednosne trake sa alatkama**.
 - **Dostavi povratne informacije o proizvodu** - otvara Web stranicu sa obrascem koji možete popuniti da biste nam saopštili svoje mišljenje o **AVG bezbednosnoj traci sa alatkama**.
 - **Osnovni podaci o...** - otvara novi prozor sa informacijama o trenutno instaliranoj verziji **AVG bezbednosne trake sa alatkama**.
- **Polje za pretragu** - pretražite Internet pomoću **AVG bezbednosne trake sa alatkama** da biste bili apsolutno sigurni i mimi, jer su prikazani rezultati pretrage u potpunosti bezbedni. Unesite ključnu reč ili frazu u polje za pretragu i kliknite na dugme **Pretraži** (ili pritisnite taster Enter). Sve rezultate pretrage neprekidno proverava usluga [štita za pretraživanje](#) (u okviru komponente [LinkScanner](#)).
- **Bezbednost lokacije** - Ovo dugme otvara novi dijalog koji potvrđuje informacije na trenutnom nivou pretnje (**Trenutno bezbedno**) stranice koju upravo posećujete. Ovaj kratak pregled može se razviti i prikazati sa svim detaljima svih bezbednosnih aktivnosti u vezi sa stranicom u prozoru pregledača (**Prikaži kompletan izveštaj**):



- **Izbriši** - Dugme „korpa za otpatke“ nudi padajući meni iz kojeg možete izabrati da li želite da izbrisete informacije o pregledanju, preuzimanjima, obrascima na mreži ili da odjednom izbrisete celu istoriju pretraživanja.
- **Vreme** - ovo dugme otvara novi dijalog sa informacijama o trenutnim vremenskim prilikama u vašem mestu, kao i sa vremenskom prognozom za naredna dva dana. Ove informacije se redovno ažuriraju na svakih 3-6 časova. U dijalogu možete ručno promeniti željeno mesto i odlučiti da li želite da se temperatura prikazuje u stepenima Celzijusa ili Farenhajta.



- **Facebook** - ovo dugme vam dozvoljava da se direktno povežete sa društvenom mrežom [Facebook](#) unutar **AVG bezbednosne trake sa alatkama**.
- Dugmad prečice za brzi pristup ovim aplikacijama: **Kalkulator**, **Beležnica**, **Windows Explorer**.



9. AVG Do Not Track

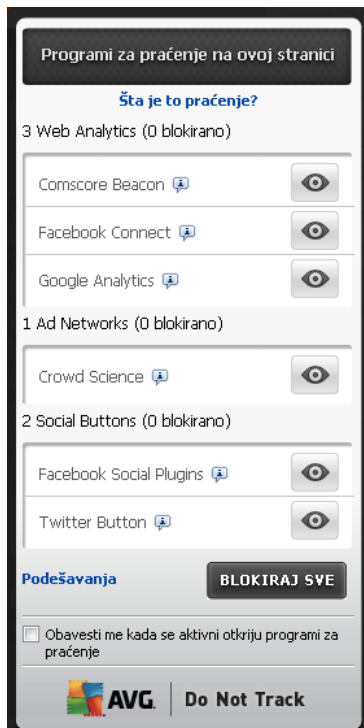
AVG Do Not Track vam pomaže da identifikujete Web lokacije koje prikupljaju podatke o vašim aktivnostima na mreži. Ikona u pregledaču prikazuje Web lokacije ili oglašivače koji prikupljaju podatke o vašoj aktivnosti i pruža vam mogućnost da ih dozvolite ili zabranite.

- **AVG Do Not Track** vam pruža dodatne informacije o smernicama za privatnost svake odgovarajuće usluge, kao i direktnu vezu za odbijanje usluge ako je to dostupno.
- Pored toga, **AVG Do Not Track** podržava [W3C DNT protokol](#) za automatsko obaveštavanje lokacija da ne želite da vas prate. Ovo obaveštenje je podrazumevano omogućeno, ali u bilo kom trenutku to možete da promenite.
- **AVG Do Not Track** se obezbeđuje pod ovim [odredbama i uslovima](#).
- **AVG Do Not Track** je podrazumevano omogućen, ali možete da ga onemogućite u bilo kom trenutku. Uputstva možete pronaći u članku sa najčešćim pitanjima [Onemogućavanje funkcije AVG Do Not Track](#).
- Za više informacija o funkciji **AVG Do Not Track** posetite našu [Web lokaciju](#).

AVG Do Not Track funkcionalnost trenutno je podržana u pregledačima Mozilla Firefox, Chrome i Internet Explorer. (U programu Internet Explorer ikona funkcije AVG Do Not Track nalazi se na desnoj strani komandne trake. Ukoliko imate problema sa pronalaženjem ikone funkcije AVG Do Not Track u podrazumevanim postavkama pregledača, uverite se da ste aktivirali komandnu traku. Ako i dalje ne vidite ikonu, prevucite komandnu traku nalevo da biste otkrili sve ikone i svu dugmad dostupne na ovoj traci sa alatkama.)

9.1. AVG Do Not Track interfejs

Dok ste na mreži, **AVG Do Not Track** vas upozorava čim otkrije bilo koju vrstu prikupljanja podataka. Videćete sledeći dijalog:



Sve otkrivene usluge za prikupljanje podataka navedene su po imenu u pregledu **Programi za praćenje na ovoj stranici**. Postoje tri tipa aktivnosti prikupljanja podataka koje **AVG Do Not Track** prepoznaje:

- **Web analiza** (*podrazumevano je dozvoljena*): usluge koje se koriste za poboljšanje performansi i doživljaja odgovarajuće Web lokacije. U ovoj kategoriji možete da pronađete usluge kao što su Google Analytics, Omniture ili Yahoo Analytics. Preporučujemo da ne blokirate usluge Web analize jer Web lokacije možda neće funkcionisati na željeni način.
- **Dugmad društvenih mreža** (*podrazumevano su dozvoljena*): elementi dizajnirani za poboljšanje doživljaja društvenog umrežavanja. Dugmad društvenih mreža lokacijama koje posećujete obezbeđuju društvene mreže. Mogu da prikupljaju podatke o vašoj aktivnosti na mreži dok ste prijavljeni. Primeri dugmadi društvenih mreža obuhvataju: dodatne komponente društvene mreže Facebook, Twitter dugme, Google +1.
- **Mreže reklama** (*neke su podrazumevano blokirane*): usluge koje prikupljaju ili dele podatke o vašoj aktivnosti na mreži na više lokacija, direktno ili indirektno, kako bi vam ponudile personalizovane reklame za razliku od reklama na osnovu sadržaja. Ovo se određuje na osnovu smernica za privatnost svake mreže reklama koje su dostupne na njihovim Web lokacijama. Neke mreže reklama podrazumevano su blokirane.

Napomena: U zavisnosti od usluga koje koristite u pozadini Web lokacije, neki od tri opisana

odeljka možda se neće pojaviti u dijalogu „AVG Do Not Track“.

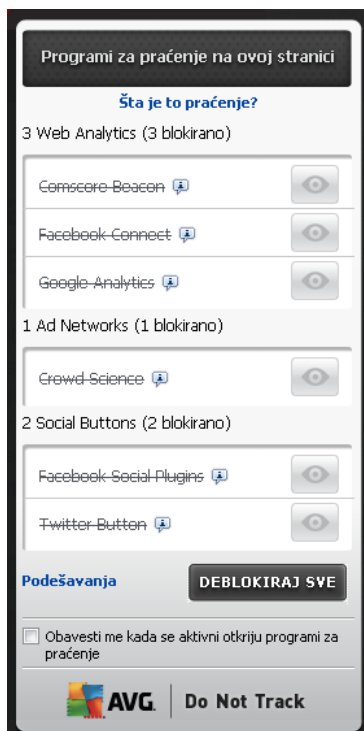
Dijalog sadrži dve hiperveze:

- **Šta je to praćenje?** – kliknite na ovu vezu u gornjem odeljku dijaloga da biste bili preusmereni na namensku Web stranicu koja pruža detaljno objašnjenje o principima praćenja i opis određenih tipova praćenja.
- **Postavke** – kliknite na ovu vezu u donjem odeljku dijaloga da biste bili preusmereni na namensku Web stranicu na kojoj možete da podesite određenu konfiguraciju raznih **AVG Do Not Track** parametara (detaljne informacije potražite u poglavlju [AVG Do Not Track postavke](#))

9.2. Informacije o procesima praćenja

Lista otkrivenih usluga za prikupljanje podataka pruža samo ime određene usluge. Da biste doneli utemeljenu odluku o tome da li odgovarajuću uslugu treba da blokirate ili dozvolite, možda će biti potrebno da saznate nešto više o tome. Prevucite mišem preko odgovarajuće stavke liste. Pojavljuje se oblačić sa informacijama koji pruža detaljne podatke o usluzi. Saznaćete da li usluga prikuplja vaše lične podatke ili druge dostupne podatke, da li se podaci dele sa trećim licima i da li se prikupljeni podaci arhiviraju radi buduće upotrebe.

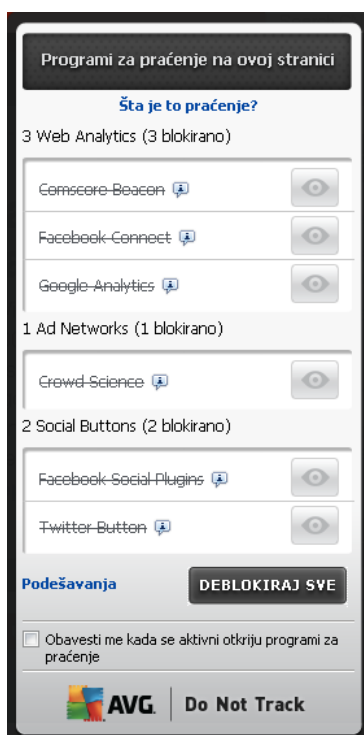
U donjem odeljku oblačića sa informacijama možete da vidite hipervezu **Smernice za privatnost** koja vas preusmerava na Web lokaciju namenjenu za smernice za privatnost odgovarajuće otkrivene usluge.



9.3. Blokiranje procesa praćenja

Pomoću lista svih mreža reklama/dugmadi društvenih mreža/Web analize sada imate opciju da kontrolirate usluge koje treba da se blokiraju. Na raspolaganju su vam dva načina:

- **Blokiraj sve** – kliknite na ovo dugme koje se nalazi u donjem odeljku dijaloga da biste izjavili da ne želite nikakvu aktivnost prikupljanja podataka. *(Međutim, imajte na umu da ova radnja može da naruši funkcionalnost na odgovarajućoj Web stranici na kojoj radi usluga!)*
-  – ako ne želite da odjednom blokirate sve otkrivene usluge, možete navesti da li usluga pojedinačno treba da se dozvoli ili blokira. Nekim od otkrivenih sistema možete i da dozvolite pokretanje (*npr. Web analizi*): ovi sistemi koriste prikupljene podatke radi optimizacije sopstvene Web lokacije i na taj način poboljšavaju zajedničko Internet okruženje za sve korisnike. Međutim, u isto vreme možete blokirati aktivnosti prikupljanja podataka svih procesa klasifikovanih kao mreže reklama. Jednostavno kliknite na ikonu  pored odgovarajuće usluge da biste blokirali prikupljanje podataka (*ime procesa će se pojaviti kao precrtano*) ili da biste ponovo dozvolili prikupljanje podataka.



9.4. AVG Do Not Track postavke

Direktno u dijalogu **AVG Do Not Track** postoji samo jedna opcija konfiguracije: u donjem delu ćete videti polje za potvrdu **Upozori me kada se otkriju aktivni programi za praćenje**. Ova stavka je podrazumevano odbijena. Potvrdite izbor u polju za potvrdu da biste potvrdili da želite da dobijate obaveštenja svaki put kada uđete na Web stranicu koja sadrži novu uslugu za prikupljanje podataka koja još nije blokirana. Kada je izbor potvrđen, ako **AVG Do Not Track** otkrije novu uslugu za prikupljanje podataka na stranici koju trenutno posećujete, na ekranu se pojavljuje dijalog sa



obaveštenjem. U suprotnom, novootkrivenu uslugu ćete moći da uočite samo po **AVG Do Not Track** ikoni (*nalazi se na komandnoj traci pregledača*) koja menja boju iz zelene u žutu.

Međutim, u donjem delu dijaloga **AVG Do Not Track** možete pronaći vezu **Postavke**. Kliknite na vezu da biste bili preusmereni na namensku Web stranicu na kojoj možete navesti detaljne **opcije funkcije AVG Do Not Track**:

AVG Do Not Track opcije

Obavesti me

Prikaži obaveštenje za sekundi

Položaj obaveštenja

- ☐ Obavesti me kada se otkriju programi za praćenje
- ☒ Obavesti Veb lokacije da ne želim se moje aktivnosti prate (pomoću Do Not Track <http://zaglavja>)

Blokiraj sledeće

☒ 24/7 Real Media	Ad Networks
☒ 33Across	Ad Networks
☒ [x+1]	Ad Networks
☒ Accelerator Media	Ad Networks
☒ AddtoAny	Ad Networks
☒ Addition	Ad Networks
☒ AdReady	Ad Networks
☒ Aggregate Knowledge	Ad Networks
☒ Baynote Observer	Ad Networks
☒ Bizo	Ad Networks

- **Položaj obaveštenja** (*podrazumevano gore desno*) – otvorite padajući meni da biste naveli položaj na kojem želite da se dijalog **AVG Do Not Track** pojavi na monitoru.
- **Prikaz obaveštenja za** (*podrazumevano 10*) - u ovom polju treba da odlučite koliko dugo (*u sekundama*) želite da vidite **AVG Do Not Track** obaveštenje na ekranu. Možete da navedete broj u opsegu od 0 do 60 sekundi (*za vrednost 0, obaveštenje se neće ni pojaviti na ekranu*).
- **Upozori me kada se otkriju aktivni programi za praćenje** (*podrazumevano isključeno*) – potvrdite izbor u polju za potvrdu da biste potvrdili da želite da dobijate obaveštenja svaki put kada uđete na Web stranicu koja sadrži novu uslugu za prikupljanje podataka koja još nije blokirana. Kada je izbor potvrđen, ako **AVG Do Not Track** otkrije novu uslugu za prikupljanje podataka na stranici koju trenutno posećujete, na ekranu se pojavljuje dijalog



sa obaveštenjem. U suprotnom, novootkrivenu uslugu ćete moći da uočite samo po **AVG Do Not Track** ikoni (*nalazi se na komandnoj traci pregledača*) koja menja boju iz zelene u žutu.

- **Obavesti Web lokacije da ne želim da me prate** (*podrazumevano uključeno*) – ostavite ovu opciju označenom da biste potvrdili da želite da **AVG Do Not Track** obavesti otkrivenu uslugu za prikupljanje podataka da ne želite da vas prati.
- **Blokiraj sledeće** (*sve navedene usluge za prikupljanje podataka podrazumevano su dozvoljene*) – u ovom odeljku možete videti okvir sa listom poznatih usluga za prikupljanje podataka koje se mogu klasifikovati kao mreže reklama. **AVG Do Not Track** podrazumevano automatski blokira neke mreže reklama, a na vama je da li će se i ostale blokirati ili će ostati dozvoljene. Da biste to uradili, ispod liste kliknite na dugme **Blokiraj sve**.

Kontrolna dugmad dostupna u okviru stranice **AVG Do Not Track opcije** sledeća su:

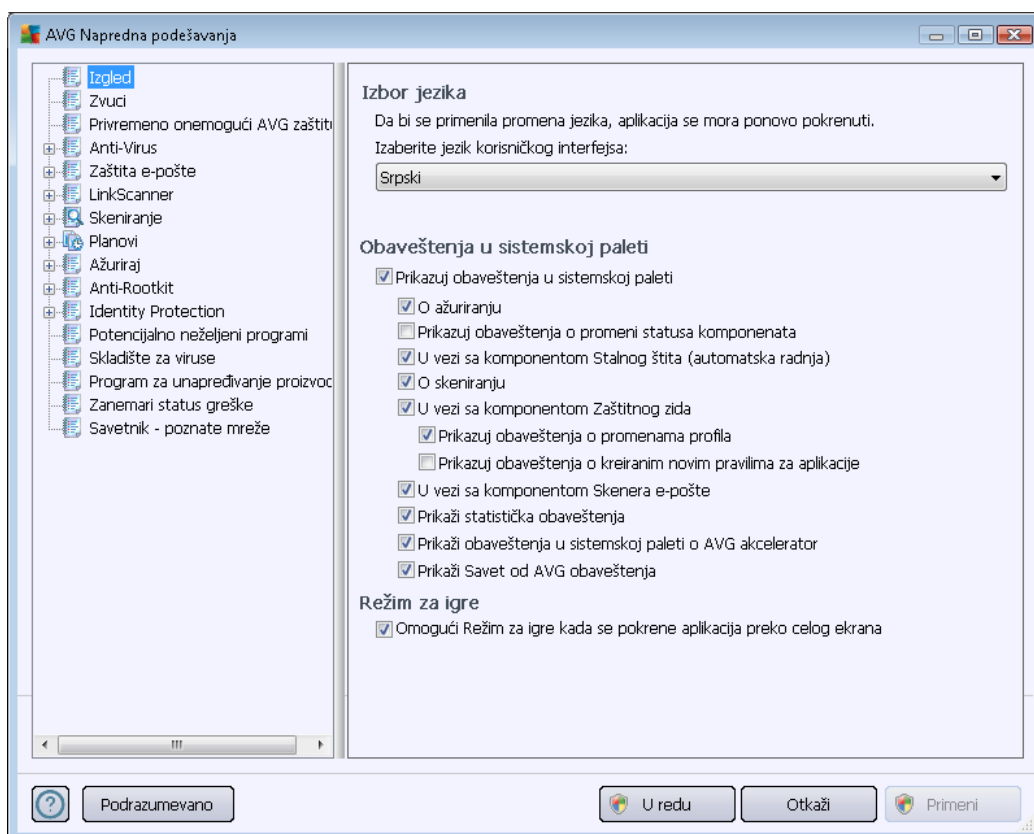
- **Blokiraj sve** - kliknite da biste odjednom blokirali sve usluge navedene u gorenavedenom polju klasifikovane kao mreže reklama;
- **Dozvoli sve** - kliknite da biste odjednom deblokirali sve prethodno blokirane usluge navedene u gorenavedenom polju i klasifikovane kao mreže reklama;
- **Podrazumevano** - kliknite da biste odbacili sve prilagođene postavke i vratili se na podrazumevanu konfiguraciju;
- **Sačuvaj** - kliknite da biste primenili i sačuvali sve navedene konfiguracije;
- **Otkazi** - kliknite da biste otkazali sve prethodno navedene postavke.

10. AVG napredna podešavanja

Dijalog za napredna podešavanja programa **AVG Internet Security 2012** se otvara u novom prozoru **Napredna podešavanja AVG programa**. Ovaj prozor je podeljen u dva odeljka: sa leve strane se nalazi stablo za navigaciju po opcijama za konfigurisanje programa. Izaberite komponentu čiju konfiguraciju želite da izmenite (*ili nekog njenog dela*), kako bi se sa desne strane otvorio dijalog za uređivanje.

10.1. Izgled

Prva stavka navigacionog stabla, **Izgled**, odnosi se na opšta podešavanja **AVG Internet Security 2012** [korisničkog interfejsa](#) i sadrži nekoliko osnovnih opcija ponašanja aplikacije:

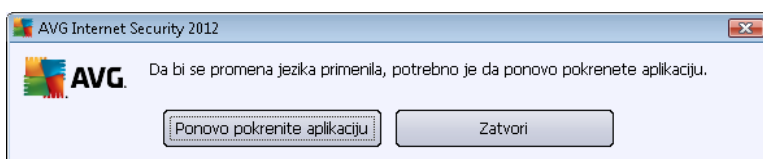


Izbor jezika

U odeljku **Izbor jezika** iz padajućeg menija možete izabrati željeni jezik. Izabrani jezik će zatim biti korišćen za ceo **AVG Internet Security 2012** [korisnički interfejs](#). Padajući meni nudi samo one jezike koje ste prethodno izabrali da budu instalirani tokom [procesa instalacije](#) (*videti poglavlje [Prilagođene opcije](#)*) plus engleski (*engleski je uvek podrazumevano automatski instaliran*). Da biste završili sa prebacivanjem **AVG Internet Security 2012** na drugi jezik, morate ponovo pokrenuti aplikaciju. Pratite sledeće korake:

- Izaberite željeni jezik aplikacije u padajućem meniju

- Potvrdite svoj izbor, tako što ćete kliknuti na dugme **Primeni** (donji desni ugao dijaloga)
- Kliknite na dugme **U redu** da biste potvrdili
- Iskočiće novi dijalog koji vas obaveštava da ukoliko želite da promenite jezik aplikacije, morate ponovo pokrenuti **AVG Internet Security 2012**
- Kliknite na dugme **Ponovo pokreni aplikaciju odmah** da biste prihvatili ponovno pokretanje programa i sačekajte trenutak da promena jezika stupi na snagu:



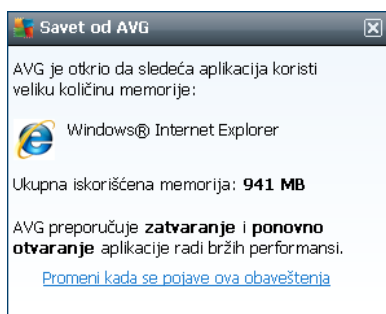
Obaveštenja u sistemskoj paleti

U ovom odeljku možete sprečiti prikazivanje obaveštenja na sistemskoj paleti o statusu aplikacije **AVG Internet Security 2012**. Prikaz sistemskih obaveštenja podrazumevano je dozvoljen. Preporučuje se da zadržite ovu konfiguraciju! Sistemski obaveštenja informišu, na primer, o pokretanju procesa skeniranja, ažuriranja ili o promeni statusa **AVG Internet Security 2012** komponente. U svakom slučaju treba da obratite pažnju na ove objave!

Međutim, ako iz nekog razloga odlučite da ne želite da se prikazuju ova obaveštenja ili biste želeli da se prikazuju samo određena obaveštenja (*vezana za određenu komponentu programa AVG Internet Security 2012*), onda možete definisati i navesti željene opcije, tako što ćete označiti/opozvati izbor sledećih opcija:

- **Prikazuj obaveštenja u sistemskoj paleti** (podrazumevano uključeno) - sva obaveštenja se podrazumevano prikazuju. Opozovite izbor ove stavke da biste potpuno isključili sva sistemski obaveštenja. Ako je ova stavka uključena, možete dodatno definisati koja će se obaveštenja prikazivati:
 - **Prikazuj obaveštenja u sistemskoj paleti o ažuriranju programa** (podrazumevano uključeno) - odlučite da li da se prikazuju informacije o **AVG Internet Security 2012** pokretanju, toku i završetku ažuriranja programa.
 - **Prikazuj obaveštenja o promeni statusa komponentata** (podrazumevano isključeno) - odlučite da li da se prikazuju informacije o aktivnosti/neaktivnosti komponente ili o potencijalnim problemima u okviru komponente. Prilikom prijavljivanja stanja greške komponente, ova opcija je jednaka informativnoj funkciji [ikone sistemske palete](#) koja prijavljuje probleme u svakoj **AVG Internet Security 2012** komponenti.
 - **Prikazuj obaveštenja vezana za Stalni štiti u sistemskoj paleti (automatska radnja)** (podrazumevano uključeno) - odlučite da li da se informacije u vezi sa procesima čuvanja, kopiranja i otvaranja prikazuju ili ne (*ova konfiguracija samo pokazuje da li je opcija Stalnog štita Automatsko lečenje uključena*).

- **Prikazuj obaveštenja u sistemskoj paleti o [skeniranju](#)** (podrazumevano uključeno) - odlučite da li da se prikazuju informacije pri automatskom pokretanju planiranog skeniranja, njegov tok i rezultati.
- **Prikazuj obaveštenja u sistemskoj paleti u vezi sa [zaštitnim zidom](#)** (podrazumevano uključeno) - odlučite da li da se prikazuju informacije u vezi sa statusom i procesima [zaštitnog zida](#), npr. upozorenja o aktiviranju/deaktiviranju komponente, mogućem blokiranju saobraćaja itd . Ova stavka obezbeđuje još dve specifične opcije za izbor (*detaljno objašnjenje o njima potražite u poglavlju [Zaštitni zid](#) u ovom dokumentu*):
 - **Prikazuj obaveštenja o promenama profila** (podrazumevano uključeno) - obaveštava vas o automatskim promenama profila [zaštitnog zida](#).
 - **Prikazuj obaveštenja o pravilima kreiranim za nove aplikacije** (podrazumevano isključeno) - obaveštava vas o automatskom kreiranju pravila [zaštitnog zida](#) za nove aplikacije na osnovu liste bezbednih aplikacija.
- **Prikazuj obaveštenja u sistemskoj paleti u vezi sa komponentom [Skener e-pošte](#)** (podrazumevano uključeno) - odlučite da li da se prikazuju informacije o skeniranju svih dolaznih i odlaznih e-poruka.
- **Prikazuj statistička obaveštenja** (podrazumevano uključeno) – ne opozivajte izbor ove opcije ako želite da se u sistemskoj paleti redovno prikazuju statistička obaveštenja.
- **Prikazuj obaveštenja u sistemskoj paleti o [AVG akceleratoru](#)** (podrazumevano uključeno) - odlučite da li da se prikazuju informacije pri izvršavanju aktivnosti **AVG akceleratora**. Usluga **AVG akceleratora** koja omogućava jednostavniju reprodukciju video zapisa na mreži i olakšava dodatna preuzimanja.
- **Prikazuj obaveštenja o performansama usluge [AVG Advice](#)** (podrazumevano uključeno) - **AVG Advice** prati performanse podržanih Internet pregledača (*Internet Explorer, Chrome, Firefox, Opera i Safari*) i obavestiće vas ako pregledač koristi više od preporučene količine memorije. U takvoj situaciji performanse računara mogu biti znatno smanjene i preporučuje se da ponovo pokrenete Internet pregledač da biste ubrzali procese. Ostavite opciju **Prikazuj obaveštenja o performansama usluge [AVG Advice](#)** uključenu da biste bili obavešteni.



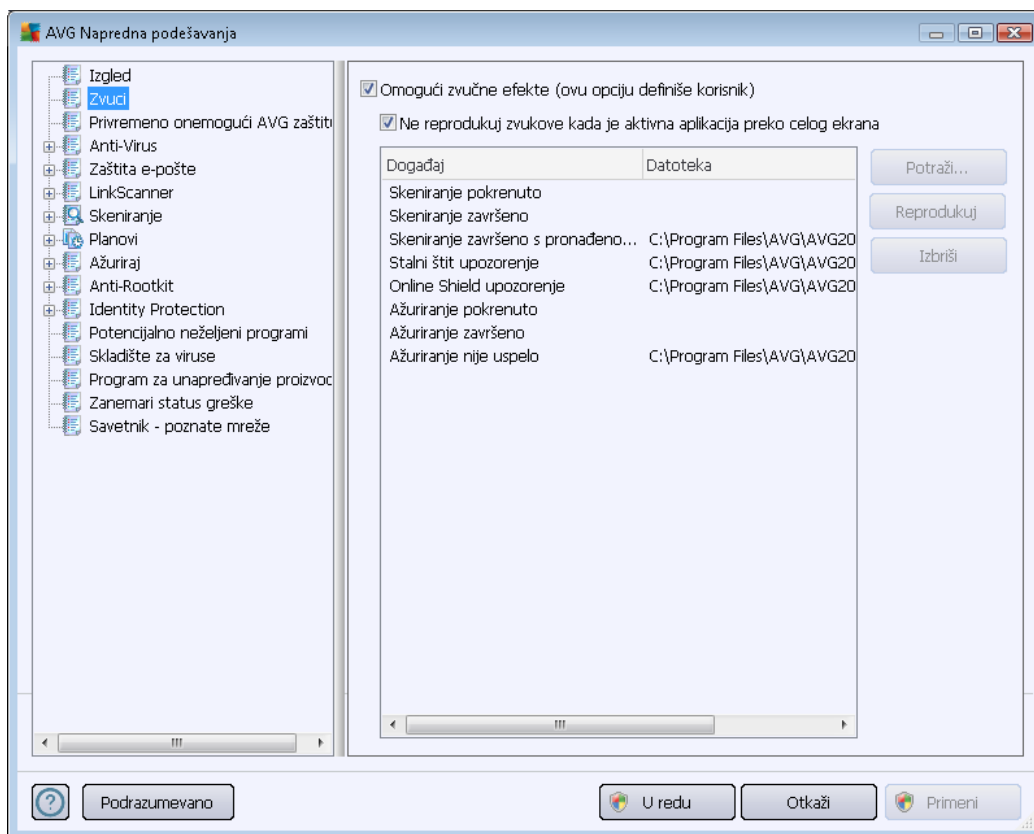


Režim za igre

Ova AVG funkcija je namenjena aplikacijama koje se prikazuju preko celog ekrana, gde su prikazani mogući balončići sa AVG informacijama (*npr. kada pokrenuto planirano skeniranje*) smeta (, *oni mogu da umanje aplikaciju ili da naruše njen grafički prikaz*). Da biste izbegli ovakvu situaciju, nemojte opozivati izbor u polju za potvrdu **Omoгуći režim za igre kada se prikazuje sadržaj preko celog ekrana** (podrazumevana postavka).

10.2. Zvuci

U okviru dijaloga **Zvuci** možete navesti da li želite da primате informacije o određenim **AVG Internet Security 2012** radnjama putem zvučnog obaveštenja:



Podešavanja su važeća samo za trenutni korisnički nalog. To znači da svaki korisnik na računaru može da ima sopstvena podešavanja zvuka. Ako želite da dozvolite zvučno obaveštavanje, ostavite izabranu opciju **Omoгуći zvučne događaje** (opcija je podrazumevano uključena) da biste aktivirali listu svih relevantnih radnji. Pored toga, možete označiti izbor opcije **Ne reprodukuј zvukove kada je aktivna aplikacijama preko celog ekrana** da biste obustavili zvučno obaveštavanje u situacijama kada vas to može ometati (pogledajte i odeljak „Režim za igre“ u poglavlju [Napredna podešavanja/Izgled](#) u ovom dokumentu).



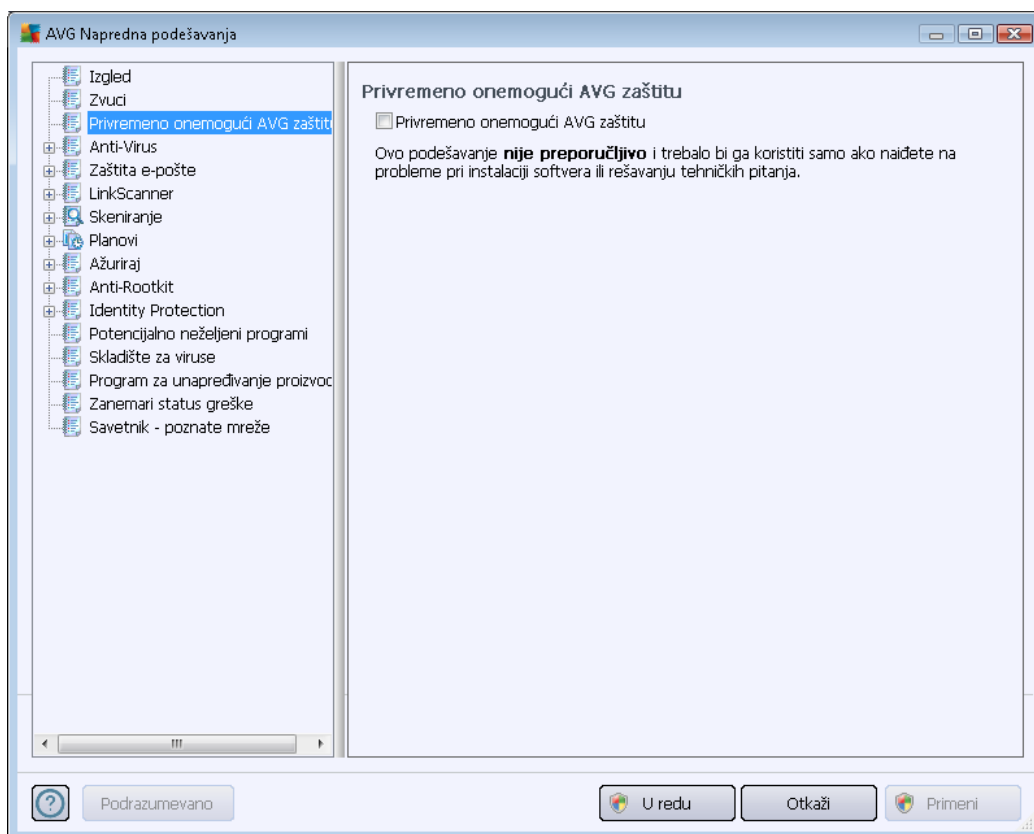
Kontrolna dugmad

- **Potraži** - kada sa liste izaberete odgovarajući događaj, koristite dugme **Potraži** da biste na disku potražili željenu zvučnu datoteku koju želite da dodelite tom događaju. (*Imajte u vidu da su trenutno podržani samo *.wav zvuci!*)
- **Reprodukuj** - da biste poslušali izabrani zvuk, označite događaj na listi i kliknite na dugme **Reprodukuj**.
- **Izbriši** - koristite dugme **Izbriši** da biste uklonili zvuk dodeljen određenom događaju.

10.3. Privremeno onemogućiti AVG zaštitu

U dijalogu **Privremeno onemogućiti AVG zaštitu** imate opciju isključivanja celokupne zaštite od strane vašeg **AVG Internet Security 2012** odjednom.

Imajte u vidu da ovu opciju ne treba da koristite, osim ako to nije apsolutno neophodno!



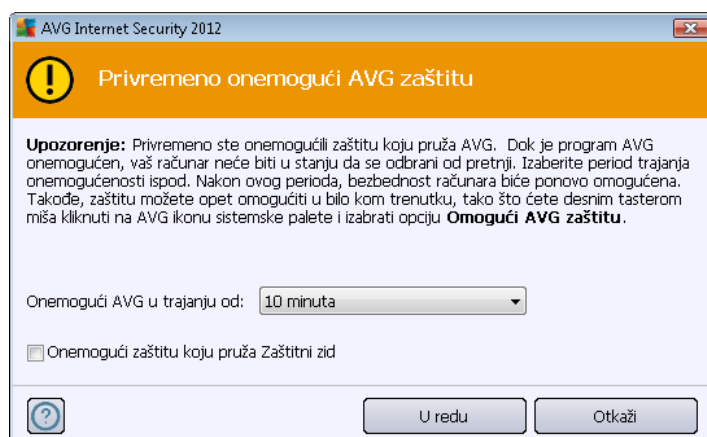
U većini slučajeva, **neće biti neophodno** da onemogućite **AVG Internet Security 2012** pre instalacije novog softvera ili upravljačkih programa, čak i ako instalator ili čarobnjak softvera predlažu da isključite pokrenute programe i aplikacije da ne bi ometale proces instalacije. Ako stvarno naidete na problem tokom instalacije, prvo pokušajte da [deaktivirate stalnu zaštitu](#) (*Omogućiti stalni štiti*). Ako se ukaže potreba da privremeno onemogućite program **AVG Internet Security**



2012, preporučujemo da ga što pre ponovo omogućite. Ukoliko ste povezani na Internet ili mrežu tokom vremena u kojem je vaš antivirusni softver onemogućen, vaš računar je podložan napadima.

Kako da se onemogući AVG zaštita

- Označite izbor u polju za potvrdu **Privremeno onemogući AVG zaštitu** i potvrdite svoj izbor klikom na dugme **Primeni**
- U novootvorenom dijalogu **Privremeno onemogući AVG zaštitu** navedite na koliko dugo želite da onemogućite **AVG Internet Security 2012**. Zaštita će podrazumevano biti isključena 10 minuta, što bi trebalo da bude dovoljno za sve uobičajene zadatke, kao što je instalacija novog softvera itd. Imajte u vidu da je početno vremensko ograničenje koje se može postaviti 15 minuta i ne možete ga zameniti svojom vrednošću iz bezbednosnih razloga. Nakon navedenog vremenskog perioda sve deaktivirane komponente ponovo će automatski biti aktivirane.

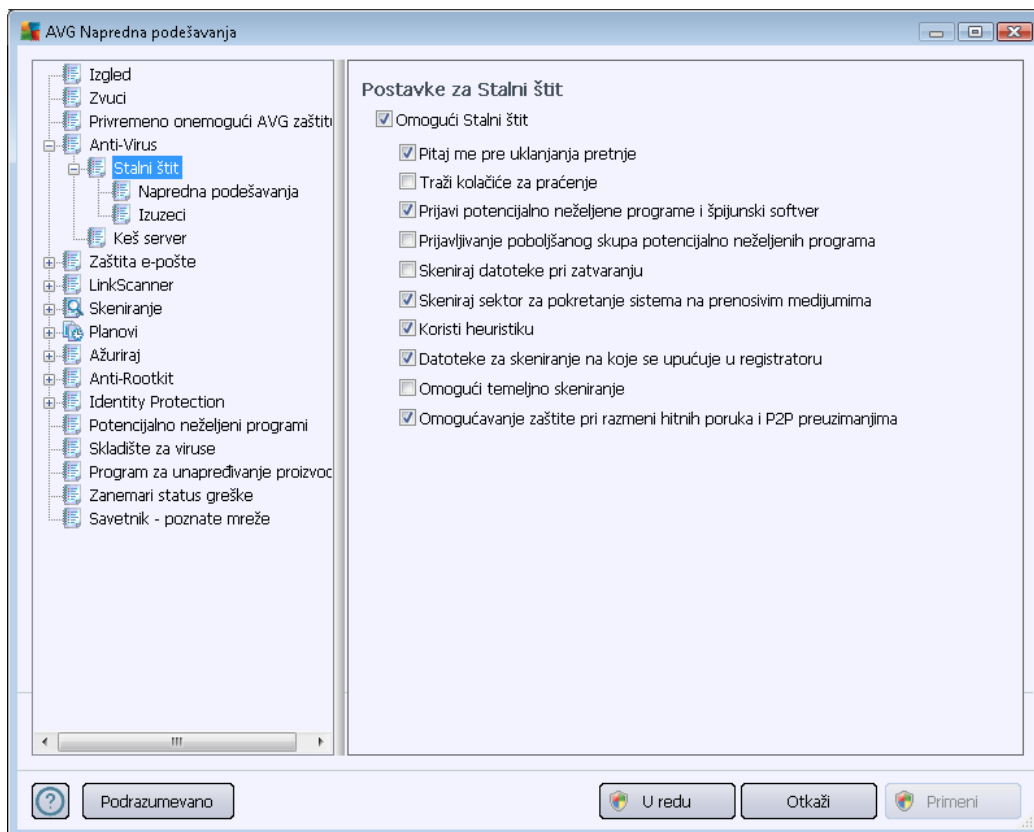


10.4. Anti-Virus

Komponenta **Anti-Virus** neprekidno štiti računar od svih poznatih vrsta virusa i špijunskog softvera (uključujući takozvani *malver u stanju spavanja* i *neaktivni malver*, tj. *malver koji je preuzet, ali još uvek nije aktiviran*).

10.4.1. Stalni štít

Stalni štít izvršava zaštitu datoteka i fascikla uživo od virusa, špijunskog softvera i drugog malvera.



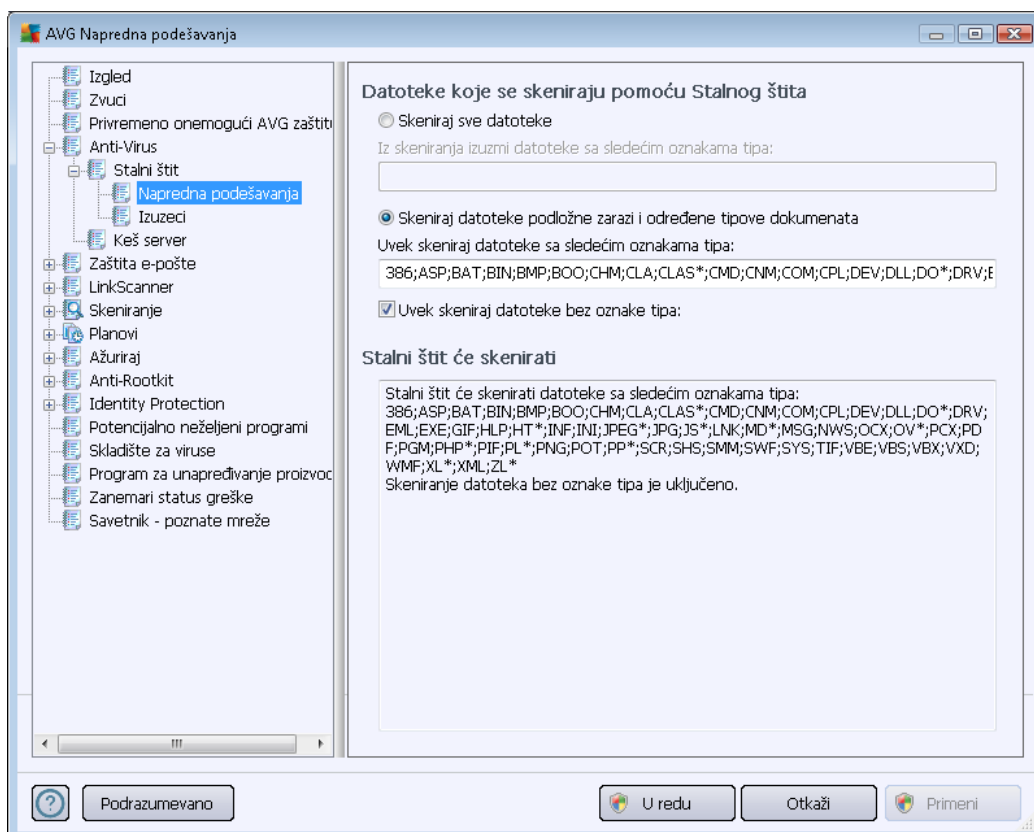
U dijalogu **Podešavanja stalnog štita** možete aktivirati ili deaktivirati stalnu zaštitu u potpunosti tako, što ćete potvrditi ili opozvati izbor stavke **Omogući stalni štít** (ova opcija je podrazumevano uključena). Pored toga, možete izabrati funkcije stalne zaštite koje treba da se aktiviraju:

- **Pitaj me pre uklanjanja pretnji** (podrazumevano uključeno) – označite ovo polje kako Stalni štít ne bi automatski vršio nikakve radnje; u suprotnom, prikazivaće dijalog koji opisuje otkrivenu pretnju, omogućavajući vam, da odlučite šta bi trebalo uraditi. Ako ne označite polje, **AVG Internet Security 2012** će automatski oporaviti zaraženu datoteku, a ako to nije moguće, objekat će biti premešten u [Skladište za viruse](#).
- **Skeniraj u potrazi za kolačićima za praćenje** (podrazumevano isključeno) - ovaj parametar definiše da tokom skeniranja treba otkrivati kolačiće. (HTTP kolačići služe za proveru identiteta, praćenje i održavanje određenih informacija o korisnicima, kao što su željene opcije za lokaciju ili sadržaj elektronskih kolica za kupovinu.)
- **Prijavi potencijalno neželjene programe i pretnje špijunskog softvera** (podrazumevano uključeno) - označite izbor da biste aktivirali mašinu za [zaštitu od špijunskog softvera](#) i skenirali u potrazi za špijunskim softverom, kao i za virusima. [Špijunski softver](#) se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.



- **Prijavi poboljšani skup potencijalno neželjenih programa** (podrazumevano isključeno) - označite da biste otkrili prošireni paket [špijunskog softvera](#): programi koji su potpuno u redu i bezbedni kada se preuzmu direktno od proizvođača, ali se mogu iskoristiti u zlonamerne svrhe kasnije. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Skeniraj datoteke pri zatvaranju** (podrazumevano isključeno) - skeniranje pri zatvaranju osigurava da AVG skenira aktivne objekte (npr. aplikacije, dokumente...) kada se otvaraju i kada se zatvaraju; ova funkcija vam pomaže da zaštitite računar od nekih tipova komplikovanih virusa.
- **Skeniraj sektor za pokretanje sistema na prenosivim medijumima** (podrazumevano uključeno)
- **Koristi heuristiku** (podrazumevano uključeno) - [heuristička analiza](#) će se koristiti za otkrivanje (dinamička emulacija uputstava skeniranog objekta u okruženju virtuelnog računara).
- **Skeniraj datoteke na koje se upućuje u registratoru** (podrazumevano uključeno) - ovaj parametar određuje da AVG skenira sve izvršne datoteke dodate u registrator za pokretanje da bi se izbeglo izvršavanje poznate zaraze pri sledećem pokretanju računara.
- **Omogući detaljno skeniranje** (podrazumevano isključeno) - u određenim situacijama (u izuzetno hitnim slučajevima) možete označiti ovu opciju da biste aktivirali najdetaljnije algoritme koji će dubinski proveriti sve moguće preteće objekte. Ipak, zapamtite da ovaj metod prilično dugo traje.
- **Omogući zaštitu razmene hitnih poruka i zaštitu P2P preuzimanja** (podrazumevano uključeno) - označite ovu stavku ako želite da potvrdite da komunikacija putem razmene hitnih poruka (npr. ICQ, MSN Messenger, ...) i P2P preuzimanja ne sadrže viruse.

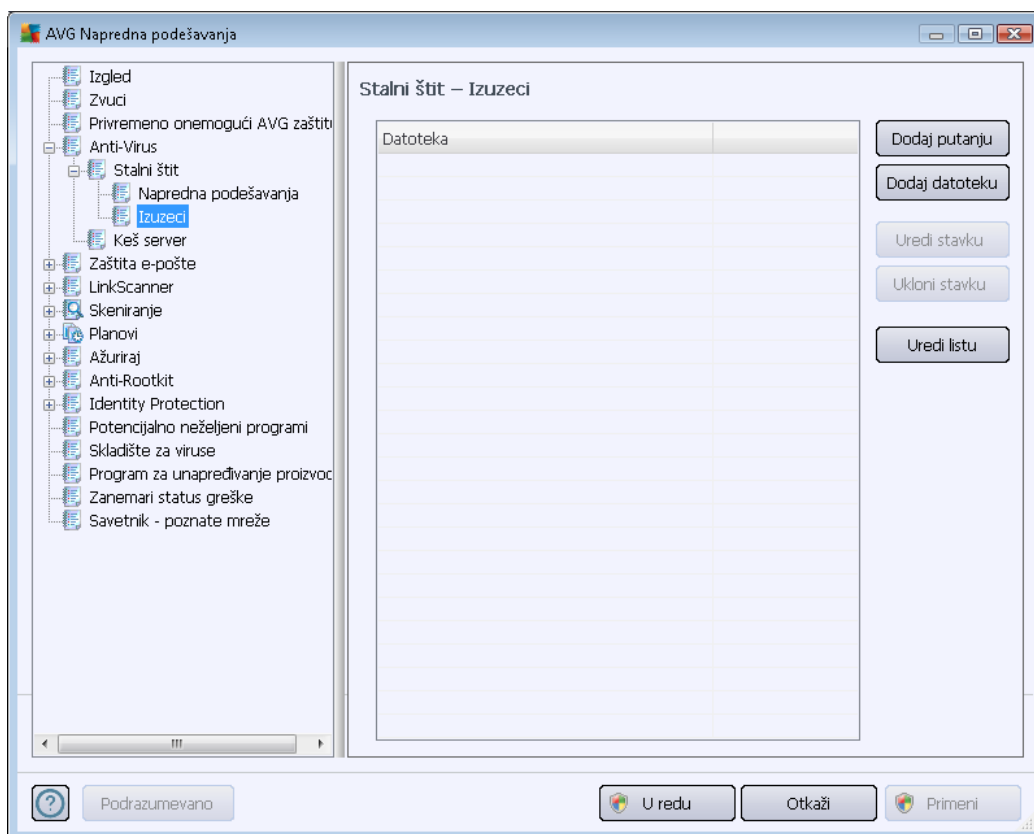
U dijalogu **Datoteke koje se skeniraju pomoću Stalnog štita** možete konfigurirati koje će se datoteke skenirati (na osnovu njihove oznake tipa):



Označite izbor u odgovarajućem polju za potvrdu da biste odlučili da li želite da **skenirate sve datoteke** ili samo da **skenirate zaražene datoteke i izabrane tipove dokumenata**. Ako ste se odlučili za drugu opciju, možete dodatno navesti listu oznaka tipa datoteka koja definiše datoteke koje treba izuzeti iz skeniranja, kao i listu oznaka tipa datoteka koje se moraju skenirati u svakom slučaju.

Označite polje **Uvek skeniraj datoteke bez oznake tipa datoteke (podrazumevano uključeno)** da biste bili sigurni da će se i datoteke bez oznake tipa datoteke i sa nepoznatim formatom skenirati komponentom Stalni štit. Preporučujemo da ova funkcija ostane uključena, pošto su datoteke bez oznake tipa sumnjive.

Odeljak ispod, nazvan **Stalni štit će skenirati** prikazuje rezime trenutnih postavki, sa detaljnim pregledom stavki koje će **Stalni štit** skenirati.



Dijalog **Stalni štiti – izuzeci** nudi mogućnost definisanja datoteka i/ili fascikli koje treba izuzeti iz skeniranja komponente **Stalni štiti**.

Preporučujemo vam da ne izuzimate nijednu stavku ako to nije neophodno!

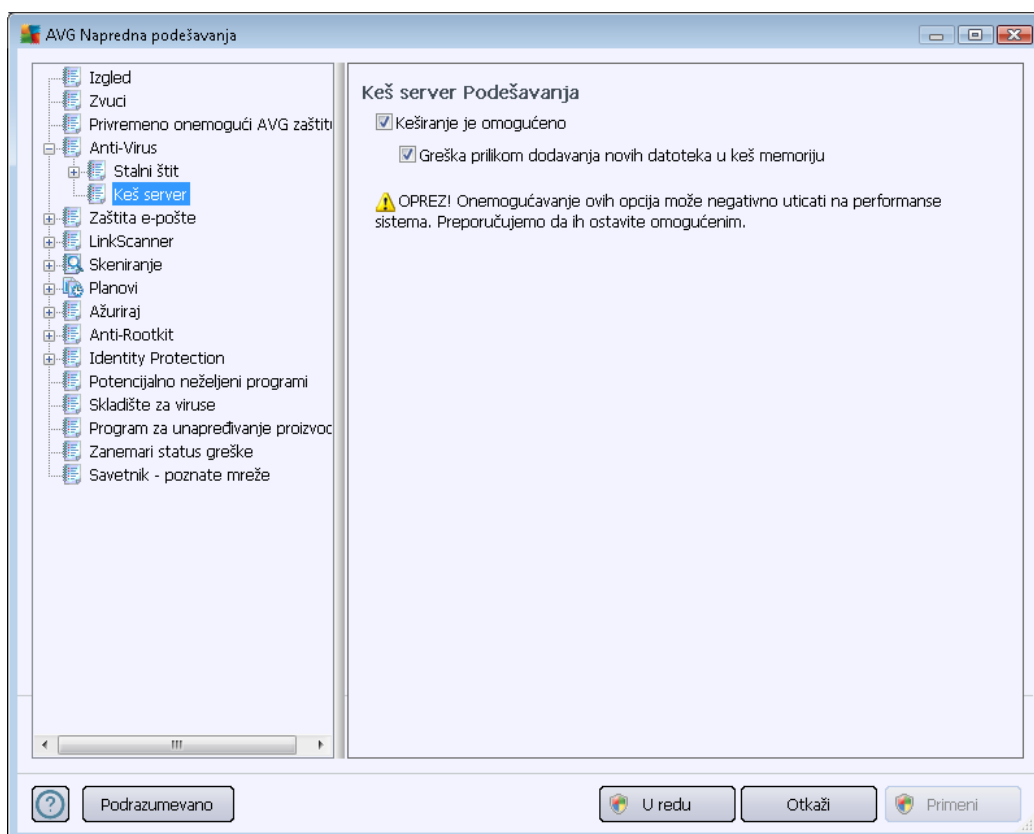
Kontrolna dugmad

Ovaj dijalog sadrži sledeću kontrolnu dugmad:

- **Dodaj putanju** – navedite direktorijum (direktorijume) koji će biti izuzeti iz skeniranja tako što ćete sa navigacionog stabla lokalnog diska izabrati jedan po jedan direktorijum
- **Dodaj datoteku** – navedite datoteke koje će biti izuzete iz skeniranja, tako što ćete sa navigacionog stabla lokalnog diska izabrati jednu po jednu datoteku
- **Uredi stavku** – omogućava vam da uređujete navedenu putanju do izabrane datoteke ili fascikle
- **Ukloni stavku** – omogućava vam da sa liste izbrišete putanju do izabrane stavke
- **Uredi listu** – omogućava vam da uredite čitavu listu definisanih izuzetaka u novom dijalogu koji se ponaša kao standardni uređivač teksta

10.4.2. Keš server

Dijalog **Podešavanja keš servera** odnosi se na proces keš servera namenjen za ubrzavanje svih tipova **AVG Internet Security 2012** skeniranja:



Keš server prikuplja i čuva informacije o pouzdanim datotekama (*datoteka se smatra pouzdanom ako je potpisana digitalnim potpisom pouzdanog izvora*). Ove datoteke se zatim automatski smatraju bezbednim i ne treba ponovo da se skeniraju; zato se one preskaču tokom skeniranja.

Dijalog **Podešavanja keš servera** nudi sledeće opcije za konfiguraciju:

- **Keširanje je omogućeno** (*podrazumevano je uključeno*) - opozovite izbor u ovom polju za potvrdu da biste isključili **Keš server** i ispraznili keš memoriju. Imajte u vidu da će se skeniranje možda usporiti i da može doći do pada ukupnih performansi računara jer će se svaka datoteka skenirati u potrazi za virusima i špijunskim programima.
- **Omogući dodavanje novih datoteka u keš memoriju** (*podrazumevano je uključeno*) - opozovite izbor u ovom polju za potvrdu da biste zaustavili dodavanje datoteka u keš memoriju. Datoteke koje se već nalaze u keš memoriji koristiće se sve dok potpuno ne isključite keširanje ili do sledećeg ažuriranja baze podataka o virusima.

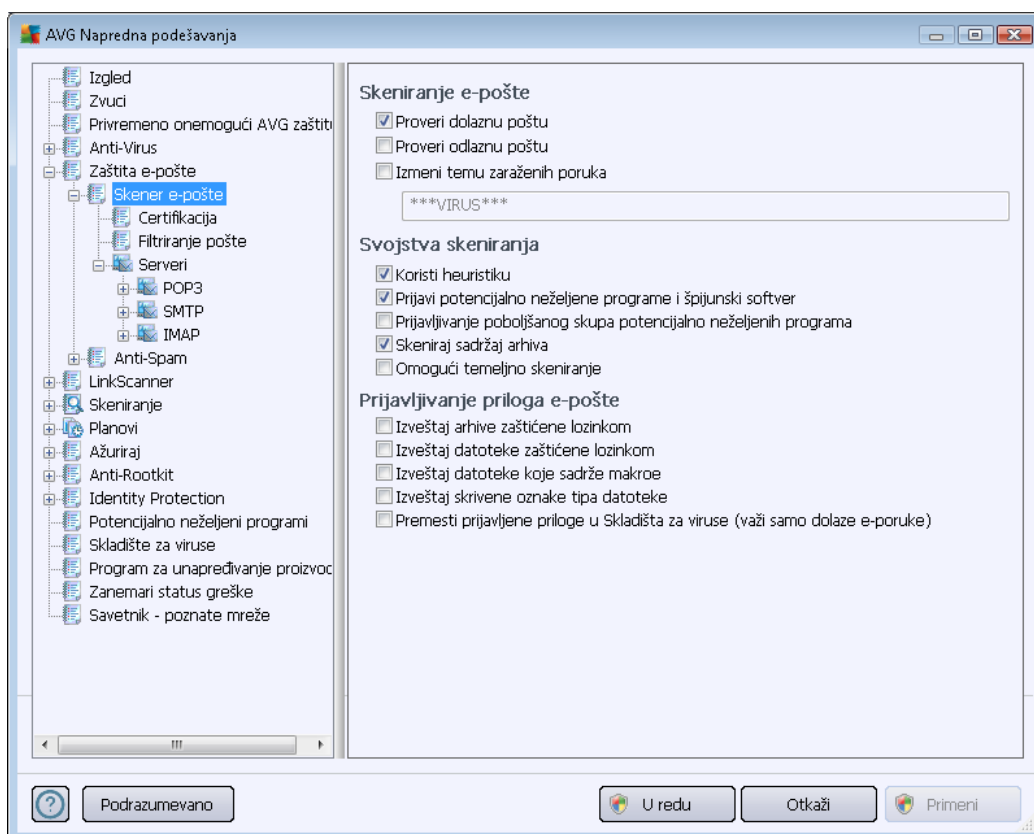
Ako nemate dobar razlog da isključite keš server, preporučuje se da zadržite podrazumevana podešavanja i ostavite obe opcije uključene! U suprotnom možete doživeti znatno smanjenje brzine i performanse sistema.

10.5. Zaštita e-pošte

U odeljku **Zaštita e-pošte** možete urediti detaljnu konfiguraciju [Skenera e-pošte](#) i [Odbrane od bezvredne pošte](#):

10.5.1. Skener e-pošte

Dijalog **Skener e-pošte** podeljen je na tri odeljka:



Skeniranje e-pošte

U ovom odeljku, možete podesiti sledeće osnove za dolazne i/ili odlazne poruke e-pošte:

- **Proveri dolazne poruke** (*podrazumevano uključeno*) - označite da postavite uključeno/isključeno opciju skeniranja svih poruka e-pošte koje dolaze do vašeg klijenta za e-poštu
- **Proveri odlazne poruke** (*podrazumevano isključeno*) - označite da postavite uključeno/isključeno opciju skeniranja svih poruka koje se šalju sa vašeg naloga
- **Izmeni naslov poruka zaraženih virusom** (*podrazumevano isključeno*) - ako želite da budete upozoreni da je skenirana poruka e-pošte detektovana kao zarazna, označite ovu stavku i unesite željeni tekst u tekstualno polje. Ovaj tekst će zatim biti dodat u polje "Naslov" svake detektovane poruke e-pošte radi lakše identifikacije i filtriranja. Podrazumevana vrednost je *****VIRUS*****, za koju vam preporučujemo da je ne menjate.

Svojstva skeniranja

U ovom odeljku možete odrediti kako će poruke e-pošte biti skenirane:

- **Koristi heuristiku** (*podrazumevano uključeno*) - označite ovo polje radi upotrebe metode heurističke detekcije prilikom skeniranja poruka e-pošte. Ako je ova opcija uključena, priloge e-poruka možete filtrirati ne samo po oznaci tipa, već i po stvarnom sadržaju priloga. Filtriranje se može podesiti u dijalogu [Filtriranje pošte](#).
- **Prijavi potencijalno neželjene programe i špijunski softver** (*podrazumevano uključeno*) - označite ovo polje radi aktivacije [Antispajver](#) mehanizma i skeniranja u potrazi za špijunskim programima kao i virusima. [Špijunski softver](#) se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.
- **Prijavi poboljšani skup potencijalno neželjenih programa** (*podrazumevano isključeno*) - potvrdite radi detekcije proširenog paketa [špijunskih programa](#): programi koji su potpuno u redu i bezopasni kada ih kupite direktno od proizvođača, ali se kasnije mogu iskoristiti u zlonamernu svrhu. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Skeniraj unutar arhiva** (*podrazumevano uključeno*) - označite ovo polje radi skeniranja sadržaja arhiva prikacenih uz poruke e-pošte.
- **Omogući temeljno skeniranje** (*podrazumevano isključeno*) - u posebnim situacijama (*npr. ako sumnjate da je vaš računar zaražen virusom ili eksploitom*) možete označiti ovu opciju da aktivirate najtemeljnije algoritme za skeniranje, koji će skenirati čak i one oblasti na računaru koji se teško mogu zaraziti, radi predostrožnosti. Ipak, zapamtite da ovaj metod prilično dugo traje.

Prijavljivanje priloga e-pošte

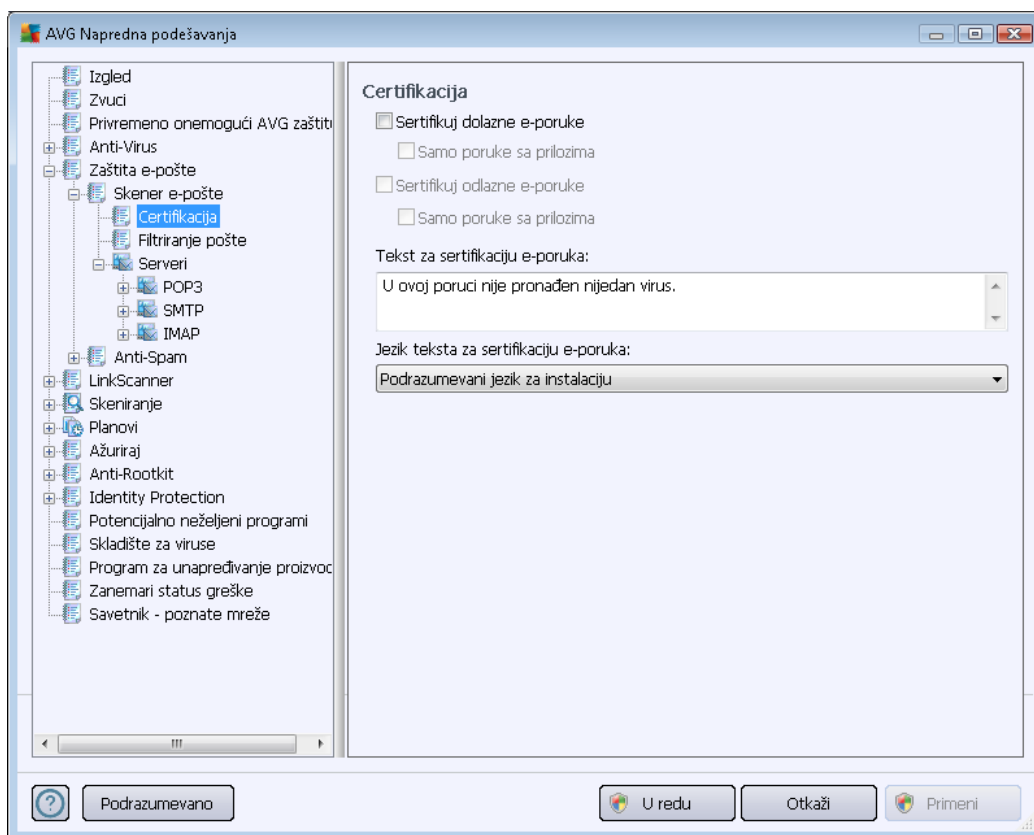
U ovom odeljku možete podesiti opcije za kreiranje dodatnih izveštaja o potencijalno opasnim ili sumnjivim datotekama. Imajte u vidu da se neće prikazati dijalog sa upozorenjem, već će na kraju poruke samo biti dodat tekst za sertifikaciju, a svi izveštaji te vrste biće navedeni na listi u dijalogu [Detekcija od strane skenera e-pošte](#):

- **Prijavi arhive zaštićene lozinkom** – arhive (*ZIP, RAR, itd.*) zaštićene lozinkom ne mogu se skenirati da bi se proverilo da li sadrže viruse; označite ovo polje da bi ih program prijavljivao kao potencijalno opasne.
- **Prijavi dokumente zaštićene lozinkom** - dokumenti zaštićeni lozinkom ne mogu se skenirati da bi se proverilo da li sadrže viruse; označite ovo polje da bi ih program prijavljivao kao potencijalno opasne.
- **Prijavi datoteke koje sadrže makro** - makro je unapred definisan niz koraka za lakše obavljanje određenih zadataka od strane korisnika (*poznati su makroi iz programa MS Word*

). Kao takvi, makroi mogu sadržati potencijalno opasne instrukcije, pa ćete možda želiti da označite ovo polje kako biste bili sigurni da će datoteke sa makroima biti prijavljene kao sumnjive.

- **Prijavi skrivene oznake tipa datoteke** – skrivene oznake tipa mogu učiniti da npr. sumnjiva izvršna datoteka „nešto.txt.exe“ izgleda kao bezopasna datoteka u formatu čistog teksta „nešto.txt“; označite ovo polje da bi ih program prijavljivao kao potencijalno opasne.
- **Premesti prijavljene priloge u skladište za viruse** - navedite da li želite da dobijate obaveštenja putem e-pošte o arhivama i dokumentima koji su zaštićeni lozinkom, makroima koji sadrže datoteke i/ili datotekama sa skrivenim oznakama tipa koje su otkrivene u prilogu skenirane e-poruke. Ako takva poruka bude otkrivena tokom skeniranja, definišite da li želite da li želite da premestite takav zaraženi objekat u [Skladište za viruse](#).

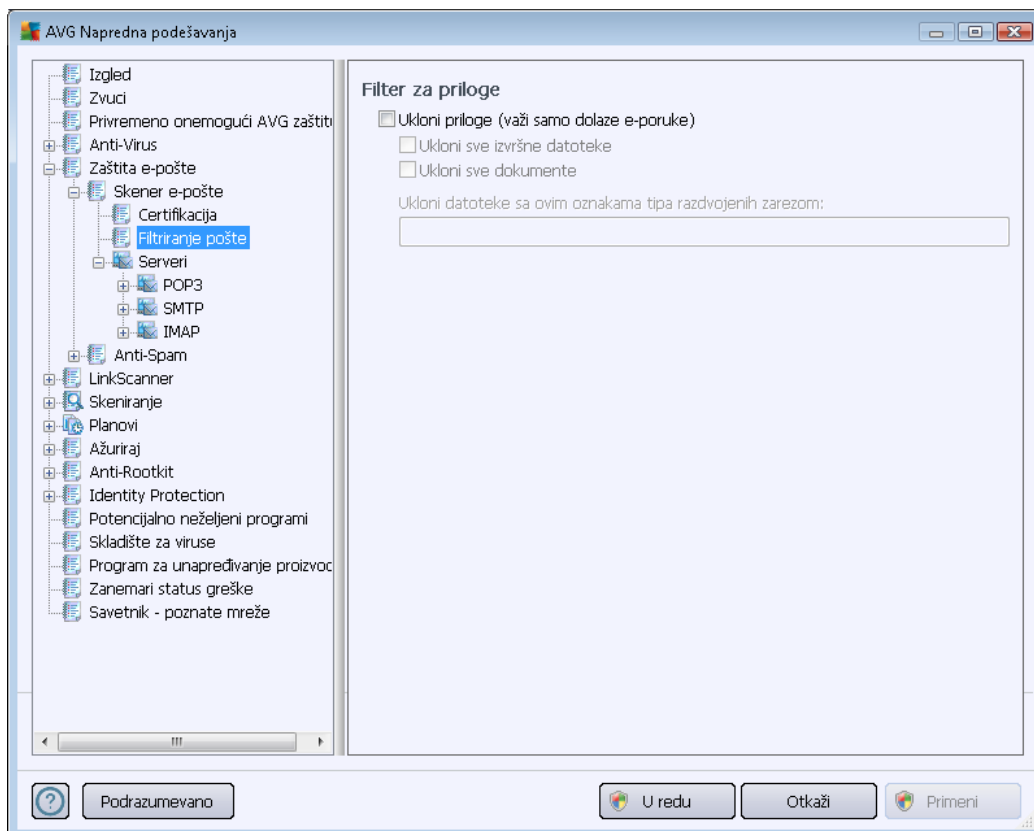
U dijalogu **Sertifikacija** možete označiti izbor u određenim poljima za potvrdu da biste odlučili da li želite da sertifikujete dolaznu poštu (**Sertifikuj dolaznu e-poštu**) i/ili odlaznu poštu (**Sertifikuj odlaznu e-poštu**). Za svaku od ovih opcija možete dodatno navesti parametar **Samo sa prilogima** da bi se sertifikacija dodala samo e-porukama sa prilogima:



Tekst sertifikacije podrazumevano se sastoji samo od informacija koje saopštavaju da *Nije pronađen nijedan virus u ovoj poruci*. Međutim, ove informacije se mogu proširiti ili promeniti u skladu sa vašim potrebama: upišite željeni tekst sertifikacije u polje **Tekst sertifikacije e-pošte**. U odeljku **Jezik korišćen za tekst sertifikacije e-pošte** možete dodatno definisati na kom jeziku treba da se prikaže

automatski generisani deo sertifikacije (*Nije pronađen nijedan virus u ovoj poruci*).

Napomena: imajte u vidu da će se samo podrazumevani tekst prikazati na traženom jeziku, a prilagođeni tekst se neće automatski prevoditi!



Dijalog **Filter za priloge** omogućava vam da podesite parametre za skeniranje priloga e-poruka. Podrazumevano, opcija **Ukloni priloge** je isključena. Ako odlučite da je aktivirate, svi prilogi e-poruka koji se prepoznaju kao zarazni ili potencijalno opasni biće automatski uklonjeni. Ako želite da definišete koji će se tip priloga uklanjati, izaberite željenu opciju:

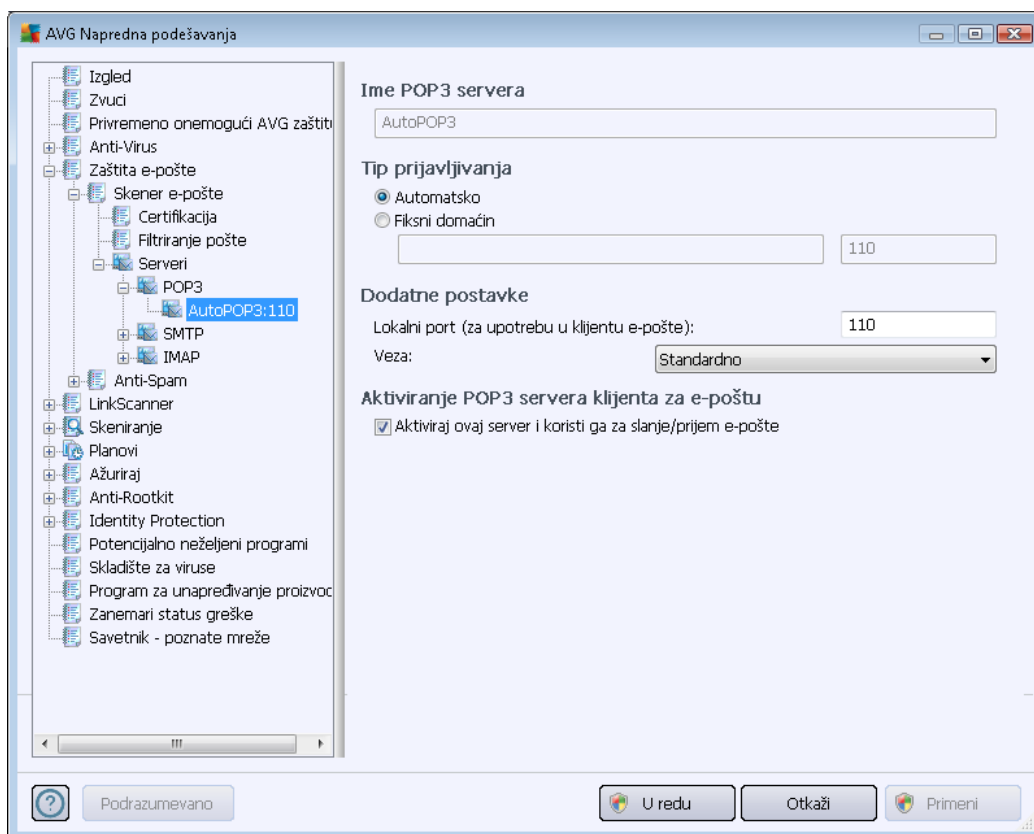
- **Ukloni sve izvršne datoteke** - sve *.exe datoteke se brišu
- **Ukloni sve dokumente** - biće izbrisane sve datoteke tipa *.doc, *.docx, *.xls, *.xlsx
- **Ukloni datoteke sa sledećim oznakama tipa datoteke razdvojenih zarezima** - uklanjanje svih datoteka sa definisanim oznakama tipa datoteke

U odeljku **Serveri** možete urediti parametre servera [skenera e-pošte](#):

- [POP3 server](#)

- [SMTP server](#)
- [IMAP server](#)

Isto tako možete definisati novi server za dolaznu ili odlaznu poštu pomoću dugmeta **Dodaj novi server**.

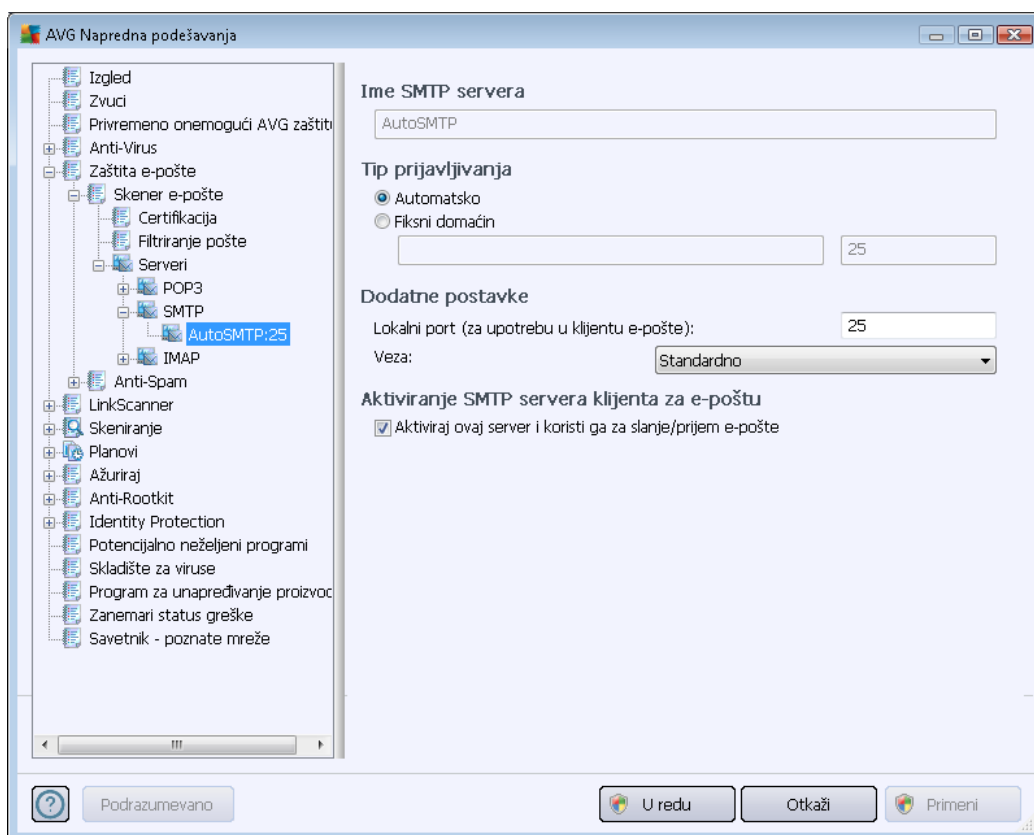


U ovom dijalogu (koji se otvara preko stavke **Serveri / POP3**) možete podesiti nov server za [Skener e-pošte](#) pomoću POP3 protokola za dolaznu e-poštu:

- **Naziv POP3 servera** - u ovom polju možete odrediti naziv novih dodatih servera (da dodate POP3 server, kliknite desnim dugmetom miša na stavku POP3 levog navigacionog menija). Za automatski kreirane "AutoPOP3" servere, ovo polje je deaktivirano.
- **Tip prijavljivanja** - definiše način određivanja servera za poštu koji se koristi za dolazne e-poruke:
 - **Automatski** - prijavljivanje se obavlja automatski u skladu sa podešavanjima klijenta e-pošte.
 - **Fiksni host** - u ovom slučaju, program će uvek koristiti server koji je ovde naveden. Navedite adresu ili ime svog servera za poštu. Korisničko ime ostaje nepromenjeno. Kao ime možete da koristite ime domena (na primer, *pop.acme.com*) kao i IP adresu

(na primer, 123.45.67.89). Ako server za poštu koristi port koji nije standardan, možete da navedete ovaj port iza imena servera koristeći dvotačku kao znak za razgraničavanje (na primer, pop.acme.com:8200). Standardni port za POP3 komunikaciju jeste 110.

- **Dodatna podešavanja** - definisanje dodatnih parametara:
 - **Lokalni port** - određuje port na kojem treba očekivati komunikaciju aplikacije za e-poštu. Zatim morate da u aplikaciji za poštu navedete ovaj port kao port za POP3 komunikaciju.
 - **Veza** – u padajućem meniju možete da izaberete vrstu veze koju želite da koristite (standardna/SSL/SSL podrazumevana). Ako odaberete SSL vezu, podaci koji se šalju biće šifrovani bez rizika da ih neko drugi može pratiti ili nadgledati. Ova funkcija je takođe dostupna samo ako je određeni server za poštu podržava.
- **Aktiviranje POP 3 servera klijenta e-pošte** - označite/opozovite izbor u ovom polju za potvrdu da biste aktivirali ili deaktivirali izabrani POP3 server

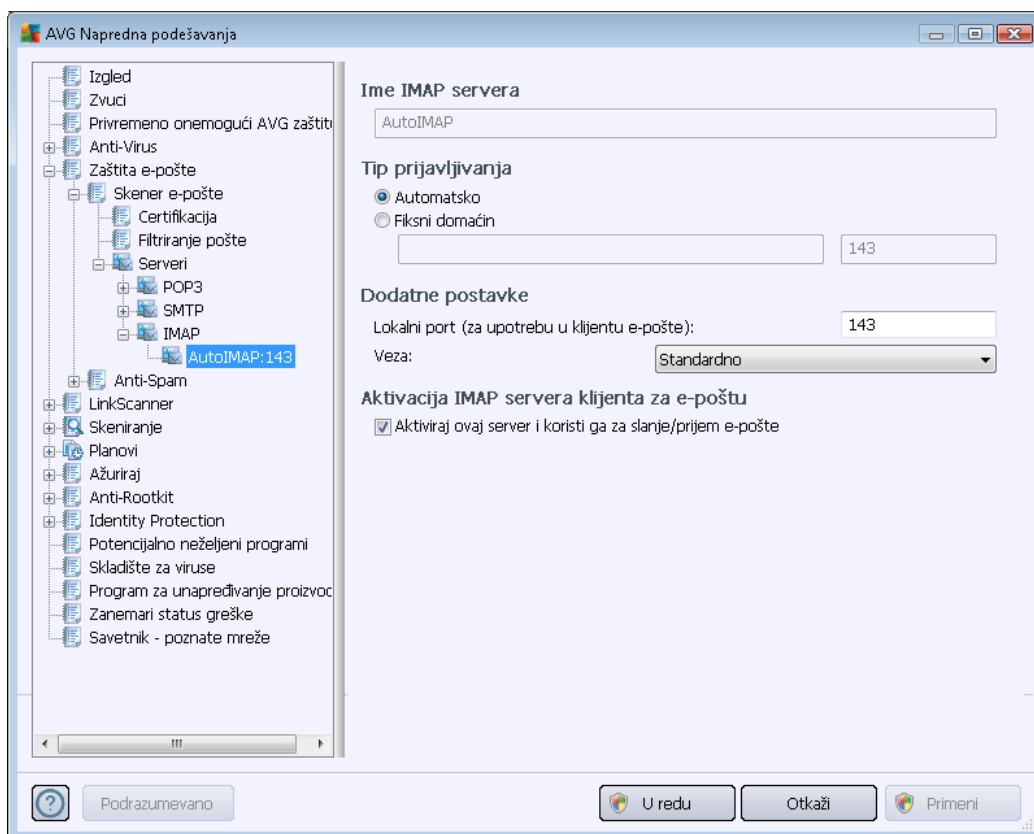


U ovom dijalogu (koji otvarate preko stavke **Serveri / SMTP**) možete podesiti novi server za [Skener e-pošte](#) pomoću SMTP protokola za odlaznu poštu:

- **Naziv SMTP servera** - u ovom polju možete odrediti naziv novih dodatnih servera (da biste

dodali SMTP server, kliknite desnim dugmetom miša na stavku SMTP levog navigacionog menija). Za automatski kreiran "AutoSMTP" server ovo polje je deaktivirano.

- **Tip prijavljivanja** - definiše način određivanja servera za poštu koji se koristi za odlaznu poštu:
 - **Automatski** - prijavljivanje se obavlja automatski, u skladu sa postavkama klijenta e-pošte
 - **Fiksni host** - u ovom slučaju, program će uvek koristiti server koji je ovde naveden. Navedite adresu ili ime svog servera za poštu. Možete da koristite ime domena (*na primer, smtp.acme.com*) kao i IP adresu (*na primer, 123.45.67.89*) kao naziv. Ako server za poštu koristi port koji nije standardan, možete da otkucate ovaj port iza imena servera, koristeći dvotačku kao znak za razgraničavanje (*na primer, smtp.acme.com:8200*). Standardni port za SMTP komunikaciju je 25.
- **Dodatna podešavanja** - definisanje dodatnih parametara:
 - **Lokalni port** - određuje port na kojem treba očekivati komunikaciju aplikacije za e-poštu. Zatim morate da u aplikaciji za poštu navedete ovaj port kao port za komunikaciju.
 - **Veza** - u ovom padajućem meniju, možete da odredite koju vrstu veze ćete koristiti (*redovna/SSL/SSL podrazumevana*). Ako odaberete SSL vezu, podaci koji se šalju biće šifrovani bez rizika da ih neko drugi može pratiti ili nadgledati. Ova funkcija je dostupna samo ako je određeni server za poštu podržava.
- **Aktivacija SMTP servera klijenta e-pošte** - označite/opozovite izbor u ovom polju za potvrdu da biste aktivirali/deaktivirali gore navedeni SMTP server



U ovom dijalogu (koji se otvara putem **Servera / IMAP**) možete podesiti novi server [Skenera e-pošte](#) koristeći IMAP protokol za odlaznu poštu:

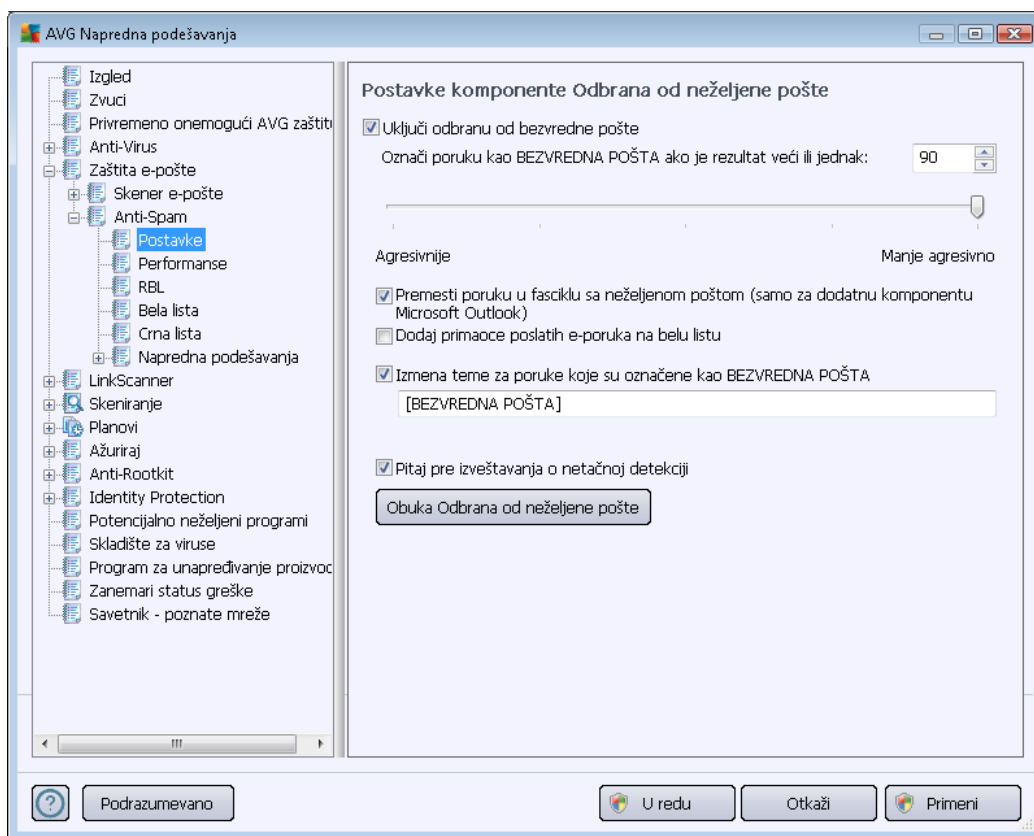
- **Naziv IMAP servera** - u ovom polju možete odrediti naziv novih dodatnih servera (da dodate IMAP server, kliknite desnim dugmetom miša na stavku IMAP levog navigacionog menija). Za automatski kreiran "AutoIMAP" server, ovo polje je deaktivirano.
- **Tip prijavljivanja** - definiše način određivanja servera za poštu koji se koristi za odlaznu poštu:
 - **Automatski** - prijavljivanje se obavlja automatski, u skladu sa postavkama klijenta e-pošte
 - **Fiksni host** - u ovom slučaju, program će uvek koristiti server koji je ovde naveden. Navedite adresu ili ime svog servera za poštu. Možete da koristite ime domena (na primer, *smtp.acme.com*) kao i IP adresu (na primer, *123.45.67.89*) kao naziv. Ako server za poštu koristi port koji nije standardan, možete da otkucate ovaj port iza imena servera, koristeći dvotačku kao znak za razgraničavanje (na primer, *smtp.acme.com:8200*). Standardni port za IMAP komunikaciju je 143.
- **Dodatna podešavanja** - definisanje dodatnih parametara:
 - **Lokalni port** - određuje port na kojem treba očekivati komunikaciju aplikacije za e-

poštu. Zatim morate u aplikaciji za poštu da navedete ovaj port kao port za IMAP komunikaciju.

- **Veza** - u ovom padajućem meniju, možete da odredite koju vrstu konekcije ćete koristiti (*standardna/SSL/SSL podrazumevana*). Ako odaberete SSL vezu, podaci koji se šalju biće šifrovani bez rizika da ih neko drugi može pratiti ili nadgledati. Ova funkcija je dostupna samo ako je određeni server za poštu podržava.

- **Aktivacija IMAP servera klijenta e-pošte** – označite/opozovite ovo polje za potvrdu da biste aktivirali/deaktivirali gorenavedeni IMAP server

10.5.2. Odbrana od bezvredne pošte



U dijalogu **Podešavanja odbrane od neželjene pošte** možete da označite/opozovete izbor u polju za potvrdu **Uključi zaštitu od neželjene pošte** da biste dozvolili/zabranili skeniranje komunikacije putem e-pošte u potrazi za bezvrednom poštom. Ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to.

Takođe možete da izaberete agresivnije ili manje agresivne mere ocenjivanja. Filter komponente **Odbrana od neželjene pošte** dodeljuje rezultat svakoj poruci (tj. *koliko je sadržaj poruke sličan NEŽELJENOJ POŠTI*) na osnovu nekoliko tehnika dinamičkog skeniranja. Postavku **Označi poruku kao neželjenu poštu ako je rezultat veći od** možete prilagoditi, tako što ćete uneti željenu vrednost ili pomeriti klizač na levo ili na desno (, *raspon vrednosti je ograničen na 50-90*).



Uglavnom preporučujemo da se granica postavi između 50–90, a ako ste i dalje neodlučni, na 90. Evo opšteg pregleda granice ocenjivanja:

- **Vrednost 80-90** - e-poruke koje su verovatno bezvredne biće filtrirane. Može se desiti da se greškom filtriraju i neke poruke koje nisu neželjene.
- **Vrednost 60-79** - smatra se prilično agresivnom konfiguracijom. E-poruke koje su možda bezvredne biće filtrirane. Postoji mogućnost da budu filtrirane i poruke koje nisu bezvredne.
- **Vrednost 50-59** - veoma agresivna konfiguracija. Jednako je verovatno da će biti obuhvaćene i e-poruke koje nisu bezvredne, kao i prave bezvredne poruke. Ovaj granični opseg se ne preporučuje za uobičajenu upotrebu.

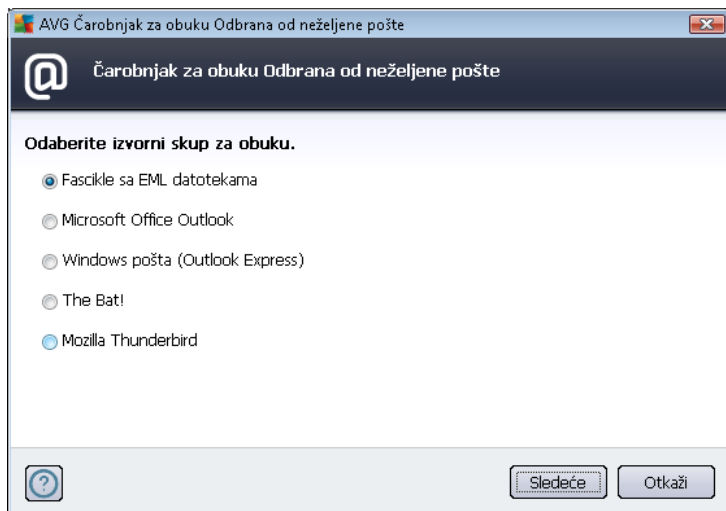
U dijalogu **Podešavanja odbrane od bezvredne pošte** možete definisati i kako će se postupati sa otkrivenim bezvrednim e-porukama:

- **Premesti poruku u fasciklu sa neželjenom poštom** (samo Microsoft Outlook dodatna komponenta)- potvrdite izbor u ovom polju za potvrdu ako želite da se svaka otkrivena neželjena poruka automatski premesti u fasciklu sa neželjenom poštom u okviru vašeg MS Outlook klijenta e-pošte. Funkcija trenutno nije podržana u drugim klijentima pošte.
- **Dodaj primaoca poslatih e-poruka na belu listu** - označite ovo polje za potvrdu da biste potvrdili da su svi primaoci poslatih e-poruka pouzdani i da sve poruke koje stižu sa njihovih naloga za e-poštu treba da budu isporučene.
- **Izmeni temu poruka koje se označene kao neželjena pošta** - potvrdite izbor u ovom polju za potvrdu ako želite da sve neželjene poruke budu označene određenom rečju ili znakom u polju za temu e-poruke; željeni tekst možete uneti u aktivirano polje za tekst.
- **Pitaj pre prijavljivanja pogrešnog otkrivanja** - uz uslov da ste se tokom [procesa instalacije](#) složili da učestvujete u [Programu unapređenja proizvoda](#). Ukoliko jeste, omogućili ste prijavljivanje detektovanih pretnji u AVG centar. Prijavljivanje se obavlja automatski. Međutim, možete označiti ovo polje radi potvrde da želite da budete pitani pre nego što bilo koja detektovana neželjena pošta bude prijavljena u AVG centar kako biste osigurali da poruka zaista treba da bude označena kao neželjena pošta.

Kontrolna dugmad

Dugme Obuka odbrane od neželjene pošte otvara [Čarobnjak za obuku odbrane od neželjene pošte](#), detaljno opisan u [sledećem poglavlju](#).

U prvom dijalogu **Čarobnjaka za obuku odbrane od neželjene pošte** od vas će se tražiti da izaberete izvor e-poruka koje želite da upotrebite za obuku. Uglavnom će biti potrebno da koristite neželjene e-poruke koje su netačno obeležene kao bezvredna pošta ili koje nisu prepoznate.



Postoje sledeće opcije:

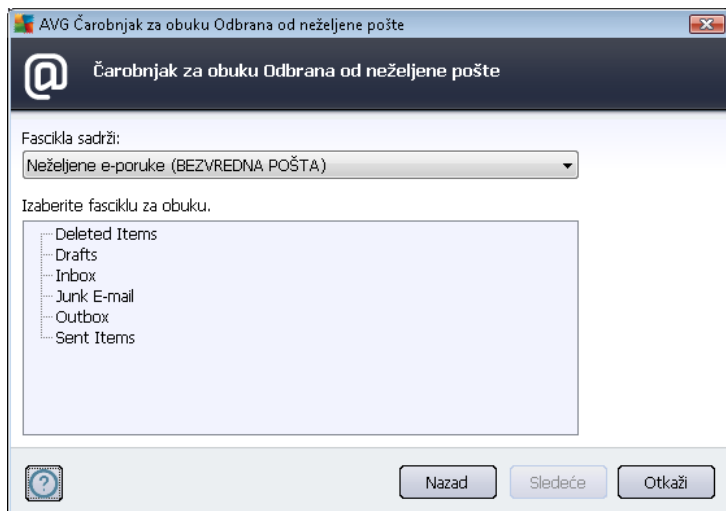
- **Određeni klijent e-pošte** – ako koristite jedan od navedenih klijenata e-pošte (*MS Outlook, Outlook Express, The Bat!*), jednostavno izaberite odgovarajuću opciju
- **Fascikla sa EML datotekama** - ako koristite neki drugi program za e-poštu, najpre bi trebalo da sačuvate poruke u određenu fasciklu (*u formatu .eml*) ili da se uverite da znate u kojoj fascikli vaš program za e-poštu čuva poruke. Zatim izaberite **Fascikla sa EML datotekama**, što će vam u sledećem koraku omogućiti da pronađete odgovarajuću fasciklu.

Da biste olakšali i ubrzali proces obuke trebalo bi da prethodno sortirate e-poruke u fasciklama tako da fascikla koju ćete koristiti za obuku sarži samo odgovarajuće e-poruke (željene ili neželjene). Međutim, to nije neophodno pošto ćete kasnije moći da filtrirate e-poruke.

Izaberite odgovarajuću opciju i kliknite na dugme **Sledeće** da biste nastavili sa čarobnjakom.

Koji će se dijalog prikazati u ovom koraku zavisi od toga šta ste prethodno izabrali.

Fascikle sa EML datotekama



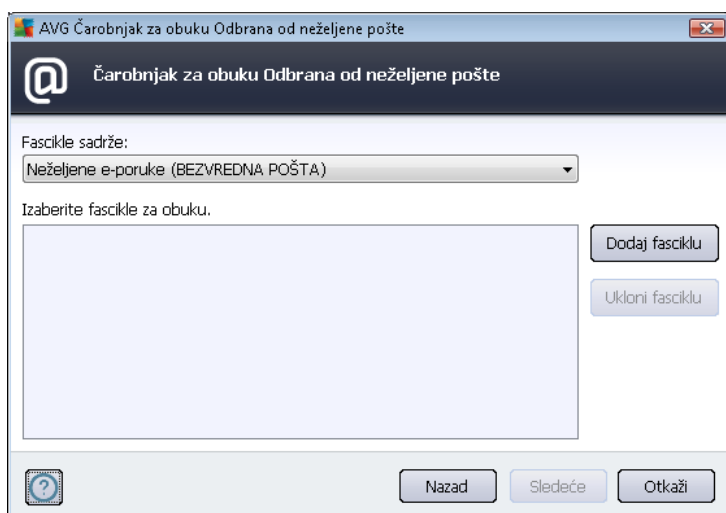
U ovom dijalogu izaberite fasciklu koja sadrži poruke koje želite da upotrebite za obuku. Kliknite na dugme **Dodaj fasciklu** da biste pronašli fasciklu koja sadrži .eml datoteke (*sačuvane e-poruke*). Izabrana fascikla biće prikazana u dijalogu.

U padajućem meniju **Fascikle sadrže** izaberite jednu od dve opcije – da li izabrana fascikla sadrži željene poruke (*željena pošta*) ili neželjene poruke (*neželjena pošta*). Obratite pažnju na to da ćete u sledećem koraku moći da filtrirate e-poruke, pa fascikla ne mora da sadrži samo e-poruke za obuku. Neželjene izabrane fascikle možete ukloniti sa liste ako kliknete na dugme **Ukloni**.

Kada završite, kliknite na dugme **Sledeće** i pređite na [Opcije za filtriranje poruka](#).

Određeni klijent e-pošte

Nakon što potvrdite neku do opcija, pojaviće se novi dijalog.

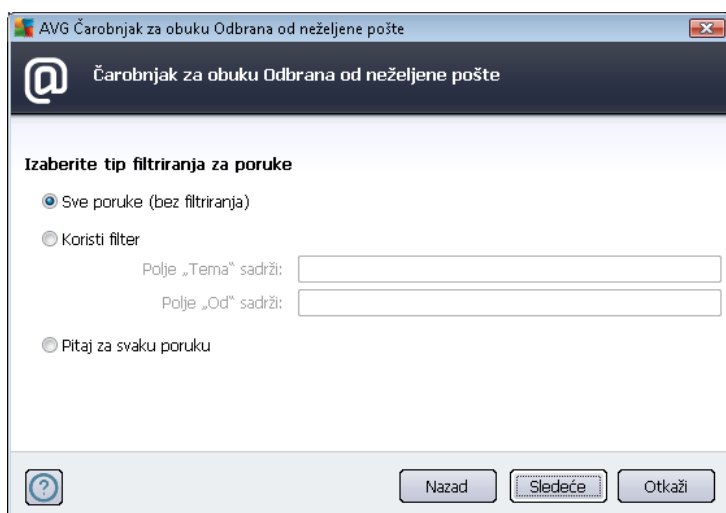


Napomena: Ako je u pitanju Microsoft Office Outlook, od vas će se zatražiti da prvo izaberete profil

MS Office Outlook.

U padajućem meniju **Fascikle sadrže** izaberite jednu od dve opcije – da li izabrana fascikla sadrži željene poruke (*željena pošta*) ili neželjene poruke (*neželjena pošta*). Obratite pažnju na to da ćete u sledećem koraku moći da filtrirate e-poruke, pa fascikla ne mora da sadrži samo e-poruke za obuku. U glavnom odeljku u dijalogu biće prikazano stablo za navigaciju za izabrani klijent e-pošte. Pronađite odgovarajuću fasciklu u stablu pa je označite pomoću miša.

Kada završite, kliknite na dugme **Sledeće** i pređite na [Opcije za filtriranje poruka](#).

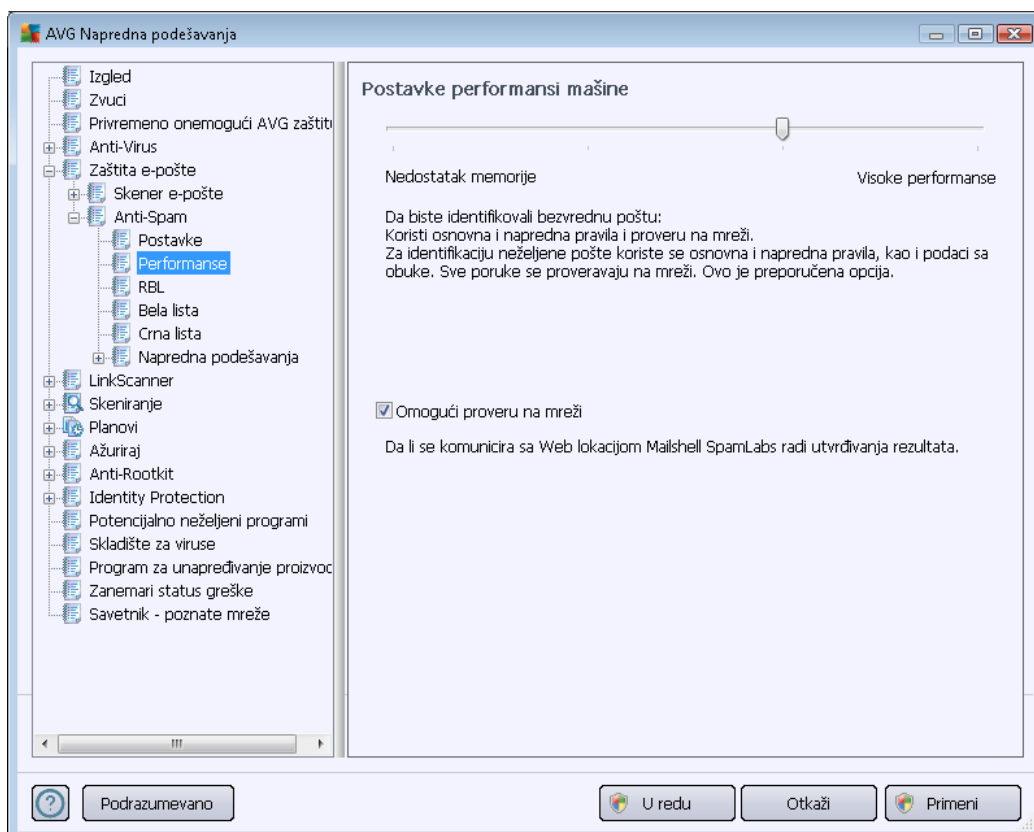


U ovom dijalogu možete da podesite filtriranje e-poruka.

- **Sve poruke (bez filtriranja)** - ako ste sigurni da izabrana fascikla sadrži samo poruke koje želite da koristite za obuku, izaberite opciju **Sve poruke (bez filtriranja)**.
- **Koristi filter** - za naprednije filtriranje izaberite opciju **Koristi filter**. Možete uneti reč (*ime*), deo reči ili frazu koja će se tražiti u temi e-poruke i/ili polju Pošiljalac. Za obuku će, bez daljih upita, biti iskorišćene sve poruke koje potpuno odgovaraju unetim kriterijumima. Kada popunite oba tekstualna polja, koristiće se i adrese koje ispunjavaju jedan od dva uslova!
- **Pitaj za svaku poruku** - ako niste sigurni u vezi sa porukama u fascikli i želite da vas čarobnjak pita za svaku poruku pojedinačno (*kako biste mogli da utvrdite da li želite da je koristite za obuku ili ne*), izaberite opciju **Pitaj za svaku poruku**.

Nakon izbora odgovarajuće opcije, kliknite na dugme **Sledeće**. Sledeći dijalog je samo informativne prirode i saopštava vam da je čarobnjak spreman da obradi poruke. Da biste pokrenuli obuku, ponovo kliknite na dugme **Sledeće**. Počeće obuka u skladu sa izabranim uslovima.

Dijalog **Podešavanja performanse mašine** (povezan putem stavke **Performansa** navigacije sa leve strane) pruža podešavanja performanse komponente **Odbrana od bezvredne pošte**:



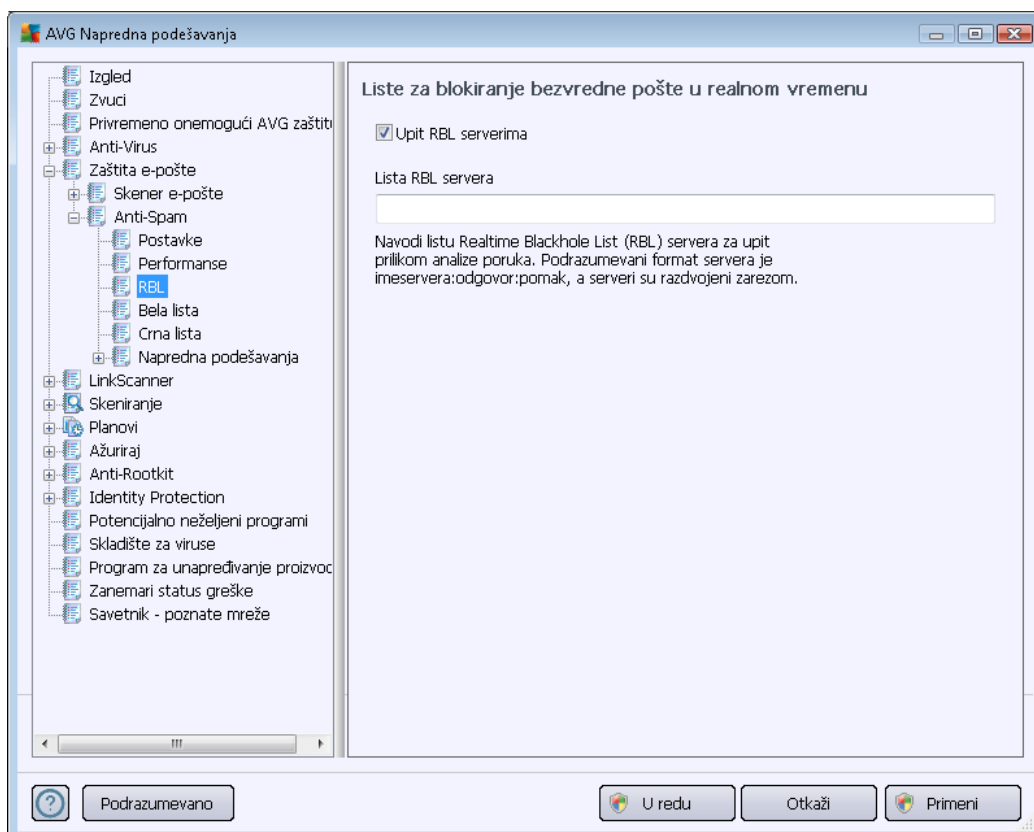
Pomerajte klizač nalevo ili nadesno da biste promenili nivo performansi skeniranja, koji se kreće između režima **Nedostatak memorije** / **Visoke performanse**.

- **Nedovoljno memorije** - tokom procesa skeniranja radi identifikovanja bezvredne pošte neće se koristiti nijedno pravilo. Za identifikaciju se koriste samo podaci za obuku. Ovaj režim nije preporučljiv za uobičajenu upotrebu, osim ukoliko hardver računara nije veoma loš.
- **Visoka performansa** - ovaj režim koristi veliku količinu memorije. U toku procesa skeniranja u cilju prepoznavanja bezvredne pošte, korišće se sledeće funkcije: pravila i keš baze podataka o bezvrednim porukama, osnovna i napredna pravila, IP adrese pošiljalaca bezvredne pošte i baze podataka pošiljalaca bezvredne pošte.

Stavka **Omogući proveru na mreži** podrazumevano je uključena. Rezultat je preciznija detekcija bezvredne pošte uz pomoć komunikacije sa [Mailshell](#) serverima, tj. skenirani podaci će se upoređivati sa [Mailshell](#) bazama podataka na mreži.

Uglavnom se preporučuje se da zadržite podrazumevana podešavanja, osim ako nemate dobar razlog da ih menjate. Ovu konfiguraciju smeju da menjaju samo iskusni korisnici!

Stavka **RBL** otvara dijalog za uređivanje pod imenom **Liste za blokiranje neželjene pošte u realnom vremenu** u kojem možete da uključite/isključite funkciju **Slanje upita RBL serverima**:

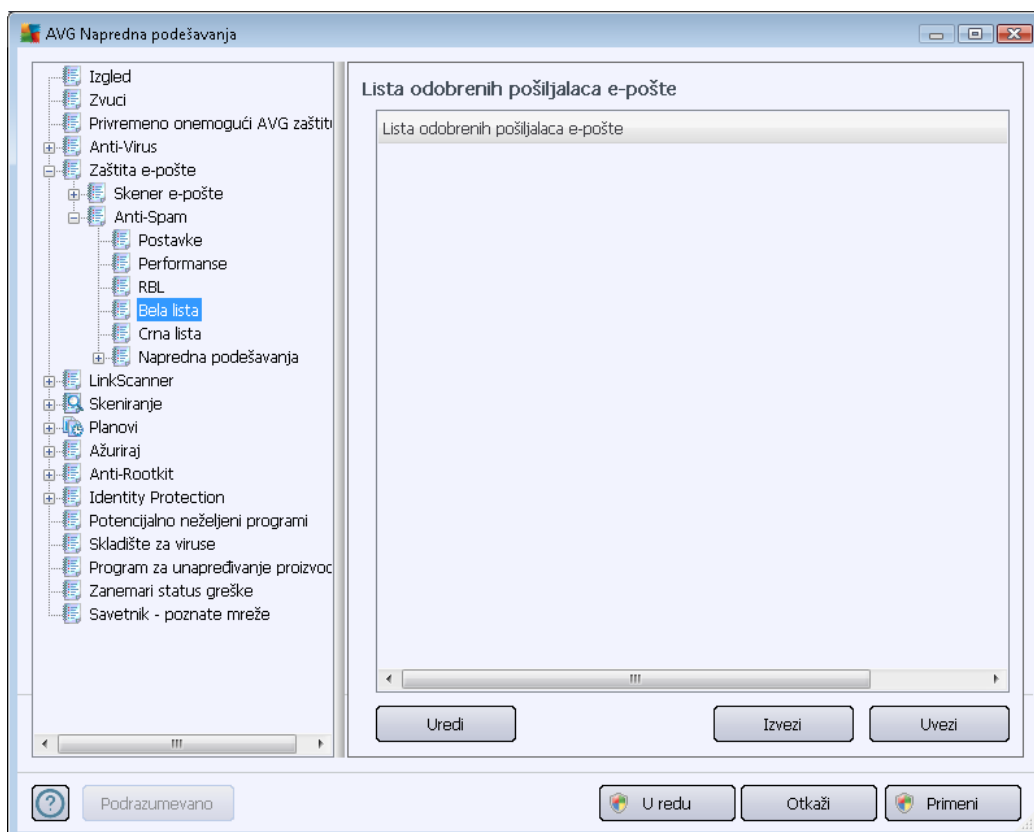


RBL (*Liste za blokiranje neželjene pošte*) server jeste DNS server sa opsežnom bazom podataka o poznatim pošiljaocima neželjene pošte. Kada se ova funkcija uključi, sve e-poruke biće proverene u bazi podataka RBL servera i označene kao neželjene ako su identične nekim stavkama u bazi podataka. Baza podataka RBL servera sadrži najnovije otiske bezvrednih poruka radi obezbeđivanja najboljeg i najtačnijeg otkrivanja bezvredne pošte. Ova funkcija je posebno korisna za korisnike koji dobijaju velike količine neželjene pošte koju mašina [Odbrana od neželjene pošte](#) obično ne otkriva.

Liste RBL servera vam omogućava da definišete specifične lokacije RBL servera (*imajte u vidu da omogućavanje ove funkcije na nekim sistemima i konfiguracijama može usporiti proces prijema e-pošte zato što se svaka poruka mora proveriti u odnosu na bazu podataka RBL servera*).

Lični podaci se ne šalju serveru!

Stavka **Bela lista** otvara dijalog **Lista odobrenih pošiljalaca e-pošte** sa opštom listom e-adresa odobrenih pošiljalaca i imena domena čije poruke nikad neće biti označene kao neželjene.



U interfejsu za uređivanje možete da sastavite listu pošiljalaca od kojih očekujete da će vam nikad neće slati bezvredne poruke (neželjene poruke). Takođe možete da sastavite listu punih imena domena (*npr. avg.com*), za koje znate da ne generišu neželjene poruke. Kada pripremite takvu listu pošiljalaca i/ili imena domena, možete je uneti pomoću sledećih metoda: direktnim unošenjem svake e-adrese ili uvoženjem čitave liste adresa odjednom.

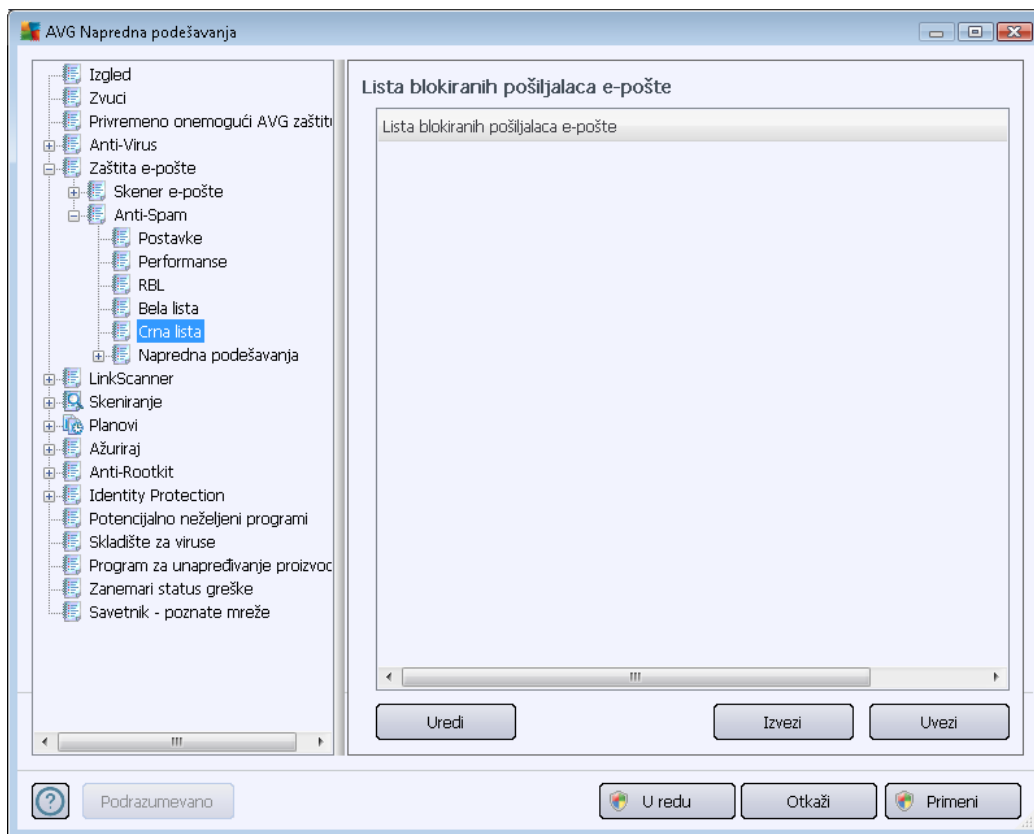
Kontrolna dugmad

Dostupna su sledeća kontrolna dugmad:

- **Uredi** - kliknite na ovo dugme da biste otvorili dijalog u kojem možete ručno da unesete listu adresa (*takođe možete da koristite metodu kopiranja i lepljenja*). Umetnite jednu stavku (*pošiljaoca, ime domena*) po redu.
- **Izvezi** - ako odlučite da iz nekog razloga izvezete zapise, možete to da uradite tako što ćete kliknuti na ovo dugme. Svi zapisi će biti sačuvani u datoteci u formatu čistog teksta.
- **Uvezi** - ako već imate pripremljenu tekstualnu datoteku e-adresa/imena domena, možete jednostavno da je uvezete tako što ćete kliknuti na ovo dugme. Datoteka mora da sadrži

samo jednu stavku (*adresa, ime domena*) po redu.

Kartica **Crna lista** služi za otvaranje dijaloga koji sadrži opštu listu blokiranih adresa e-pošte pošiljalaca i imena domena čije će poruke uvek biti označene kao neželjene.



U interfejsu za uređivanje možete da sastavite listu pošiljalaca od kojih očekujete da će vam slati neželjene poruke (*bezzvrednu poštu*). Takođe možete da sastavite listu punih imena domena (*npr. preduzeće_koje_salje_bezvrednu_poštu.com*), od kojih očekujete ili dobijate neželjene poruke. Sve e-poruke sa navedenih adresa/domena biće identifikovane kao bezvredna pošta. Kada pripremite takvu listu pošiljalaca i/ili imena domena, možete je uneti pomoću sledećih metoda: direktnim unošenjem svake e-adrese ili uvoženjem čitave liste adresa odjednom.

Kontrolna dugmad

Dostupna su sledeća kontrolna dugmad:

- **Uredi** - kliknite na ovo dugme da biste otvorili dijalog u kojem možete ručno da unesete listu adresa (*takođe možete da koristite metodu kopiranja i lepljenja*). Umetnite jednu stavku (*pošiljaoca, ime domena*) po redu.
- **Izvezi** - ako odlučite da iz nekog razloga izvezete zapise, možete to da uradite tako što



ćete kliknuti na ovo dugme. Svi zapisi će biti sačuvani u datoteci u formatu čistog teksta.

- **Uvezi** - ako već imate pripremljenu tekstualnu datoteku e-adresa/imena domena, možete jednostavno da je uvezete tako što ćete kliknuti na ovo dugme.

Grana Napredna podešavanja sadrži detaljne opcije za podešavanje komponente Odbrana od neželjene pošte. Ova podešavanja namenjena su izričito za iskusne korisnike, obično za administratore mreže koji treba detaljno da konfigurišu zaštitu od bezvredne pošte kako bi se na najbolji način zaštitili serveri e-pošte. Iz tog razloga, nije dostupna dodatna pomoć za pojedinačne dijaloge; međutim, u samom korisničkom interfejsu nalaze se kratki opisi svake opcije.

Preporučujemo vam da ne menjate nijednu postavku ukoliko niste u potpunosti upoznati za naprednim postavkama alatke Spamcatcher (MailShell Inc.). Neodgovarajuće promene mogu da dovedu do loših performansi ili nepravilnog rada komponente.

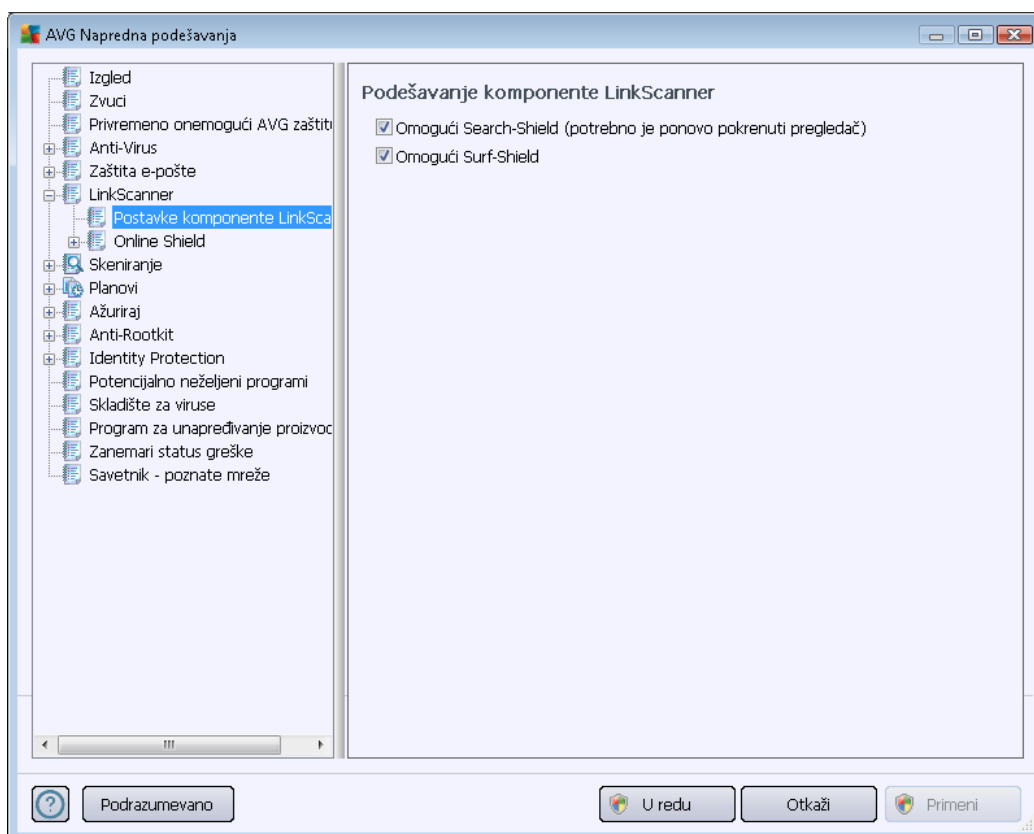
Ako ipak smatrate da je potrebno da promenite konfiguraciju komponente [Odbrana od neželjene pošte](#) na veoma naprednom nivou, pratite uputstva koja se nalaze u samom korisničkom interfejsu. Uglavnom se u svakom dijalogu nalazi po jedna određena funkcija koju možete urediti - njen opis se uvek nalazi u samom dijalogu:

- **Keš** - otisak prsta, reputacija domena, LegitRepute
- **Obuka** - maksimum unosa reči, granična vrednost za automatsku obuku, vrednost
- **Filtriranje** - lista jezika, lista zemalja, odobrene IP adrese, blokirane IP adrese, blokirane zemlje, blokirani skupovi znakova, lažni pošiljaoci
- **RBL** - RBL serveri, više pogodaka, granica, vremensko ograničenje, maksimalan broj IP adresa
- **Internet veza** - vremensko ograničenje, proxy server, provera identiteta proxy servera

10.6. LinkScanner

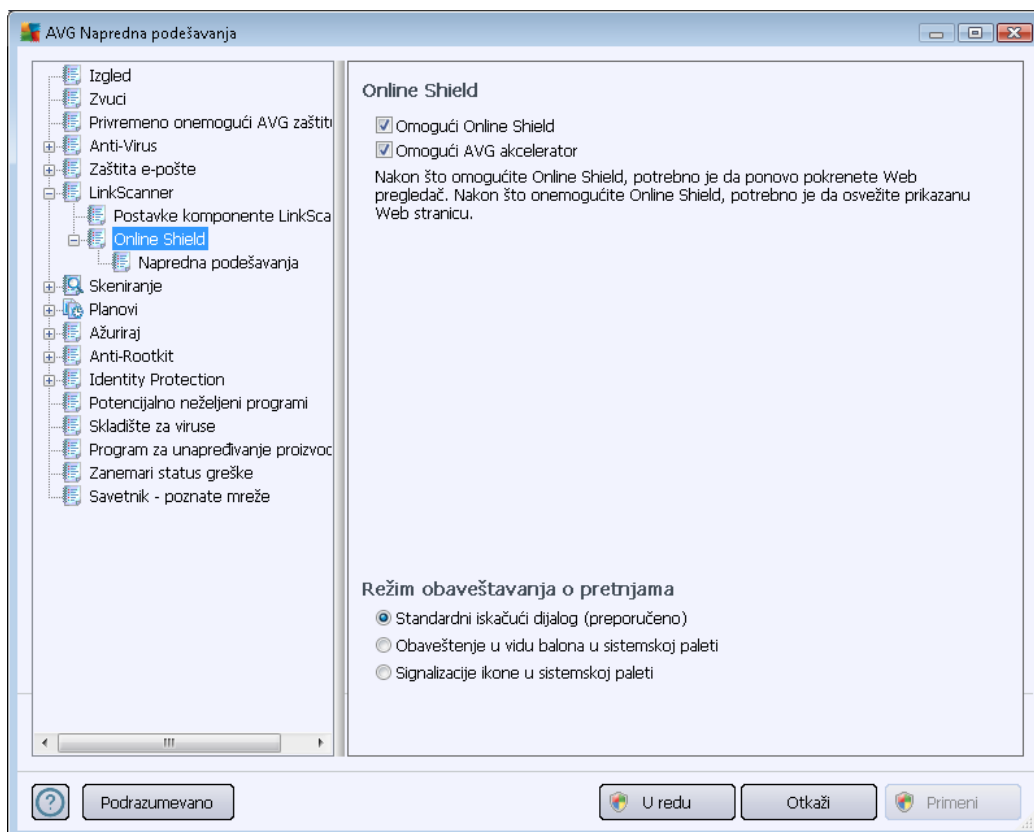
10.6.1. Postavke Skenera linkova

Dijalog **Postavke skenera linkova** vam omogućava da uključite/isključite osnovne funkcije komponente **LinkScanner**:



- **Omogući Štit za pretraživanje** - (podrazumevano uključeno): ikone obaveštenja koje daju savete o rezultatima pretrage pomoću Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg ili SlashDot pregledača: nakon provere sadržaja Web lokacija koje je vratio pretraživač.
- **Omogući Štit za pregledanje Interneta** - (podrazumevano uključeno): aktivna zaštita (u *realnom vremenu*) od zlonamernih Web lokacija u trenutku kada im se pristupa. Veze do poznatih zlonamernih Web lokacija i njihov opasan sadržaj se blokiraju dok im korisnik pristupa pomoću Web pregledača (ili neke druge aplikacije koja koristi HTTP).

10.6.2. Online Shield

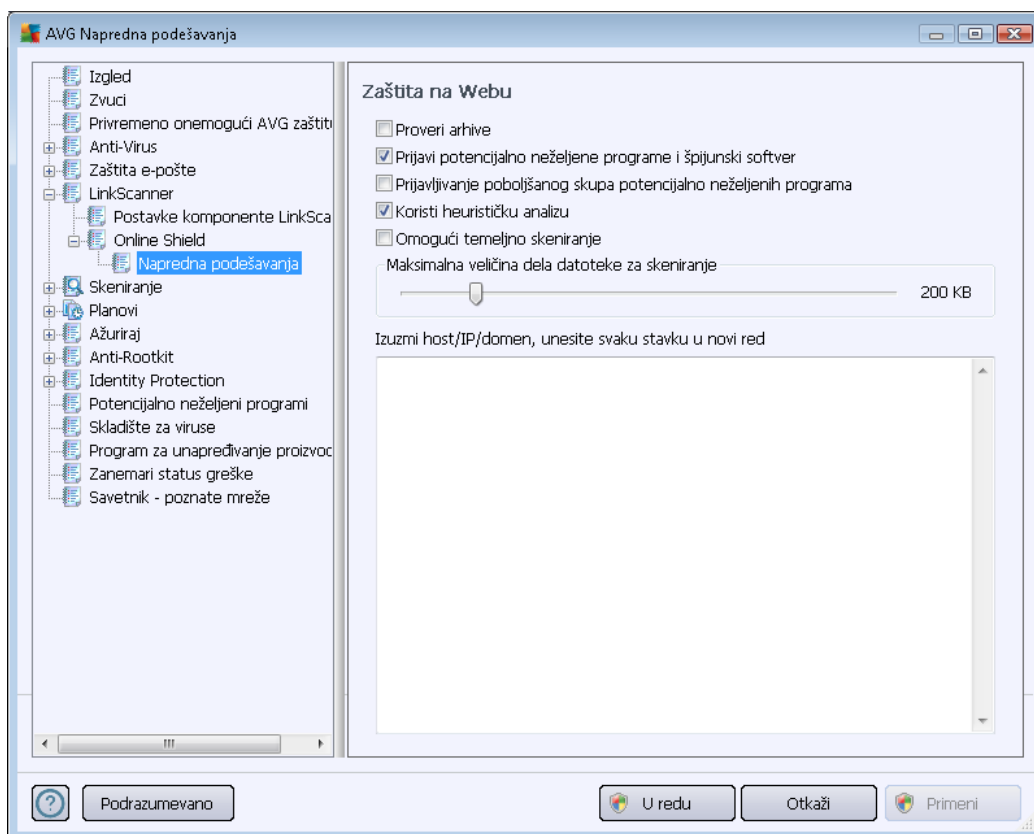


Dijalog **Online Shield** nudi sledeće opcije:

- **Omogući Online Shield** (*podrazumevano uključeno*) - aktivirajte/deaktivirajte kompletnu uslugu **Online Shield**. Za dodatna napredna podešavanja usluge **Online Shield** pređite na sledeći dijalog koji se zove [Zaštita na Webu](#).
- **Omogući AVG akcelerator** (*podrazumevano uključeno*) - aktivirajte/deaktivirajte uslugu **AVG akceleratora** koja omogućava jednostavniju reprodukciju video zapisa na mreži i olakšava dodatna preuzimanja.

Režim obaveštavanja o pretnjama

U donjem odeljku ovog dijaloga, izaberite način na koji želite da budete obaveštavani o mogućoj otkrivenoj pretnji: putem standardnog iskačućeg dijaloga, obaveštenja u sistemskoj paleti u obliku balončića ili pomoću signalizacije ikone u sistemskoj paleti.



U dijalogu **Zaštita na Webu** možete urediti konfiguraciju komponente u vezi sa skeniranjem sadržaja Web lokacija. Interfejs za uređivanje omogućava vam da konfigurišete sledeće osnovne opcije:

- **Omogući zaštitu na Webu** - ovom opcijom se potvrđuje da **Online Shield** treba da obavlja skeniranje sadržaja www stranica. Ako je ova opcija uključena (*podrazumevano*), možete uključiti/isključiti sledeće stavke:
 - **Proveri arhive** - (*podrazumevano isključeno*): skeniranje sadržaja arhiva koje se potencijalno nalaze na www stranici koja se prikazuje.
 - **Prijavi potencijalno neželjene programe i pretnje špijunskog softvera** - (*podrazumevano uključeno*): potvrdite izbor da biste aktivirali mašinu za [zaštitu od špijunskog softvera](#) i skenirali u potrazi za špijunskim softverom, kao i za virusima. [Špijunski softver](#) se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.
 - **Prijavi poboljšani skup potencijalno neželjenih programa** - (*podrazumevano isključeno*): označite radi detekcije proširenog paketa [špijunskih programa](#): programi koji su potpuno u redu i bezopasni kada ih kupite direktno od proizvođača, ali se kasnije mogu iskoristiti u zlonamernu svrhu. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost

blokiranja legalnih programa, ova opcija je podrazumevano isključena.

- **Koristi heurističku analizu-** (podrazumevano uključeno): skeniranje sadržaja stranice koja se prikazuje pomoću metoda [heurističke analize](#) (dinamičke emulacije naredbi skeniranog objekta u virtualnom računarskom okruženju).
- **Omogući temeljno skeniranje** (podrazumevano isključeno) - u posebnim situacijama (ako sumnjate da je vaš računar zaražen) možete označiti ovu opciju da aktivirate najtemeljnije algoritme za skeniranje, koji će skenirati čak i one oblasti na računaru koji se teško mogu zaraziti, radi predostrožnosti. Ipak, zapamtite da ovaj metod prilično dugo traje.
- **Maksimalna veličina datoteke za skeniranje** - ako se na prikazanoj stranici nalaze datoteke, možete skenirati njihov sadržaj pre nego što ih preuzmete na vaš računar. Međutim, skeniranje velikih datoteka može potrajati i, samim tim, znatno usporiti učitavanje Web stranice. Možete da koristite klizač da biste naveli maksimalnu veličinu datoteke za skeniranje komponentom **Online Shield**. Čak i u slučaju da je preuzeta datoteka veća nego što je određeno i Online Shield neće zbog toga da je skenira, ipak ćete biti zaštićeni: ako je datoteka zaražena, **Online Shield** će je odmah detektovati.
- **Izuzmi host/IP/domen** - u polje za tekst možete upisati tačno ime servera (host, IP adresu, IP adresu sa maskom ili URL adresu) ili domen koji ne bi trebalo da skenira **Online Shield**. Zbog toga izuzmite samo hostove za koje ste sigurni da ne sadrže Web lokacije sa opasnim sadržajem.

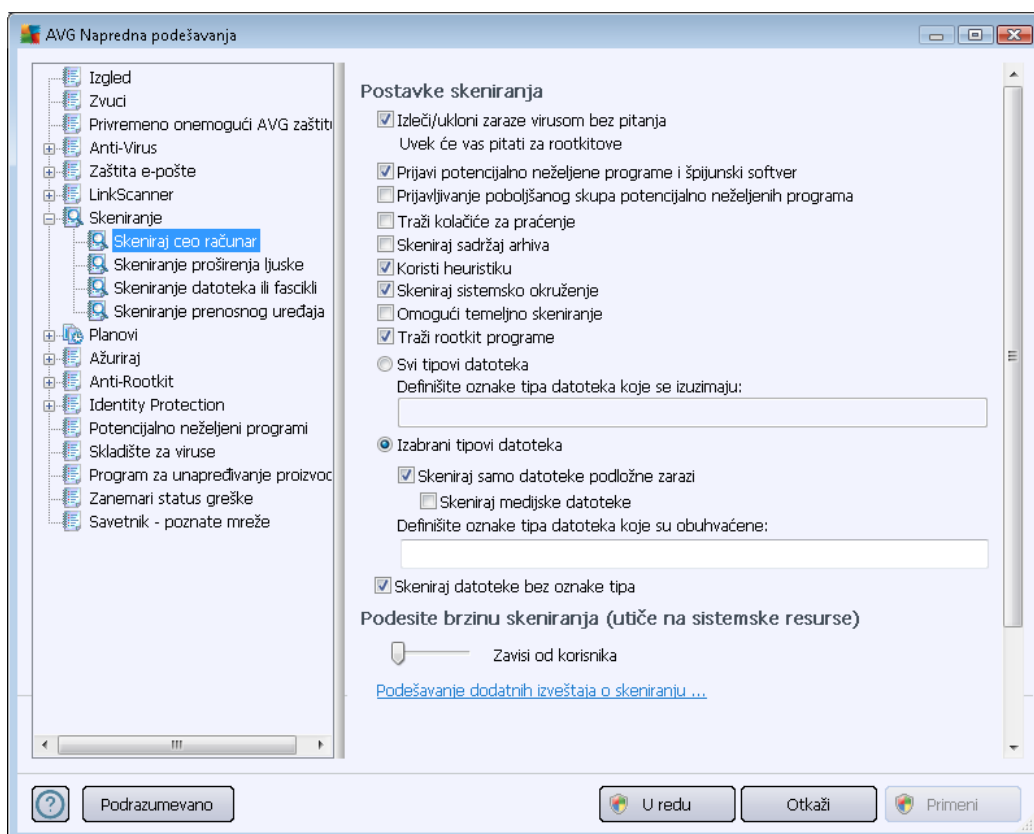
10.7. Skeniranja

Napredna podešavanja skeniranja podeljena su na četiri kategorije koje se odnose na određene tipove skeniranja, definisane od strane proizvođača softvera:

- [Skeniraj ceo računar](#) - standardno unapred definisano skeniranje celog računara
- [Shell Extension skeniranje](#) - posebno skeniranje izabranog objekta direktno iz programa Windows Explorer
- [Skeniranje datoteka ili fascikli](#) - standardno unapred definisano skeniranje izabranih oblasti na računaru
- [Skeniranje prenosnog uređaja](#) - posebno skeniranje prenosnih uređaja povezanih na računar

10.7.1. Skeniranje celog računara

Opcija **Skeniranje celog računara** vam omogućava da uredite parametre jednog od skeniranja koje je prodavac softvera unapred definisao, [Skeniranje celog računara](#):



Podešavanja skeniranja

U odeljku **Podešavanja skeniranja** pronaći ćete listu parametara za skeniranje koje je moguće opcionalno uključiti ili isključiti.

- **Izleči/ukloni virusnu infekciju bez upita** (podrazumevano uključeno): ako tokom skeniranja bude otkriven virus, moguće ga je automatski izlečiti ukoliko je dostupan lek. Ukoliko zaraženu datoteku nije moguće automatski izlečiti, ona će biti premeštena u [Skladište za viruse](#).
- **Prijavi potencijalno neželjene programe i pretnje špijunskog softvera** (podrazumevano uključeno) - označite radi aktivacije [Antispajver](#) mehanizma i skeniranja u potrazi za špijunskim programima kao i virusima. Špijunski softver se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.
- **Prijavi poboljšani skup potencijalno neželjenih programa** (podrazumevano isključeno)

- označite radi detekcije proširenog paketa špijunskih programa: programi koji su potpuno u redu i bezopasni kada ih kupite direktno od proizvođača, ali se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.

- **Skeniraj kolačiće za praćenje** (podrazumevano isključeno) - ovaj parametar komponente [Antispajver](#) definiše da bi trebalo da kolačići budu otkriveni kolačići; (*HTTP kolačići služe za proveru identiteta, praćenje, i održavanje određenih informacija o korisnicima, kao što su omiljene Web lokacije ili sadržaj njihovih elektronskih korpi za kupovinu*)
- **Skeniraj sadržaj arhiva** (podrazumevano isključeno) - ovaj parametar definiše da bi tokom skeniranja trebalo proveravati sve datoteke koje se nalaze unutar arhiva, npr. ZIP, RAR, ...
- **Koristi heuristiku** (podrazumevano uključeno) - heuristička analiza (*dinamička emulacija naredbi skeniranih objekata u virtuelnom računarskom okruženju*) biće jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja.
- **Skeniraj sistemsko okruženje** (podrazumevano uključeno) - skeniranje će obuhvatiti i sistemske oblasti vašeg računara.
- **Omogući temeljno skeniranje** (podrazumevano isključeno) - u posebnim situacijama (*ako sumnjate da je vaš računar zaražen*), možete označiti ovu opciju da aktivirate najtemeljnije algoritme za skeniranje, koji će skenirati čak i one oblasti na računaru koji se teško mogu zaraziti, radi predostrožnosti. Ipak, zapamtite da ovaj metod prilično dugo traje.
- **Skeniraj u potrazi za rootkit programima** (podrazumevano uključeno) - [Anti-Rootkit](#) skeniranje na računaru pretražuje moguće rootkit programe, tj. programe i tehnologije koji mogu pokriti aktivnost malvera na računaru. Ako se otkrije rootkit program, to ne znači da je vaš računar zaražen. U nekim slučajevima, određeni upravljački programi ili delovi običnih aplikacija mogu biti pogrešno protumačeni kao rootkit programi.

Trebalo bi i da odlučite da li želite da skenirate

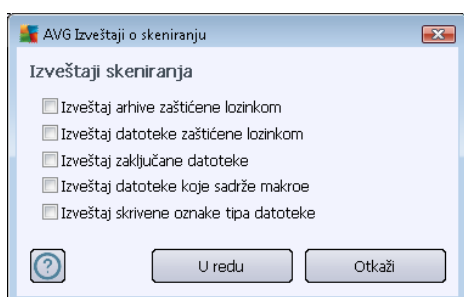
- **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka tako što ćete uneti listu oznaka tipa datoteka razdvojenih zarezima koje ne bi trebalo skenirati (*kada sačuvate listu, zarez i se pretvaraju u tačku i zarez*);
- **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteka možete označiti datoteke koje treba uvek skenirati.
- Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteka** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteka su sumnjive i treba ih uvek skenirati.

Podesite željenu brzinu završetka skeniranja

U odeljku **Podesite željenu brzinu završetka skeniranja** možete dalje odrediti željenu brzinu skeniranja, zavisno od iskorišćenosti kapaciteta sistema. Vrednost ove opcije podrazumevano je postavljena na nivo automatske zauzetosti resursa koja *zavisi od korisnika*. Ako želite da se skeniranje obavlja brže, biće potrebno manje vremena, ali će se iskorišćenost sistemskih resursa značajno povećati tokom skeniranja, a to će usporiti ostale aktivnosti na računaru (*ovu opciju možete koristiti kada je računar uključen, ali niko ne radi na njemu*). Sa druge strane, iskorišćenost sistemskih resursa možete smanjiti tako što ćete produžiti trajanje skeniranja.

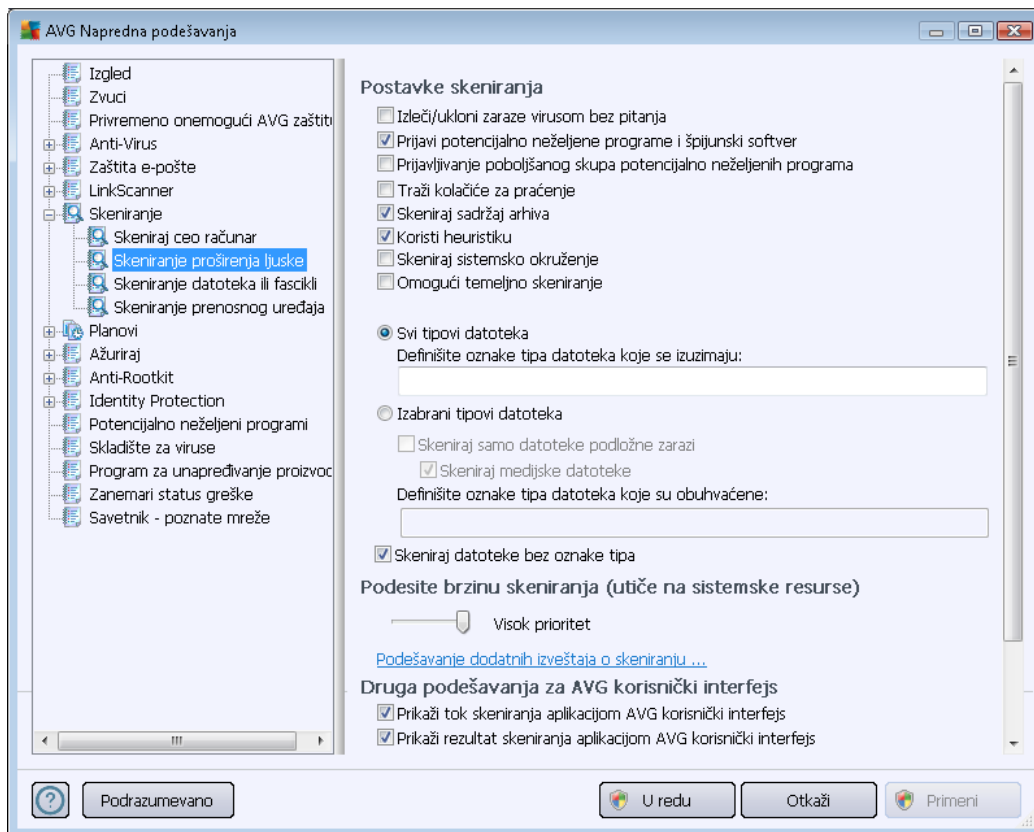
Podešavanje dodatnih izveštaja o skeniranju ...

Kliknite na link **Podešavanje dodatnih izveštaja o skeniranju ...** da biste otvorili samostalan dijalog po imenu **Izveštaji skeniranja** u kojem možete označiti nekoliko stavki kako biste definisali koji će se rezultati prijavljivati:



10.7.2. Skeniranje proširenja ljuske

Slično kao i prethodna stavka [Skeniraj ceo računar](#), stavka **Skeniranje proširenja ljuske** takođe nudi nekoliko opcija za uređivanje skeniranja koje je unapred definisano od strane proizvođača softvera. Ovog puta konfiguracija se odnosi na [skeniranje određenih objekata koji se pokreću direktno iz programa Windows Explorer](#) (*shell extension*), pogledajte poglavlje [Skeniranje u programu Windows Explorer](#):



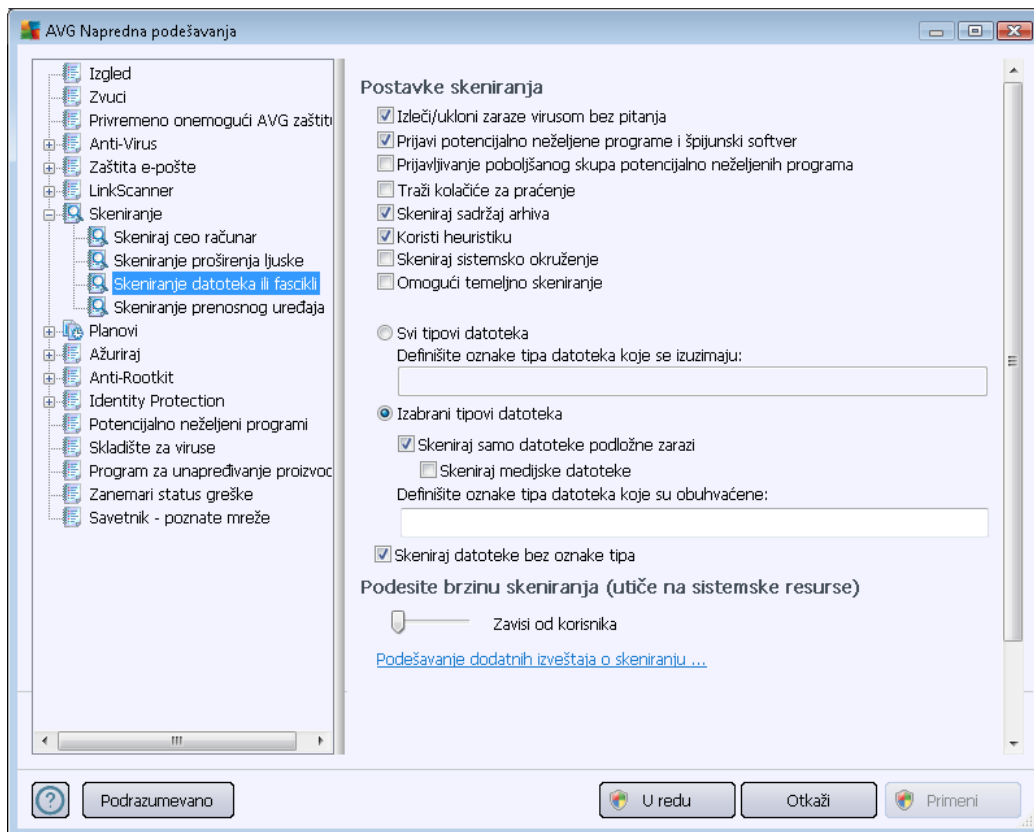
Lista parametara identična je listi koja je dostupna za opciju [Skeniranje celog računara](#). Međutim, podrazumevana podešavanja variraju (*na primer, skeniranje celog računara ne proverava podrazumevano arhive, ali skenira sistemsko okruženje, dok je sa skeniranjem proširenja ljuske stvar drugačija*).

Napomena: Opis pojedinačnih parametara potražite u poglavlju [AVG napredna podešavanja / Skeniranje / Skeniraj ceo računar](#).

U poređenju sa dijalogom [Skeniranje celog računara](#), dijalog **Skeniranje proširenja ljuske** uključuje i odeljak pod imenom **Ostale postavke u vezi sa AVG korisničkim interfejsom**, odakle možete navesti da li želite da se toku skeniranja i rezultatima skeniranja pristupa iz AVG korisničkog interfejsa. Takođe, možete definisati da se rezultati skeniranja prikazuju samo u slučaju ako je infekcija detektovana tokom skeniranja.

10.7.3. Skeniranje datoteka ili fascikli

Interfejs za uređivanje opcije **Skeniraj određene datoteke ili fascikle** isti je kao dijalog za uređivanje [Skeniraj ceo računar](#) opcije. Sve opcije za konfigurisanje su iste, ali su podrazumevane postavke strožije za [Skeniranje celog računara](#):

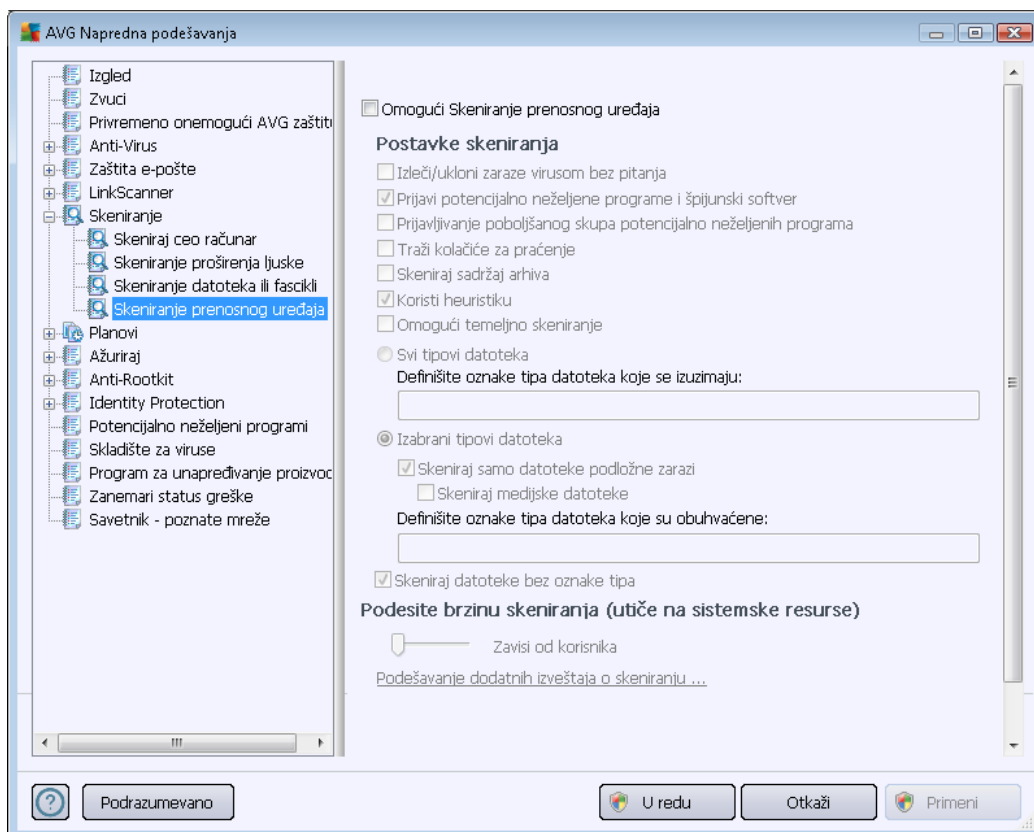


Svi parametri koji su definisani u ovom dijalogu za konfiguraciju odnose se samo na oblasti koje će se skenirati postavkom [Skeniraj određene datoteke ili fascikle!](#)

Napomena: Opis pojedinačnih parametara potražite u poglavlju [AVG napredna podešavanja / Skeniranje / Skeniraj ceo računar.](#)

10.7.4. Skeniranje prenosnog uređaja

Uređivački interfejs za **Skeniranje prenosnog uređaja** je vrlo sličan uređivačkom dijalogu [Skeniranja celog računara](#):



Funkcija **Skeniranje prenosnog uređaja** pokreće se automatski kada na računar povežete bilo koji prenosni uređaj. Podrazumevano, ovaj vid skeniranja je isključen. Međutim, od ključne je važnosti da se prenosni uređaji skeniraju u potrazi za pretnjama pošto oni predstavljaju jedan od najčešćih izvora zaraze. Da bi ovaj vid skeniranja bio u stanju pripravnosti i automatski se pokretao po potrebi, označite opciju **Skeniranje prenosnog uređaja**.

Napomena: Opis pojedinačnih parametara potražite u poglavlju [AVG napredna podešavanja / Skeniranje / Skeniraj ceo računar](#).

10.8. Planovi

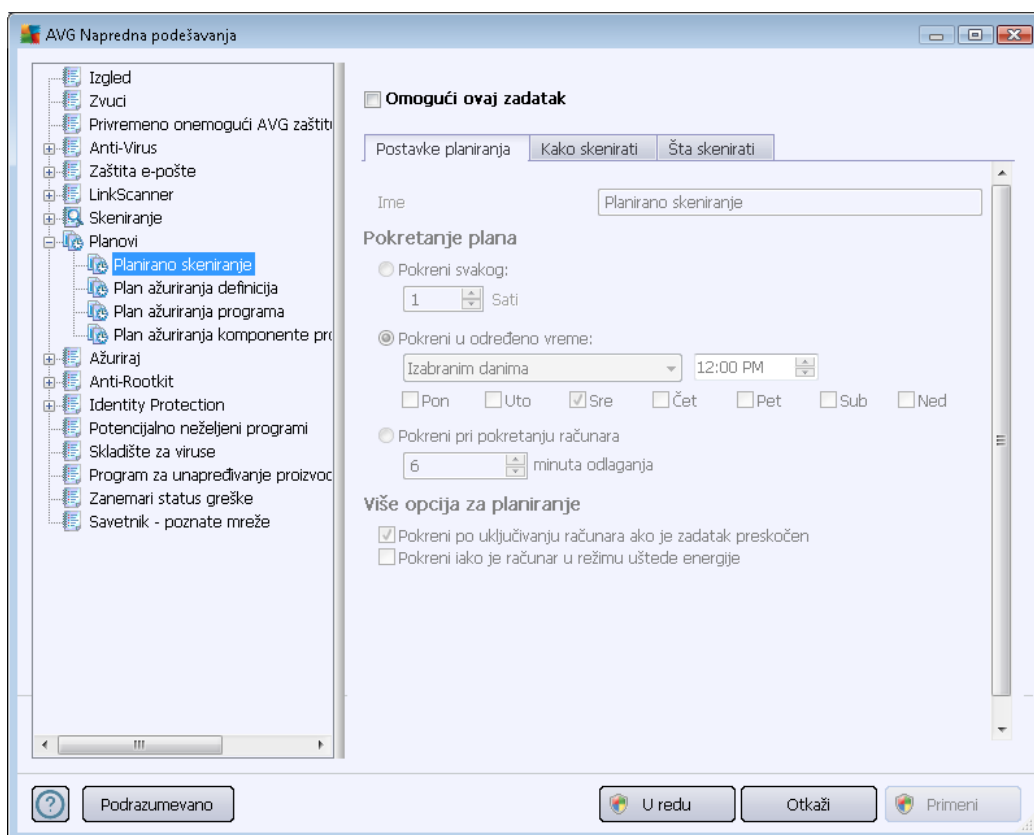
U odeljku **Planovi** možete urediti podrazumevane postavke za:

- [Planirano skeniranje](#)
- [Plan ažuriranja definicija](#)
- [Plan ažuriranja programa](#)

- [Plan ažuriranja komponente Odbrana od bezvredne pošte](#)

10.8.1. Planirano skeniranje

Parametri planiranog skeniranja mogu se uređivati (ili se može kreirati novi plan) na tri kartice. Na svakoj kartici možete prvo označiti/ponišiti izbor stavke **Omoгуći ovaj zadatak** da biste jednostavno deaktivirali zakazano skeniranje, a kasnije ga možete opet uključiti po potrebi:



U tekstualnom polju **Ime** (deaktivirano za sve podrazumevane planove) nalazi se ime koje je prodavac programa dodelio ovom planu. Ukoliko se radi o planovima koje ste naknadno dodali (novi plan možete dodati tako što ćete kliknuti desnim tasterom miša iznad stavke **Planirano skeniranje** u levom stablu za navigaciju), možete da definišete sopstveno ime i u tom slučaju tekstualno polje je moguće urediti. Koristite kratka, opisna i prikladna imena za skeniranja da biste ih kasnije lakše razlikovali.

Primer: Nije dobro nazvati skeniranje „Novo skeniranje“ ili „Moje skeniranje“, pošto ta imena ne opisuju ono što se tim skeniranjem proverava. S druge strane, primer dobrog opisanog imena bio bi „Skeniranje sistemskih oblasti“ itd. Takođe, nije obavezno da u imenu skeniranja navedete da li je u pitanju skeniranje celog računara ili samo određenih datoteka ili fascikli - vaši načini skeniranja uvek će predstavljati određenu verziju [skeniranja određenih datoteka ili fascikli](#).

U ovom dijalogu možete definisati sledeće parametre skeniranja:

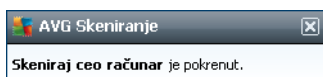


Pokretanje plana

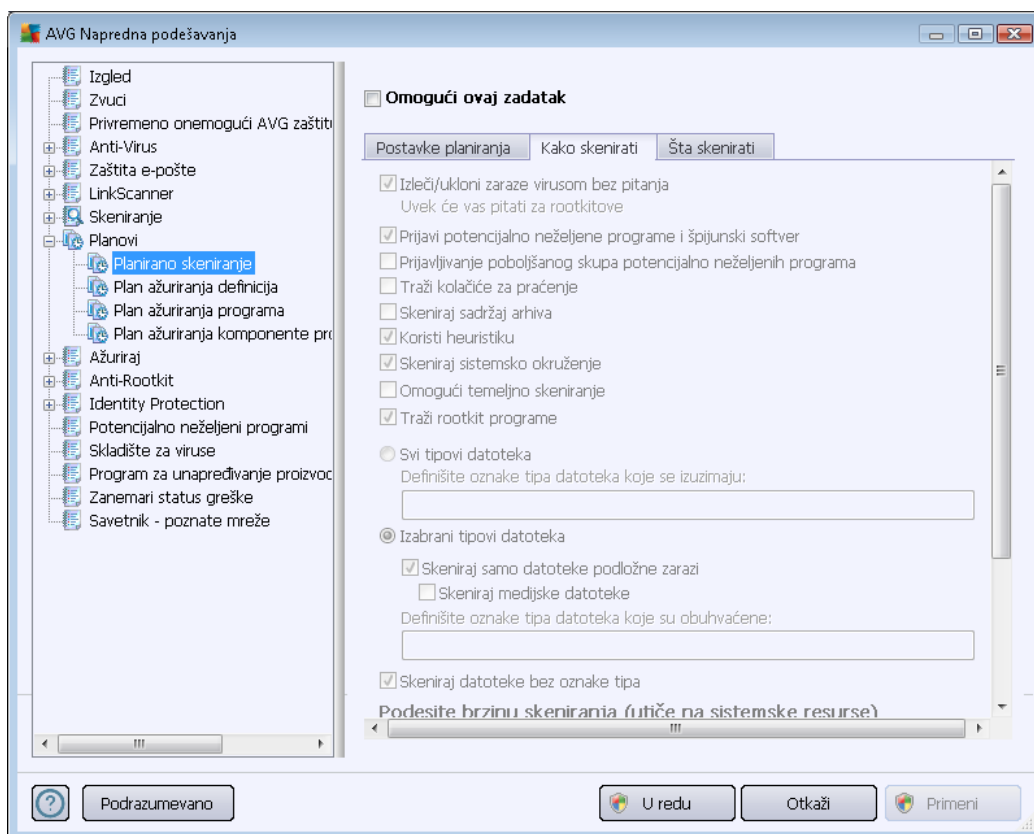
Ovde možete da navedete vremenske intervale za pokretanje novog planiranog skeniranja. Vremenski interval se može definisati po ponovljenom pokretanju skeniranja nakon određenog vremena (***Pokreni na svakih...***) ili definisanjem tačnog datuma i vremena (***Pokreni u određenom vremenskom intervalu...***) ili po mogućnosti definisanjem događaja sa kojim treba povezati pokretanje skeniranja (***Pokreni pri pokretanju računara***).

Napredne opcije za planiranje

U ovom odeljku možete definisati pod kojim se okolnostima skeniranje pokreće/ne pokreće ako je računar u režimu niske potrošnje energije ili je potpuno isključen. Kada se pokrene planirano skeniranje u navedenom vremenskom periodu, bićete obavešteni putem iskaćućeg prozora koji se otvorio iznad [AVG ikone na sistemskoj paleti](#):



Potom se pojavljuje nova [AVG ikona na sistemskoj traci](#) (u boji sa baterijskom lampom) koja vas obaveštava da je planirano skeniranje u toku. Kliknite desnim tasterom miša na ikonu pokrenutog AVG skeniranja da biste otvorili kontekstualni meni gde možete odlučiti da pauzirate ili čak i zaustavite pokrenuto skeniranje, a takođe i da promenite prioritet tekućeg skeniranja:



Na kartici **Kako skenirati** pronaći ćete listu parametara za skeniranje koje je moguće opcionalno uključiti ili isključiti. Većina parametara je podrazumevano uključena i primenjivaće se tokom skeniranja. **Ukoliko nemate određen razlog da promenite ta podešavanja, preporučuje se da zadržite unapred definisanu konfiguraciju:**

- **Izleći/ukloni virusnu infekciju bez upita** (podrazumevano uključeno): ako tokom skeniranja bude otkriven virus, moguće ga je automatski izlečiti ukoliko je dostupan lek. Ukoliko zaraženu datoteku nije moguće automatski izlečiti, ona će biti premeštena u [Skladište za viruse](#).
- **Prijavi potencijalno neželjene programe i pretnje špijunskog softvera** (podrazumevano uključeno): označite radi aktivacije [Antispajver](#) mehanizma, i skeniranja u potrazi za špijunskim programima, kao i virusima. Špijunski softver se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.
- **Prijavi poboljšani skup potencijalno neželjenih programa** (podrazumevano isključeno): označite radi detekcije proširenog paketa špijunskih programa: programi koji su potpuno u redu i bezopasni kada ih kupite direktno od proizvođača, ali se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.

- **Skeniraj kolačiće za praćenje** (podrazumevano isključeno): ovaj parametar komponente [Antispajver](#) definiše da bi tokom skeniranja trebalo otkrivati kolačiće; (*HTTP kolačići služe za proveru identiteta, praćenje, i održavanje određenih informacija o korisnicima, kao što su omiljene web lokacije ili sadržaj njihovih elektronskih korpi za kupovinu*)
- **Skeniraj unutar arhiva** (podrazumevano isključeno): ovim parametrom se definiše da bi skeniranje trebalo da obuhvati sve datoteke, čak i ako se one nalaze unutar arhive, npr. ZIP, RAR, ...
- **Koristi heuristiku** (podrazumevano uključeno): heuristička analiza (*dinamička emulacija naredbi skeniranih objekata u virtuelnom računarskom okruženju*) biće jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja.
- **Skeniraj sistemsko okruženje** (podrazumevano uključeno): skeniranje će obuhvatiti i sistemske oblasti vašeg računara;
- **Omogući temeljno skeniranje** (podrazumevano isključeno) - u posebnim situacijama (*ako sumnjate da je vaš računar zaražen*), možete označiti ovu opciju da aktivirate najtemeljnije algoritme za skeniranje, koji će skenirati čak i one oblasti na računaru koji se teško mogu zaraziti, radi predostrožnosti. Ipak, zapamtite da ovaj metod prilično dugo traje.
- **Skeniraj u potrazi za rootkit programima** (podrazumevano uključeno): [Anti-Rootkit](#) skeniranje na računaru pretražuje moguće rootkit programe, tj. programe i tehnologije koji mogu pokriti aktivnost malvera na računaru. Ako se otkrije rootkit program, to ne znači da je vaš računar zaražen. U nekim slučajevima, određeni upravljački programi ili delovi običnih aplikacija mogu biti pogrešno protumačeni kao rootkit programi.

Trebalo bi i da odlučite da li želite da skenirate

- **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka tako što ćete uneti listu oznaka tipa datoteka razdvojenih zarezima koje ne bi trebalo skenirati (*kada sačuvate listu, zarezi se pretvaraju u tačku i zarez*);
- **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteka možete označiti datoteke koje treba uvek skenirati.
- Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteka** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteka su sumnjive i treba ih uvek skenirati.

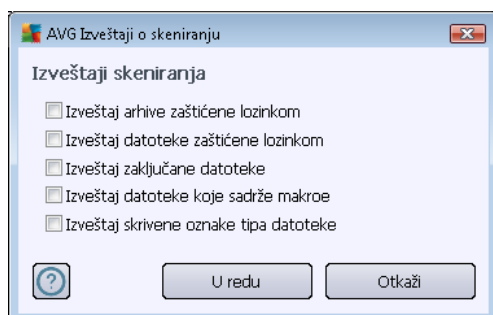
Podesite željenu brzinu završetka skeniranja

U odeljku **Podesite željenu brzinu završetka skeniranja** možete dalje odrediti željenu brzinu skeniranja, zavisno od iskorišćenosti kapaciteta sistema. Vrednost ove opcije podrazumevano je postavljena na nivo automatske zauzetosti resursa koja zavisi od korisnika. Ako želite da se

skeniranje obavlja brže, biće potrebno manje vremena, ali će se iskorišćenost sistemskih resursa značajno povećati tokom skeniranja, a to će usporiti ostale aktivnosti na računaru (*ovu opciju možete koristiti kada je računar uključen, ali niko ne radi na njemu*). Sa druge strane, iskorišćenost sistemskih resursa možete smanjiti tako što ćete produžiti trajanje skeniranja.

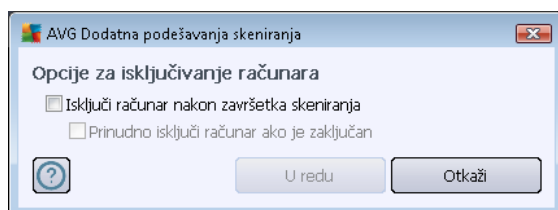
Podešavanje dodatnih izveštaja o skeniranju

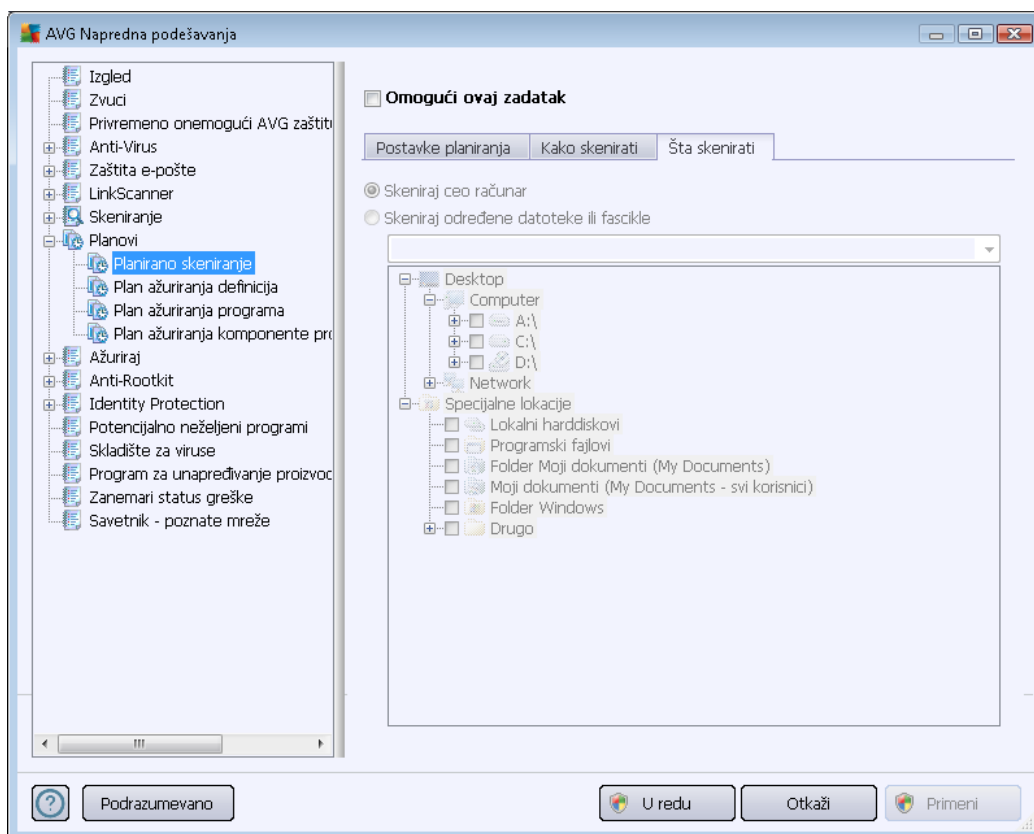
Kliknite na link **Podešavanje dodatnih izveštaja o skeniranju ...** da biste otvorili samostalan dijalog po imenu **Izveštaji skeniranja** u kojem možete označiti nekoliko stavki kako biste definisali koji će se rezultati prijavljivati:



Dodatna podešavanja skeniranja

Kliknite na **Dodatna podešavanja skeniranja ...** da biste otvorili novi dijalog **Opcije za isključivanje računara** u kojem možete izabrati da li će se računar automatski isključiti nakon što se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Isključi računar nakon završetka skeniranja**), aktiviraće se nova opcija koja omogućava da se računar isključi čak i ako je trenutno zaključan (**Prinudno isključi računar ako je zaključan**).

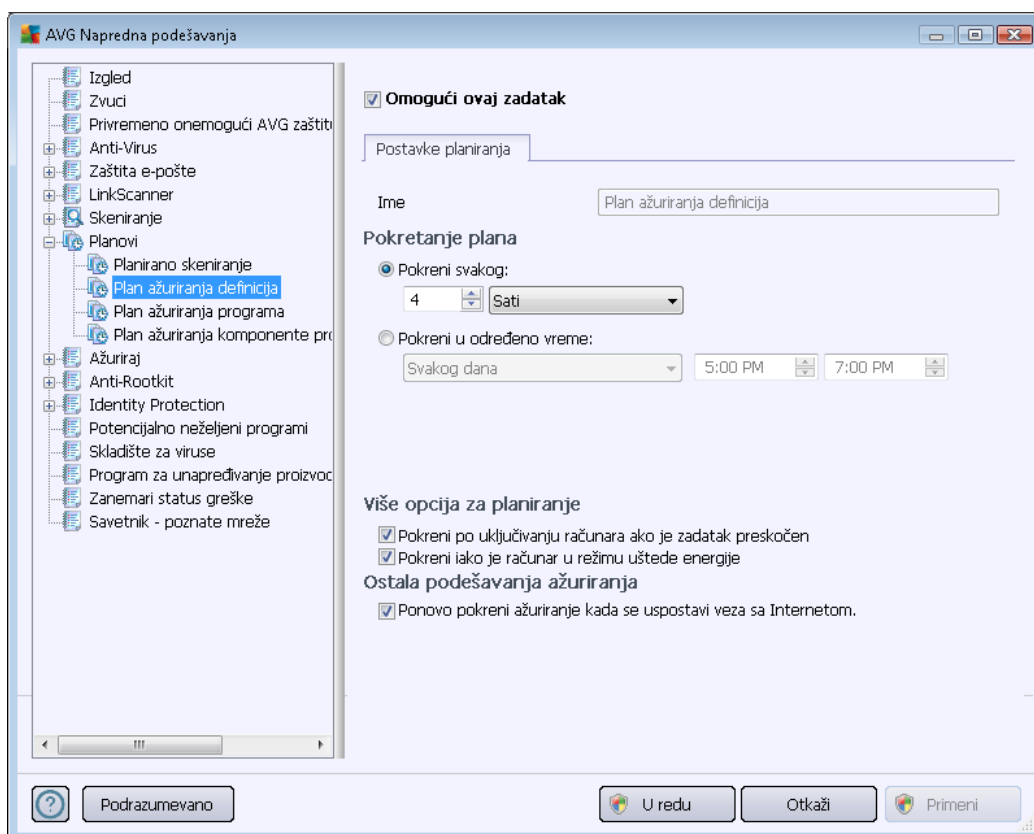




Na kartici **Šta skenirati**, možete definisati da li želite da zakažete [skeniranje celog računara](#) ili [skeniranje datoteka ili fascikli](#). Ako izaberete skeniranje datoteka ili fascikli, aktiviraće se struktura stabla u donjem delu dijaloga, pa možete navesti koje fascikle želite da skenirate.

10.8.2. Plan ažuriranja definicija

Ako je **zaista neophodno**, možete opozvati izbor stavke **Omogući ovaj zadatak** da biste jednostavno privremeno deaktivirali planirano ažuriranje definicija i kasnije ga ponovo uključili:



U ovom dijalogu možete podesiti neke detaljne parametre plana ažuriranja definicija. U tekstualnom polju **Ime** (*deaktivirano za sve podrazumevane planove*) nalazi se ime koje je prodavac programa dodelio ovom planu.

Pokretanje plana

U ovom odeljku navedite vremenske intervale za novo planirano pokretanje ažuriranja definicija. Tajming je moguće definisati uzastopnim pokretanjem ažuriranja nakon određenog vremenskog perioda (**Pokreni svakih ...**) ili definisanjem tačnog datuma i vremena (**Pokreni u određeno vreme ...**).

Više opcija za planiranje

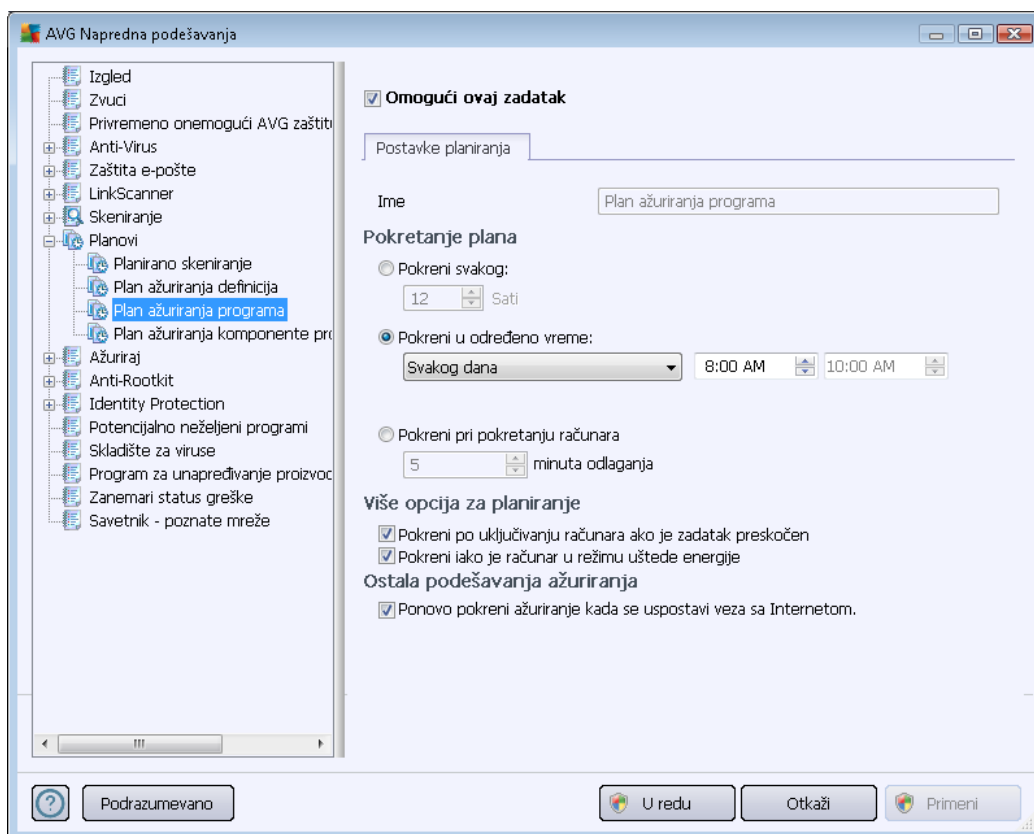
U ovom odeljku možete da definišete pod kojim okolnostima da se pokreće/ne pokreće ažuriranje definicija ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

Ostala podešavanja ažuriranja

Na kraju proverite opciju **Ponovo pokreni ažuriranje čim se uspostavi veza sa Internetom** da biste bili sigurni da će, ako dođe do prekida procesa ažuriranja usled prekida veze sa Internetom, taj proces biti odmah ponovo pokrenut nakon ponovnog uspostavljanja veze sa Internetom. Kada se pokrene planirano skeniranje u navedenom vremenskom periodu, bićete obavešteni putem iskaćueg prozora koji se otvorio iznad [AVG ikone na sistemskoj paleti](#) (pod uslovom da niste menjali podrazumevanu konfiguraciju u dijalogu [Napredna podešavanja/Izgled](#)).

10.8.3. Plan ažuriranja programa

Ako je **zaista neophodno**, možete opozvati izbor stavke **Omogući ovaj zadatak** da biste jednostavno privremeno deaktivirali planirano ažuriranje programa i kasnije ga ponovo aktivirali:



U tekstualnom polju **Ime** (deaktivirano za sve podrazumevane planove) nalazi se ime koje je prodavac programa dodelio ovom planu.

Pokretanje plana

Ovde navedite vremenski interval za pokretanje novog planiranog ažuriranja programa. Vremenski interval je moguće definisati uzastopnim pokretanjem skeniranja nakon određenog vremenskog perioda (**Pokreni svakih ...**), definisanjem tačnog datuma i vremena (**Pokreni u određeno vreme ...**).



) ili definisanjem događaja sa kojim bi trebalo povezati pokretanje skeniranja (***Radnja zasnovana na pokretanju računara***).

Više opcija za planiranje

U ovom odeljku možete da definišete pod kojim se okolnostima pokreće/ne pokreće ažuriranje programa ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

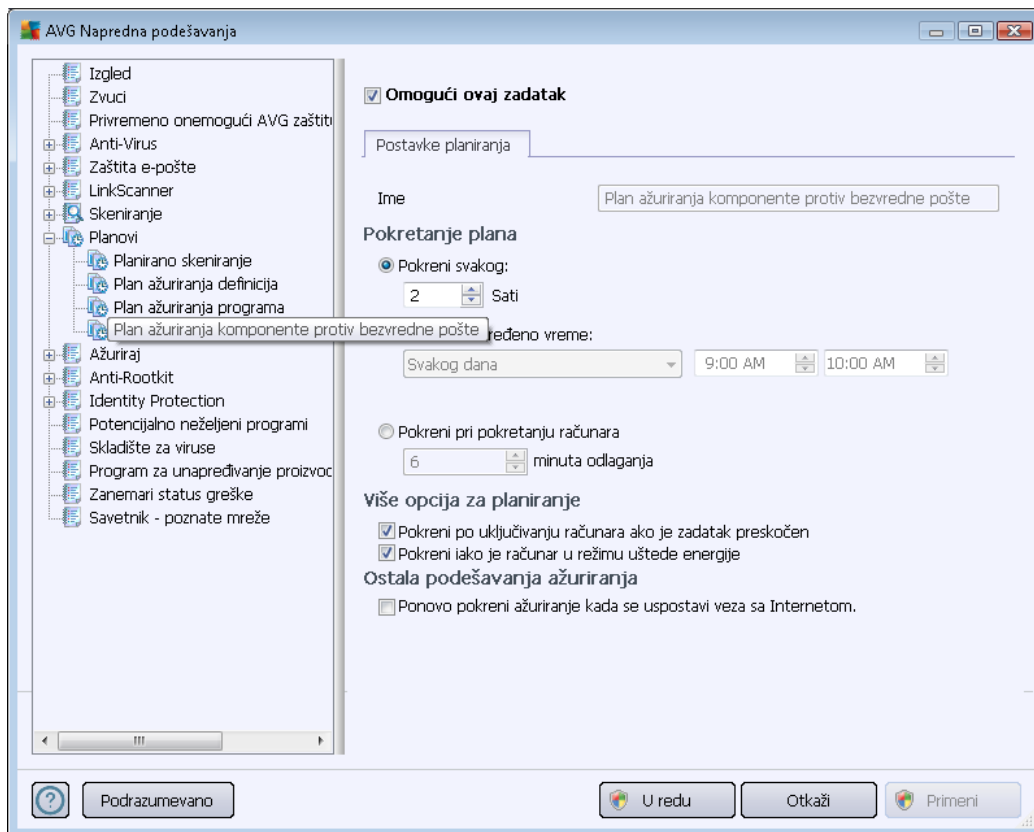
Ostala podešavanja ažuriranja

Izaberite opciju ***Ponovo pokreni ažuriranje čim se uspostavi veza sa Internetom*** da biste bili sigurni da će, ako dođe do prekida procesa ažuriranja usled prekida veze sa Internetom, taj proces biti odmah ponovo pokrenut nakon ponovnog uspostavljanja veze sa Internetom. Kada se pokrene planirano ažuriranje u navedenom vremenskom periodu, bićete obavešteni putem iskaćućeg prozora koji se otvara iznad [AVG ikone na sistemskoj paleti](#) (pod uslovom da niste menjali podrazumevanu konfiguraciju u dijalogu [Napredna podešavanja/Izgled](#)).

Napomena: Ako dođe do podudaranja u vremenu planiranog ažuriranja programa i planiranog skeniranja, proces ažuriranja ima veći prioritet pa će skeniranje biti prekinuto.

10.8.4. Plan ažuriranja Anti-Spam komponente

Ako je zaista neophodno, možete opozvati izbor stavke ***Omogući ovaj zadatak*** da biste jednostavno privremeno deaktivirali planirano ažuriranje [Odbrane od bezvredne pošte](#) i kasnije ga ponovo aktivirali:



U ovom dijalogu možete podesiti neke detaljne parametre planiranja ažuriranja. U tekstualnom polju **Ime** (*deaktivirano za sve podrazumevane planove*) nalazi se ime koje je prodavac programa dodelio ovom planu.

Pokretanje plana

Ovde navedite vremenske intervale za novo planirano pokretanje ažuriranja komponente [Odbrana od bezvredne pošte](#). Vremenski interval se može definisati kao redovno pokretanje ažuriranja komponente [Odbrana od bezvredne pošte](#) nakon izvesnog perioda (**Pokreni svakog ...**) ili pomoću tačnog datuma i vremena (**Pokreni u određeno vreme**), a možete i definisati događaj za koji sve vezuje pokretanje ažuriranja (**Radnja zasnovana na pokretanju računara**).

Više opcija za planiranje

U ovom odeljku možete da definišete pod kojim okolnostima da se pokreće/ne pokreće ažuriranje komponente [Odbrana od bezvredne pošte](#) ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

Ostala podešavanja ažuriranja

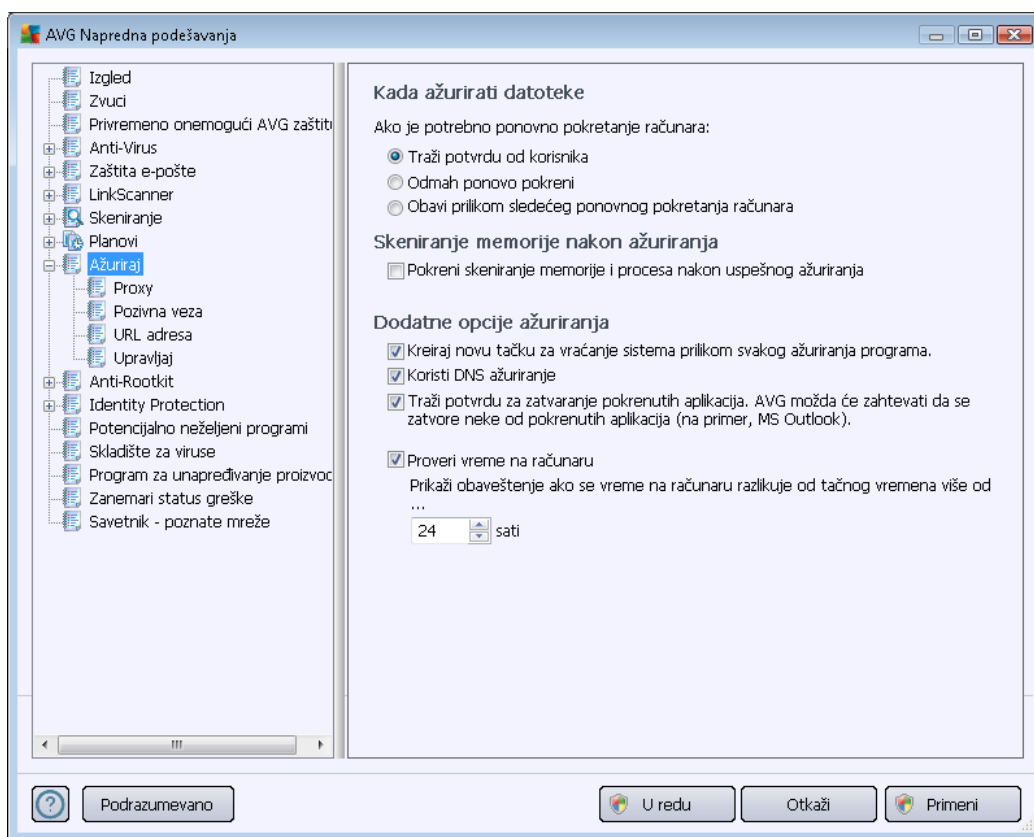


Izaberite opciju **Ponovo pokreni ažuriranje čim se uspostavi veza sa Internetom** da biste bili sigurni da će, ako dođe do prekida procesa ažuriranja komponente [Odbrana od bezvredne pošte](#) usled prekida veze sa Internetom, taj proces biti odmah ponovo pokrenut nakon ponovnog uspostavljanja veze sa Internetom.

Kada se pokrene planirano skeniranje u navedenom vremenskom periodu, bićete obavešteni putem iskašućeg prozora koji se otvorio iznad [AVG ikone na sistemskoj paleti](#) (pod uslovom da niste menjali podrazumevanu konfiguraciju u dijalogu [Napredna podešavanja/Izgled](#)).

10.9. Ažuriranje

Stavka za navigaciju **Ažuriraj** otvara novi dijalog u kojem možete definisati opšte parametre u vezi sa [ažuriranjem programa AVG](#):



Kada ažurirati datoteke

U ovom odeljku možete izabrati neku od tri opcije koje će se koristiti u slučaju da proces ažuriranja zahteva ponovno pokretanje računara. Dovršavanje ažuriranja možete zakazati za sledeće pokretanje računara ili možete odmah ponovo pokrenuti računar:

- **Zahtevaj potvrdu od korisnika** (podrazumevano) - od vas će se tražiti da odobrite ponovno pokretanje računara, koje je potrebno za završetak [procesa](#) ažuriranja



- **Ponovo pokreni odmah** - računar će se automatski odmah ponovo pokrenuti kada se proces [ažuriranja](#) završi i vaše odobrenje neće biti potrebno
- **Dovrši pri sledećem ponovnom pokretanju računara** - završetak procesa [ažuriranja](#) će biti odložen do sledećeg ponovnog pokretanja računara. Imajte u vidu da se ova opcija preporučuje samo ako ste sigurni da se računar redovno ponovo pokreće, najmanje jednom dnevno!

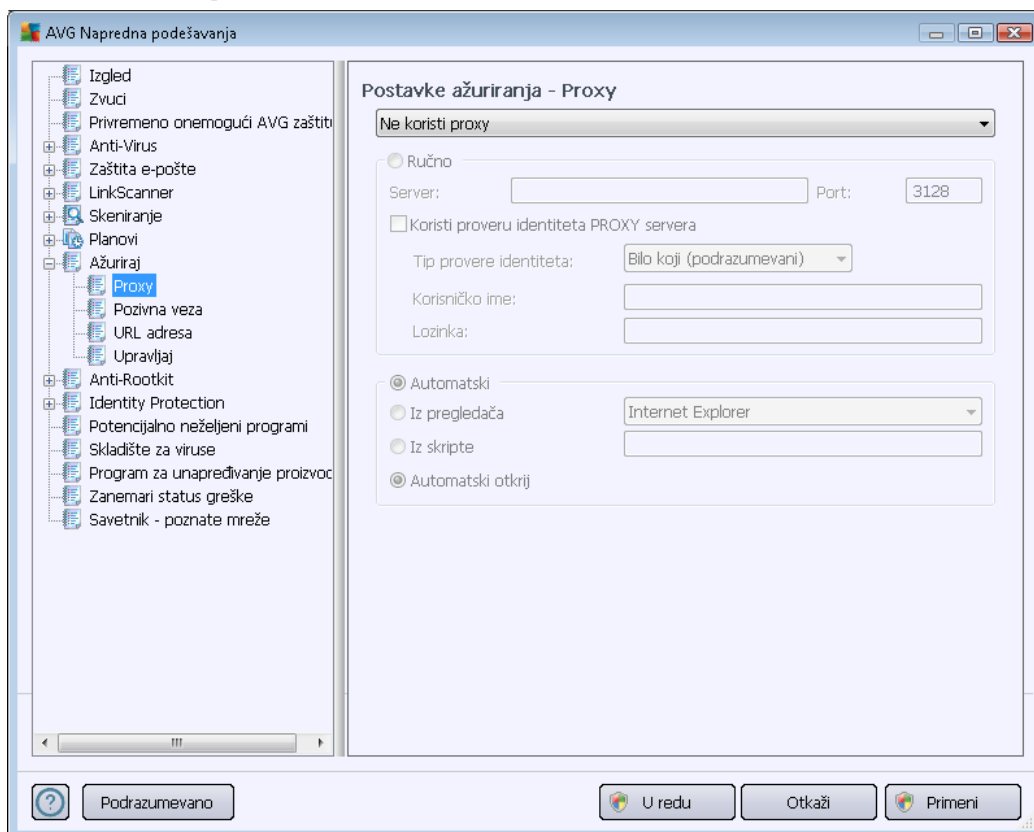
Skeniranje memorije nakon ažuriranja

Označite izbor u ovom polju za potvrdu ako želite da se novo skeniranje memorije pokreće nakon svakog uspešnog ažuriranja. Najnovija preuzeta ispravka možda sadrži nove definicije virusa i one se mogu odmah primeniti tokom skeniranja.

Dodatne opcije ažuriranja

- **Kreiraj novu tačku za vraćanje sistema nakon svakog ažuriranja programa** - pre svakog pokretanja ažuriranja programa AVG, kreira se tačka za vraćanje sistema. Ako proces ažuriranja ne uspe i dođe do pada operativnog sistema, možete ga uvek vratiti u stanje prvobitne konfiguracije. Ovoj opciji možete pristupiti ako kliknete na Start / Svi programi / Pribor / Sistemske alate / Oporavak sistema, ali se ne preporučuje da unosite izmene, osim ako niste iskusan korisnik! Neka ovo polje za potvrdu ostane označeno ako želite da koristite ovu funkciju.
- **Koristi DNS ažuriranje (podrazumevano uključeno)** – ako je označen izbor u ovom polju za potvrdu, nakon pokretanja ažuriranja **AVG Internet Security 2012** traži informacije o najnovijoj bazi podataka o virusima i najnovijoj verziji programa na DNS serveru. Zatim se preuzimaju i primenjuju samo najmanje neophodne datoteke za ažuriranje. Na taj način smanjuje se ukupna količina podataka za preuzimanje i proces ažuriranja traje kraće.
- **Traži potvrdu za zatvaranje pokrenutih aplikacija (podrazumevano je uključeno)** - izborom ove opcije bićete sigurni da AVG neće bez vašeg odobrenja zatvarati trenutno pokrenute aplikacije - ako je to potrebno da bi se završio proces ažuriranja.
- **Proveri vreme na računaru** - označite ovu opciju ako želite da se prikazuje obaveštenje ako se vreme podešeno na računaru razlikuje od tačnog vremena za više od podešenog broja sati.

10.9.1. Proxy



Proxy server je samostalni server ili usluga koja radi na računarima i garantuje bezbedniju vezu sa Internetom. U skladu sa navedenim mrežnim pravilima, možete da pristupite Internetu direktno ili preko proxy servera. Obe mogućnosti takođe mogu da budu istovremeno dozvoljene. Zatim u prvoj stavki u dijalogu **Podešavanja ažuriranja - Proxy** iz padajućeg menija morate da izaberete jednu od sledećih opcija:

- **Koristi proxy**
- **Ne koristi proxy** - podrazumevane postavke
- **Pokušaj da uspostaviš vezu pomoću proxy servera. U slučaju neuspeha, uspostavi vezu direktno**

Ako izaberete neku opciju koja podrazumeva upotrebu proxy servera, moraćete da unesete dodatne podatke. Podešavanje servera moguće je podesiti ručno ili automatski.

Ručno podešavanje

Ako izaberete ručno podešavanje (uključite opciju **Ručno** da biste aktivirali odgovarajući odeljak dijaloga) morate podesiti sledeće stavke:



- **Server** – navedite IP adresu servera ili ime servera
- **Port** – navedite broj porta koji omogućava pristup Internetu (*po podrazumevanoj vrednosti, ovaj broj je podešen na 3128, ali se može drugačije postaviti – obratite se administratoru mreže ako niste sigurni*)

Proxy server takođe može da ima konfigurisana određena pravila za svakog korisnika. Ako je vaš proxy server podešen na ovaj način, uključite opciju **Koristi proveru identiteta PROXY servera** da biste proverili da li su vaše korisničko ime i lozinka važeći za povezivanje na Internet pomoću proxy servera.

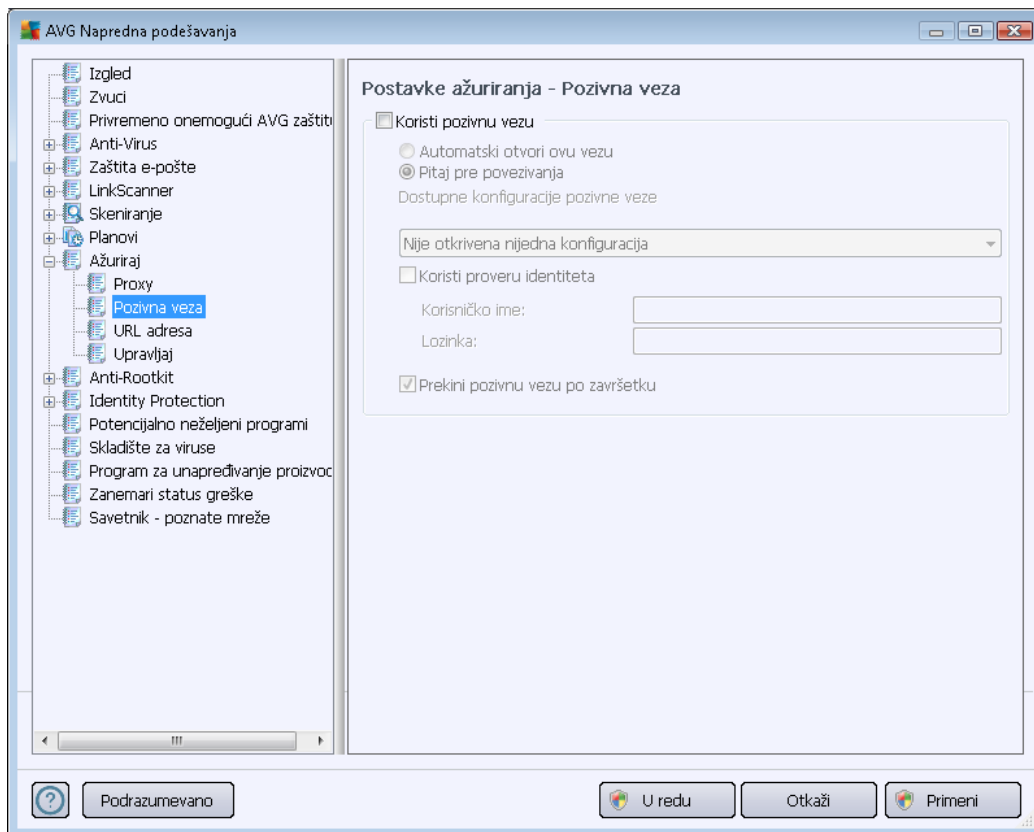
Automatsko podešavanje

Ako izaberete automatsko podešavanje (*uključite opciju **Automatski** da biste aktivirali odgovarajući odeljak dijaloga*), a zatim izaberite odakle bi trebalo preuzeti konfiguraciju proxy servera:

- **Iz pregledača** - konfiguracija će biti preuzeta iz podrazumevanog Internet pregledača
- **Iz skripte** - konfiguracija će biti preuzeta iz preuzete skripte koja sadrži funkciju davanja adrese proxy servera
- **Automatski otkrij** - konfiguracija će biti automatski otkrivena direktno sa proxy servera

10.9.2. Pozivna veza

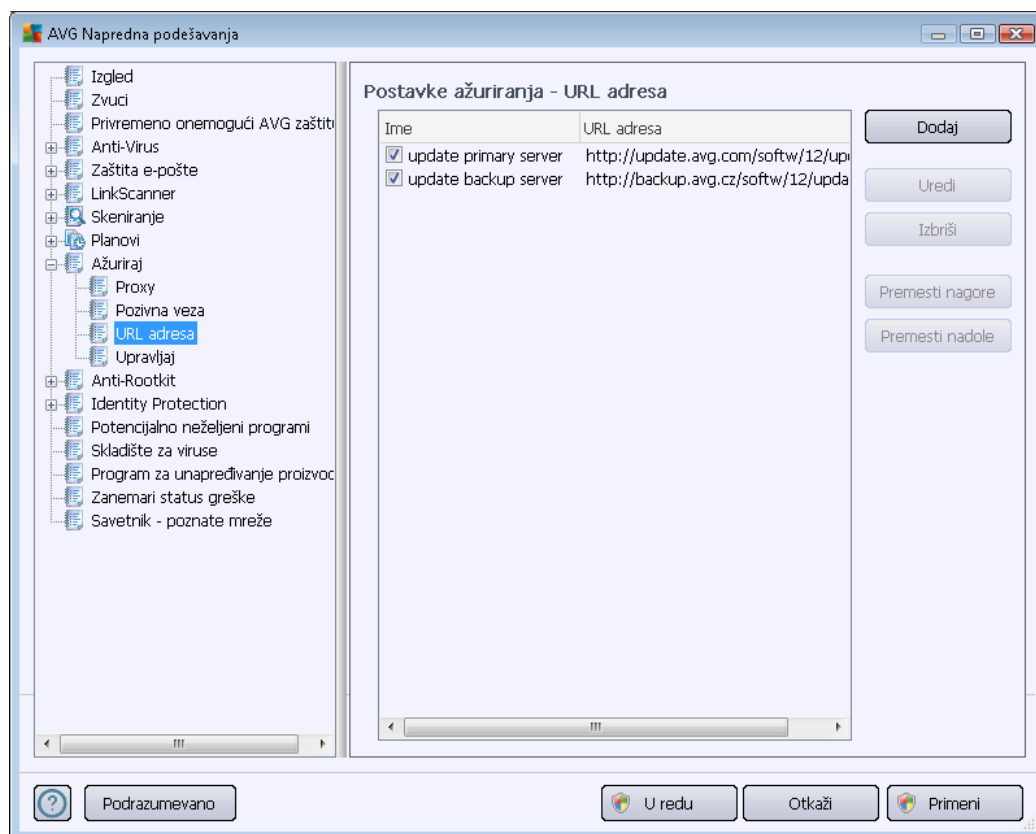
Svi parametri koji su opcionalno definisani u dijalogu **Postavke ažuriranja - Pozivna veza** odnose se na pozivnu vezu sa Internetom. Polja na kartici nisu aktivna dok ne označite opciju **Koristi pozivne veze** koja aktivira polja:



Navedite da li želite da se automatski povežete sa Internetom (***Automatski otvori ovu vezu***) ili želite da svaki put ručno potvrdite vezu (***Pitaj pre povezivanja***). Kod automatskog povezivanja, potrebno je još da izaberete da li će se veza prekidati nakon završetka ažuriranja (***Prekini pozivnu vezu po završetku***).

10.9.3. URL adresa

Dijalog **URL** nudi listu Internet adresa sa kojih se mogu preuzeti datoteke ažuriranja:



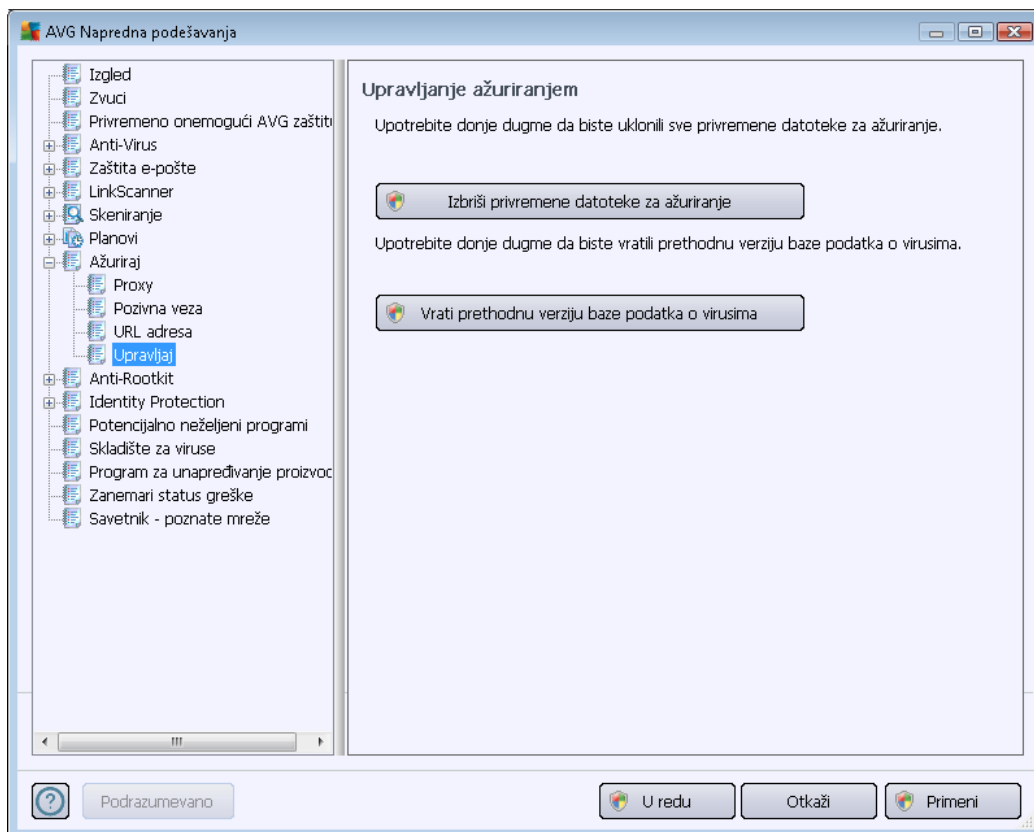
Kontrolna dugmad

Ova lista i njene stavke mogu se izmeniti pomoću sledeće kontrolne dugmadi:

- **Dodaj** – otvara dijalog u kojem možete da navedete novu URL adresu koja će biti dodata na listu
- **Uredi** - otvara dijalog u kojem možete da uredite izabrane parametre URL adrese
- **Izbriši** – briše izabranu URL adresu sa liste
- **Premesti nagore** – premešta izabranu URL adresu nagore za jedno mesto na listi
- **Premesti nadole** – premešta izabranu URL adresu nadole za jedno mesto na listi

10.9.4. Upravljanje

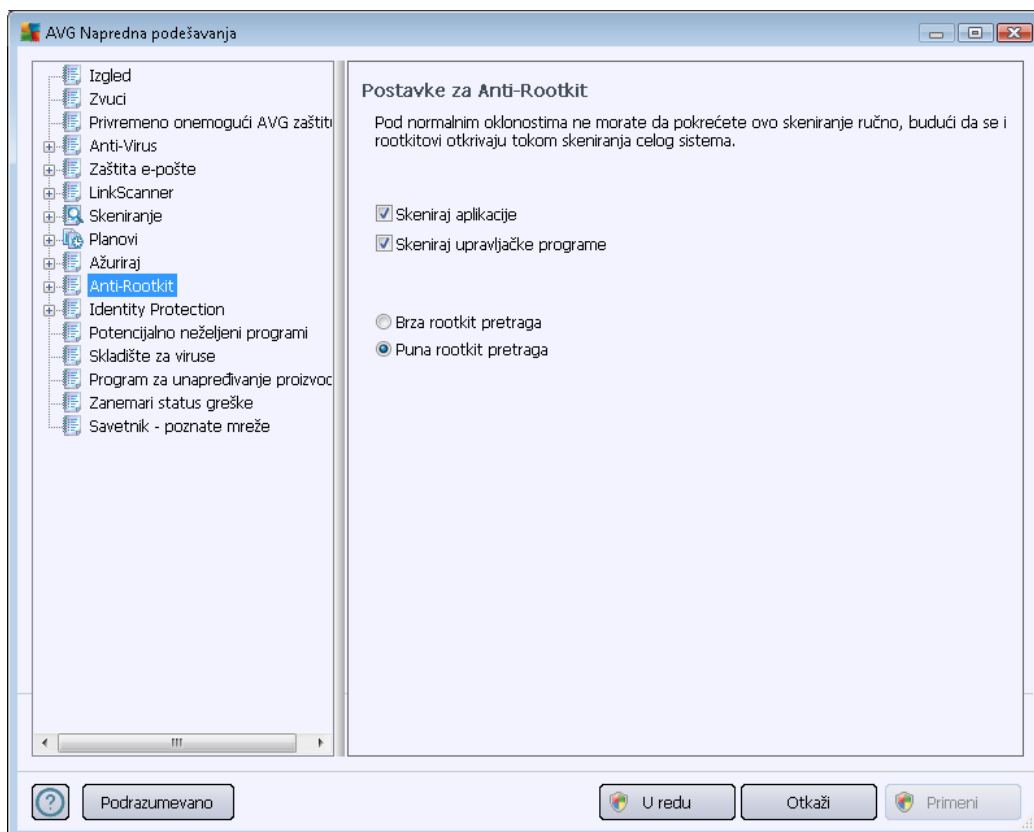
Dijalog **Upravljanje ažuriranjem** nudi dve opcije kojima se pristupa putem dva dugmeta:



- **Izbriši privremene datoteke za ažuriranje** - pritisnite ovo dugme da biste izbrisali sve nepotrebne datoteke za ažuriranje sa čvrstog diska (*podrazumevano, te datoteke se čuvaju 30 dana*)
- **Vrati prethodnu verziju baze podataka o virusima** – kliknite na ovo dugme da biste izbrisali najnoviju verziju baze podataka o virusima sa čvrstog diska i da biste se vratili na prethodno sačuvanu verziju (*nova verzija baze podataka o virusima preuzeće se prilikom sledećeg ažuriranja*)

10.10. Anti-Rootkit

U dijalogu **Anti-Rootkit podešavanja** možete da uredite konfiguraciju [Anti-Rootkit](#) komponente i određene parametre anti-rootkit skeniranja. Anti-rootkit skeniranje je podrazumevani proces uključen u [skeniranje celog računara](#):



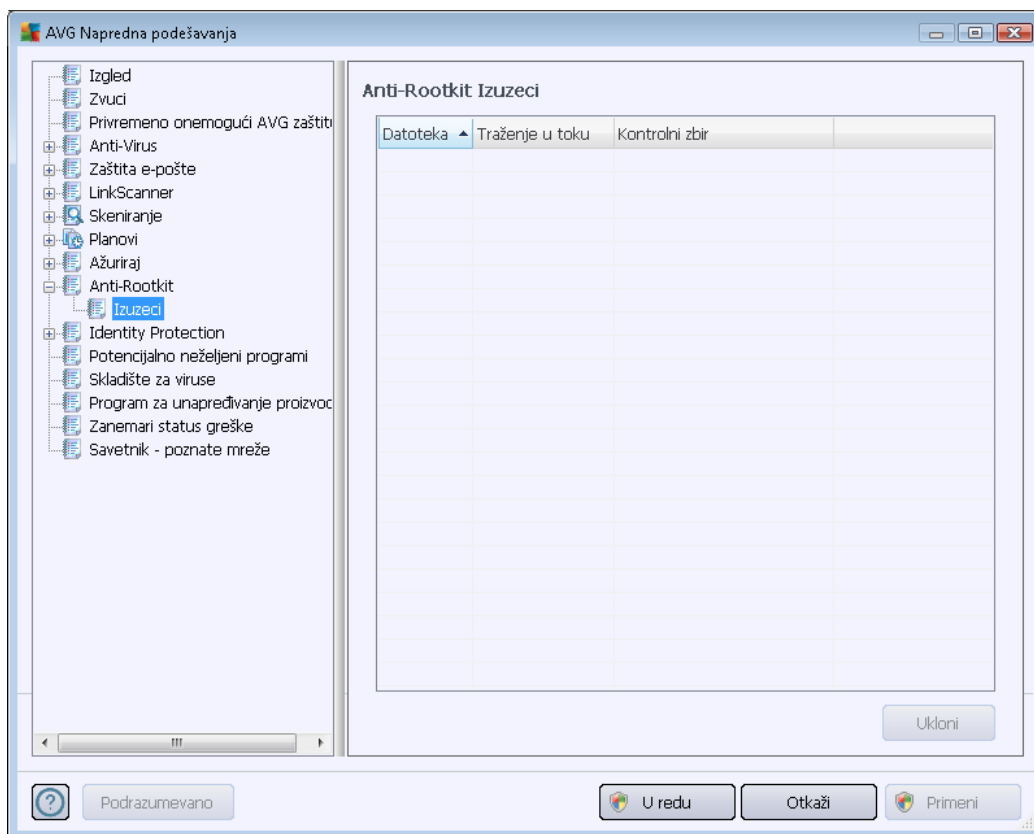
Uređivanju svih funkcija komponente [Anti-Rootkit](#) navedenih u ovom dijalogu može da se pristupi i direktno iz [interfejsa komponente Anti-Rootkit](#).

Opcije **Skeniraj aplikacije** i **Skeniraj upravljačke programe** omogućavaju vam da detaljno odredite šta će biti obuhvaćeno anti-rootkit skeniranjem. Ove postavke su namenjene za napredne korisnike; preporučujemo da sve opcije ostavite uključene. Zatim možete da izaberete režim rootkit skeniranja:

- **Brzo rootkit skeniranje** - skeniranje svih aktivnih procesa, učitanih upravljačkih programa i sistemske fascikle (*obično c:\Windows*)
- **Potpuno rootkit skeniranje** - skeniranje svih aktivnih procesa, učitanih upravljačkih programa, sistemske fascikle (*obično c:\Windows*), kao i svih lokalnih diskova (*uključujući fleš disk, ali izuzimajući disketnu/CD jedinicu*)

10.10.1. Izuzeci

U okviru dijaloga **Anti-Rootkit izuzeci** možete da definišete određene datoteke (*npr. neke upravljačke programe koji su možda pogrešno otkriveni kao rootkit*) koje treba izuzeti iz ovog skeniranja:

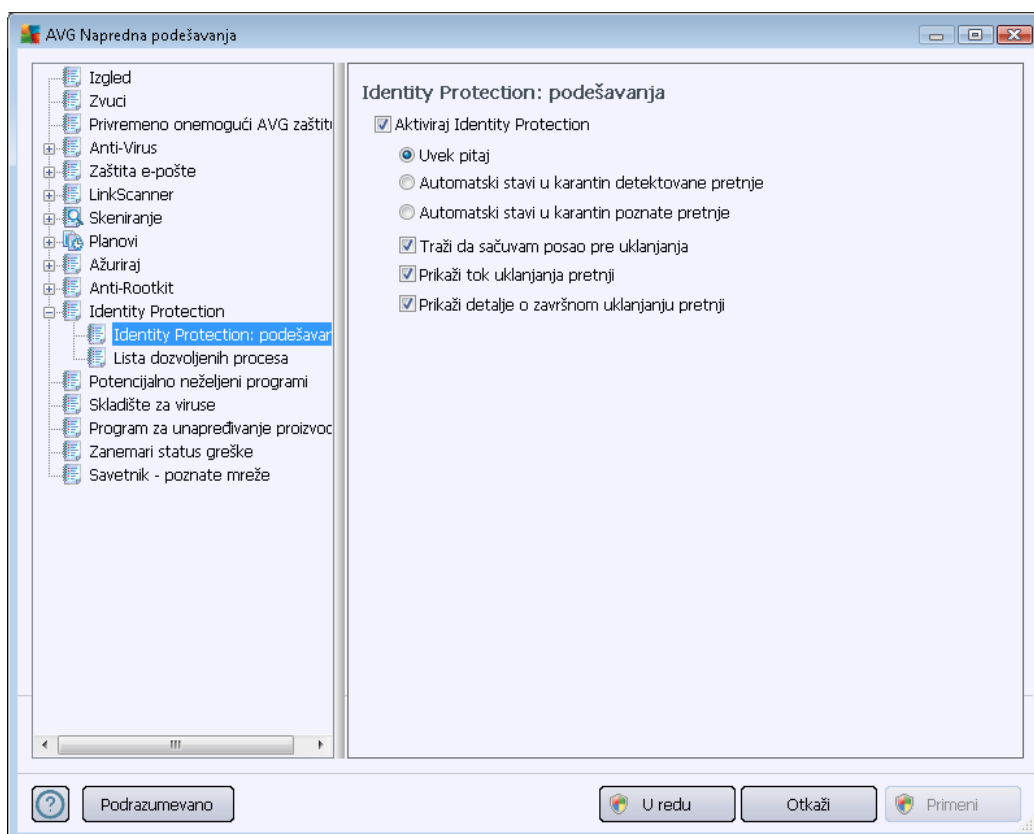


10.11. Identity Protection

Identity Protection je komponenta za zaštitu od malvera koja vas pomoću tehnologija ponašanja štiti od svih vrsta malvera (*špijunski softver, botovi, krađa identiteta...*) i obezbeđuje zaštitu od nepredviđenih napada novih virusa (*detaljan opis funkcionalnosti komponente potražite u poglavlju [Identity Protection](#)*).

10.11.1. Postavke zaštite identiteta

Dijalog **Postavke zaštite identiteta** vam omogućava da uključite/isključite osnovne funkcije komponente [Identity Protection](#):



Aktiviraj zaštitu identiteta (podrazumevano uključeno) - opozovite ovo polje radi isključivanja komponente [Zaštite identiteta](#).

Preporučujemo vam da to ne činite, osim ako nije neophodno!

Kada je komponenta [Identity Protection](#) aktivirana, možete da navedete radnju koja će se preduzeti kada se otkrije pretnja:

- **Uvek pitaj** (podrazumevano je uključeno) - kadase detektuje pretnja, od vas će se tražiti da odlučite da li želite da je premestite u karantin kako biste bili sigurni da nijedna aplikacija koju želite da pokrenete neće biti uklonjena.
- **Automatski stavi u karantin detektovane pretnje** – potvrdite izbor u ovom polju za potvrdu ako želite da sve potencijalne pretnje odmah premestite na sigurno mesto, odnosno [skladište za viruse](#). Ako zadržite podrazumevane postavke i ukoliko se otkrije pretnja, od vas će se tražiti da odlučite da li želite da je premestite u karantin kako biste bili sigurni da nijedna aplikacija koju želite da pokrenete neće biti uklonjena.
- **Automatski stavi u karantin poznate pretnje** – ne opozivajte izbor u ovom polju za potvrdu ako želite da se sve aplikacije koje su detektovane kao potencijalni malver automatski



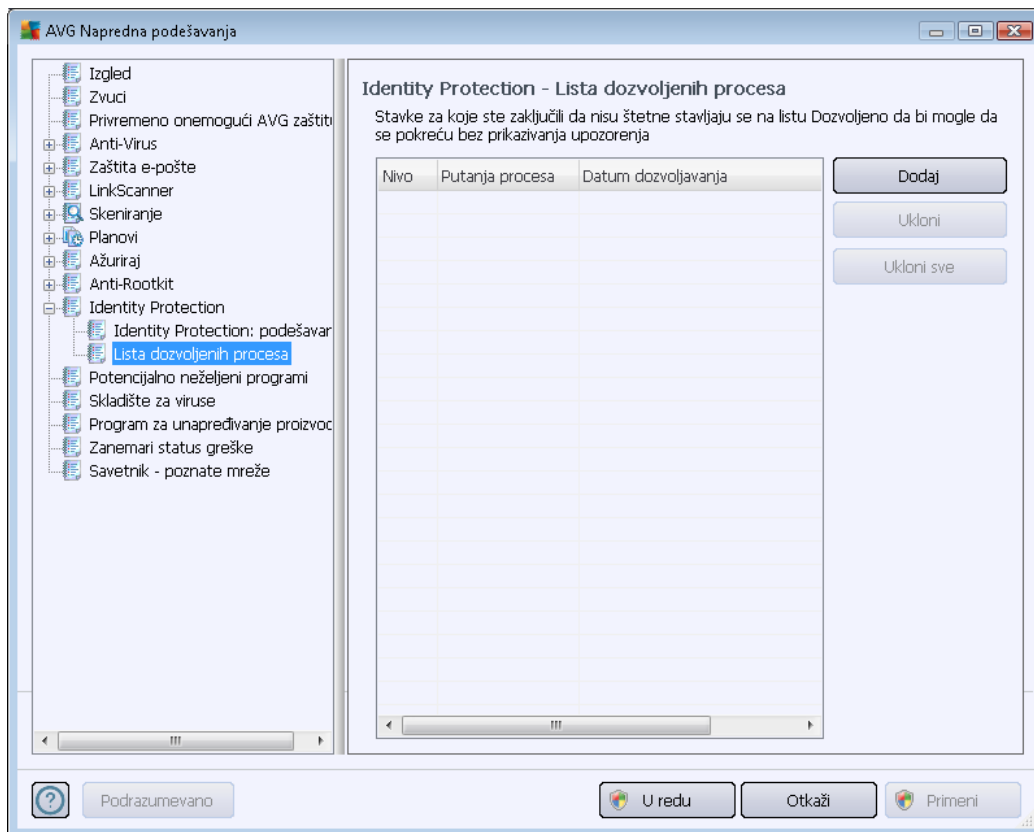
smeštaju u [skladište za viruse](#).

Osim toga, možete da izaberete i dodatne stavke kako biste opcionalno aktivirali još funkcija komponente [Identity Protection](#):

- **Pitaj da sačuvaš svoj rad pre nego što se ukloni** - (podrazumevano je isključeno) - ne opozivajte izbor u ovom polju za potvrdu ako želite da budete upozoreni pre nego što se aplikacija detektovana kao potencijalni malver stavi u karantin. Ukoliko radite samo sa aplikacijom, vaš projekat će možda biti izgubljen i potrebno je da ga prvo sačuvate. Ova stavka je podrazumevano uključena i preporučujemo vam da je ne isključujete.
- **Prikaži tok uklanjanja pretnji** - (podrazumevano je uključeno) - ako je ova stavka uključena, kada se detektuje potencijalni malver, otvoriće se novi dijalog u kojem se prikazuje tok uklanjanja malvera i njegovog stavljanja u karantin.
- **Prikaži završne detalje o uklanjanju pretnji** - (podrazumevano je uključeno) - ako je ova stavka uključena, komponenta **Identity Protection** će prikazivati detaljne informacije o svakom objektu stavljenom u karantin (*nivo ozbiljnosti, lokacija itd.*).

10.11.2. Lista „Dozvoljeno“

Ako u dijalogu **Postavke zaštite identiteta** niste potvrdili izbor u polju za potvrdu **Automatski stavi u karantin otkrivene pretnje**, svaki put kada se otkrije potencijalno opasan malver od vas će se tražiti da odlučite da li želite da ga uklonite. Ako zatim označite sumnjivu aplikaciju (*otkrivenu na osnovu njenog ponašanja*) kao bezbednu i potvrdite da je treba zadržati na računaru, aplikacija će biti dodata na takozvanu listu **Dozvoljena Identity Protection** i više se neće prijavljivati kao potencijalno opasna:



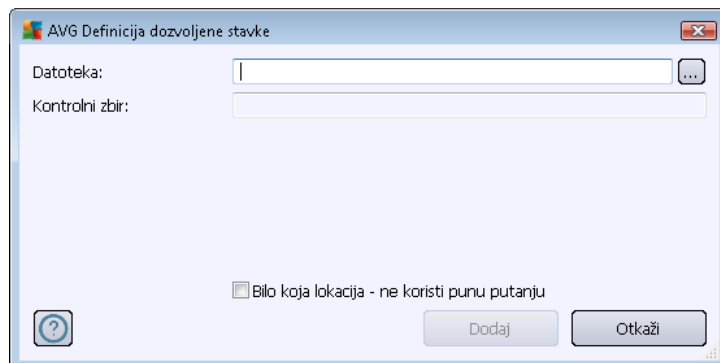
Lista **Dozvoljena Identity Protection** pruža sledeće informacije o svakoj aplikaciji:

- **Nivo** - grafički prikaz ozbiljnosti odgovarajućeg procesa na skali od četiri nivoa, od manje ozbiljne pretnje (■□□□) pa do veoma ozbiljne (■■■■)
- **Putanja procesa** - putanja do lokacije na kojoj se nalazi izvršna datoteka aplikacije (procesa)
- **Datum dozvoljavanja** - datum kada ste ručno označili aplikaciju kao bezbednu

Kontrolna dugmad

U dijalogu **Identity Protection - Lista dozvoljenih procesa** nalaze se sledeća kontrolna dugmad:

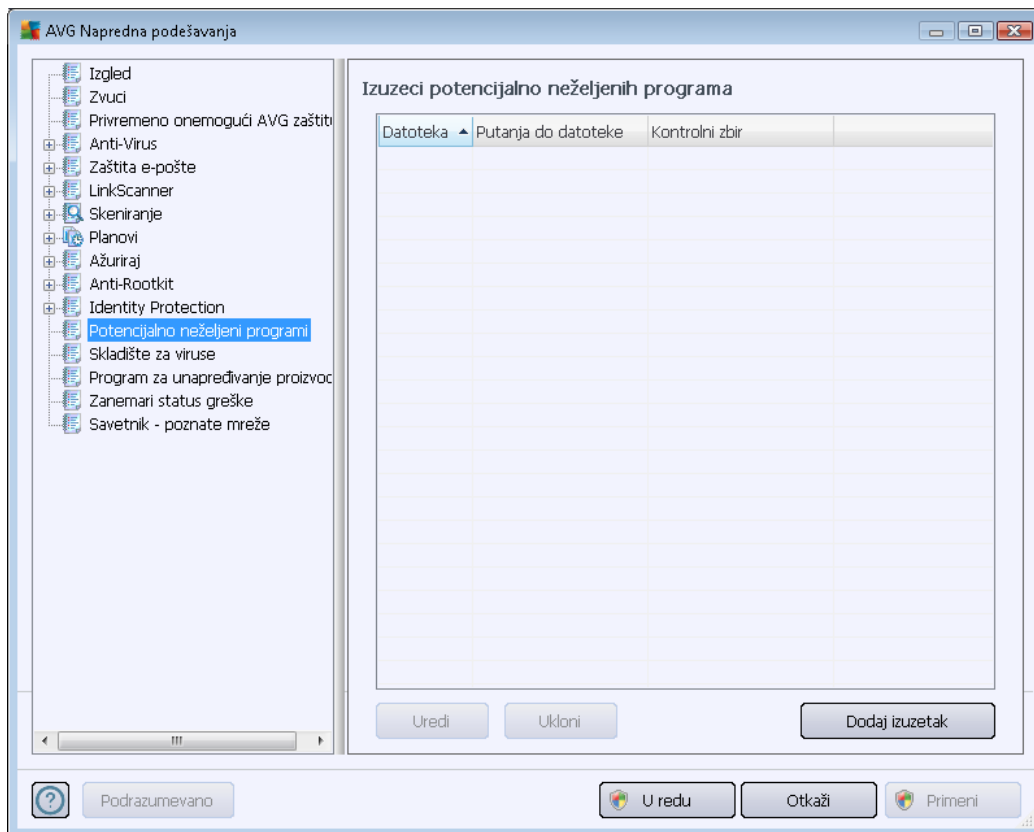
- **Dodaj** - kliknite na ovo dugme da biste dodali novu aplikaciju na listu dozvoljenih aplikacija. Pojaviće se sledeći dijalog:



- **Datoteka** - upišite punu putanju do datoteke (*aplikacije*) koju želite da označite kao izuzetak
 - **Kontrolni zbir** - prikazuje jedinstveni „potpis“ izabrane datoteke. Kontrolni zbir je automatski generisana niska znakova koja dozvoljava AVG programu da nedvosmisleno razlikuje odabranu datoteku od drugih datoteka. Kontrolni zbir se generiše i prikazuje nakon uspešnog dodavanja datoteke.
 - **Bilo koja lokacija - ne koristi punu putanju** - ako želite da definišete ovu datoteku kao izuzetak samo za određenu lokaciju, onda nemojte označiti izbor u ovom polju za potvrdu
- **Ukloni** - kliknite na ovo dugme da biste izabranu aplikaciju uklonili sa liste
 - **Ukloni sve** - kliknite na ovo dugme da biste sa liste uklonili sve aplikacije

10.12. Potencijalno neželjeni programi

AVG Internet Security 2012 može da analizira i otkrije izvršne aplikacije ili DLL biblioteke koje mogu da budu potencijalno neželjene u okviru sistema. U nekim slučajevima korisnik će možda želeći da zadrži određene neželjene programe na računaru (programe koji su namerno instalirani). Neki programi, naročito oni besplatni, sadrže adver. **AVG Internet Security 2012** može otkriti i prijaviti takav adver kao *potencijalno neželjeni program*. Ako takav program želite da zadržite na računaru, možete da ga definišete kao izuzetak potencijalno neželjenih programa:

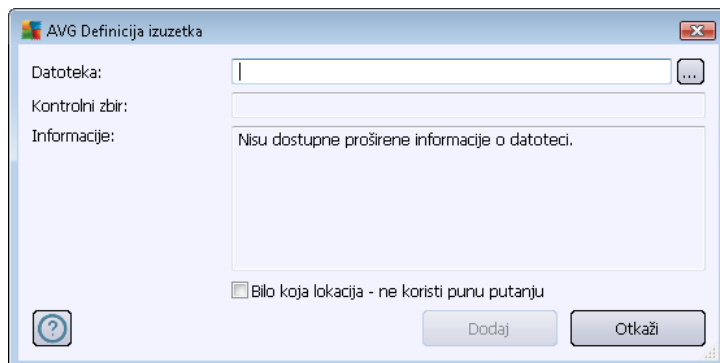


U dijalogu ***Izuzeci potencijalno neželjenih programa*** nalazi se lista već definisanih i važećih izuzetaka potencijalno neželjenih programa. Listu možete da uredite, kao i da izbrišete postojeće stavke ili da dodate nove izuzetke. Na listi se mogu naći sledeće informacije o svakom izuzetku:

- **Datoteka** - obezbeđuje tačno ime odgovarajuće aplikacije
- **Putanja datoteke** - pokazuje put do lokacije aplikacije
- **Kontrolni zbir** - prikazuje jedinstveni „potpis“ izabrane datoteke. Kontrolni zbir je automatski generisana niska znakova koja dozvoljava AVG programu da nedvosmisleno razlikuje odabranu datoteku od drugih datoteka. Kontrolni zbir se generiše i prikazuje nakon uspešnog dodavanja datoteke.

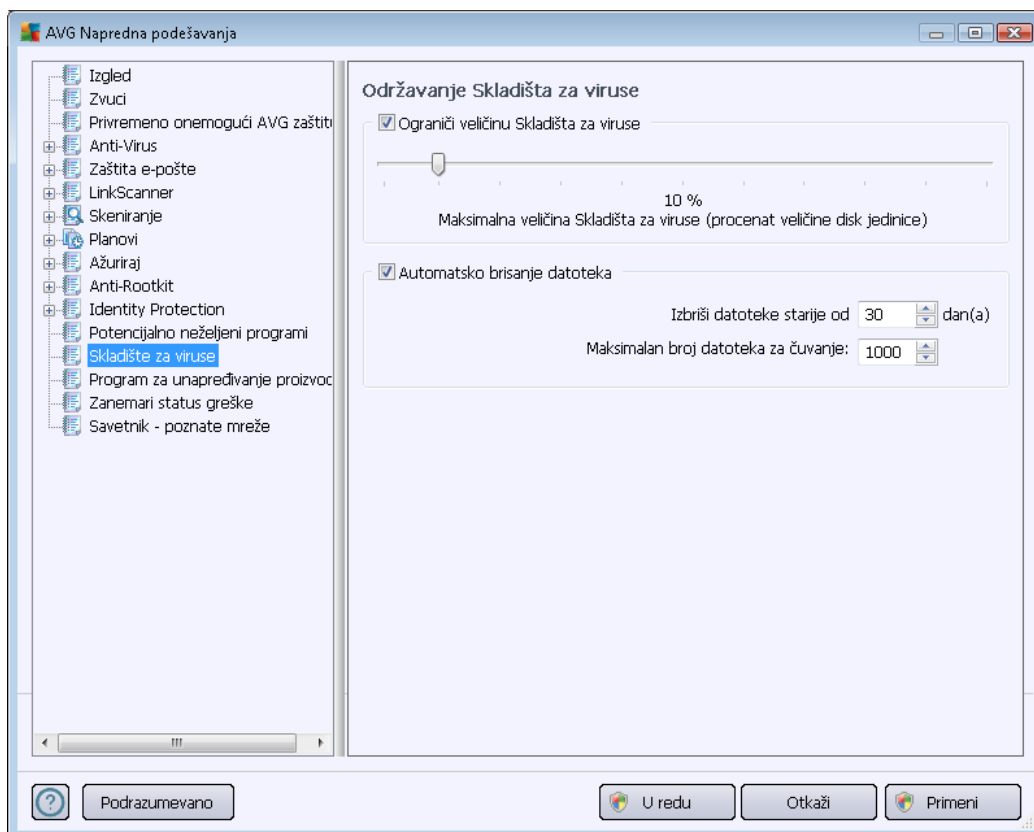
Kontrolna dugmad

- **Uredi** – otvaranje dijaloga za uređivanje (*isti je kao dijalog za definisanje novog izuzetka, pogledajte ispod*) nekog od već definisanih izuzetaka u kojem možete promeniti parametre izuzetka
- **Ukloni** - brisanje izabrane stavke sa liste izuzetaka
- **Dodaj izuzetak** – otvaranje dijaloga za uređivanje u kojem možete definisati parametre novog izuzetka koji će biti kreiran:



- **Datoteka** - unesite punu putanju do datoteke koju želite da označite kao izuzetak
- **Kontrolni zbir** - prikazuje jedinstveni „potpis“ izabrane datoteke. Kontrolni zbir je automatski generisana niska znakova koja dozvoljava AVG programu da nedvosmisleno razlikuje odabranu datoteku od drugih datoteka. Kontrolni zbir se generiše i prikazuje nakon uspešnog dodavanja datoteke.
- **Informacije o datoteci** - prikazuje sve dodatne dostupne informacije o datoteci (informacije o licenci/verziji itd.)
- **Bilo koja lokacija - ne koristi punu putanju** - ako želite ovu datoteku da definišete kao izuzetak samo na određenoj lokaciji, ostavite ovo polje neoznačeno. Ako je u polju za potvrdu potvrđen izbor, navedena datoteka se definiše kao izuzetak bez obzira na to gde se nalazi (međutim, ipak morate uneti punu putanju do određene datoteke; datoteka će se zatim koristiti kao jedinstveni primer za slučaj da se u sistemu pojave dve datoteke sa istim imenom).

10.13. Skladište za viruse



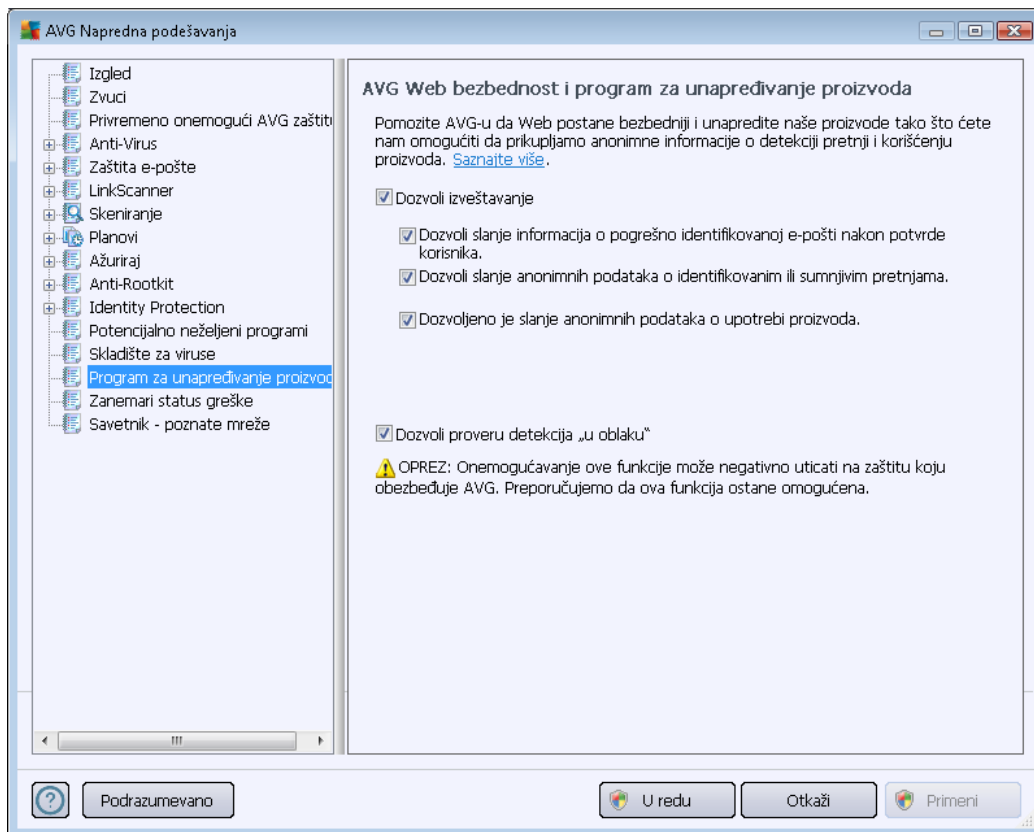
U dijalogu **Održavanje Skladišta za viruse** možete definisati nekoliko parametara u vezi sa administracijom objekata koji se čuvaju u [Skladištu za viruse](#):

- **Ograničavanje veličine skladišta za viruse** - koristite klizač da biste podesili maksimalnu veličinu [skladišta za viruse](#). Veličina se definiše kao procenat veličine lokalnog diska.
- **Automatsko brisanje datoteka** - u ovom odeljku definišite maksimalni vremenski period tokom kojeg objekti treba da budu uskladišteni u [skladištu za viruse](#) (**Izbriši datoteke starije od... dana**) i maksimalan broj datoteka koje treba da se uskladište u [skladištu za viruse](#) (**Maksimalan broj datoteka koje treba uskladišiti**).

10.14. Program za poboljšanje proizvoda

Dijalog **AVG program za Web bezbednost i poboljšanje proizvoda** poziva vas da učestvujete u poboljšanju AVG proizvoda i da nam pomognete da povećamo ukupan nivo Internet bezbednosti. Ostavite opciju **Dozvoli prijavljivanje** označenu da biste omogućili prijavljivanje otkrivenih pretnji AVG laboratorijama. To nam omogućava da prikupljamo ažurirane informacije o najnovijim pretnjama od svih korisnika širom sveta, kako bismo unapredili zaštitu svih korisnika.

Prijavljivanje se obavlja automatski i zato vam ne predstavlja nikakav problem. U izveštaje nisu uključeni nikakvi lični podaci. Prijavljivanje otkrivenih pretnji je opcionalno, ali vas molimo da ovu opciju ostavite uključenu. To nam pomaže u zaštiti vas i drugih AVG korisnika.



U dijalogu su dostupne sledeće opcije za podešavanje:

- **Dozvoli izveštavanje** (*podrazumevano uključeno*) - ako želite da nam pomognete da dodatno poboljšamo **AVG Internet Security 2012**, ostavite označeno ovo polje za potvrdu. Time ćete omogućiti izveštavanje o svim pronađenim pretnjama kompaniji AVG kako bismo prikupljali najnovije informacije o malveru od svih korisnika širom sveta i, zahvaljujući tome, poboljšali zaštitu za sve. Izveštavanje se obavlja automatski, pa vam neće predstavljati teret, a u izveštajima nema ličnih podataka.
- **Dozvoli slanje informacija o pogrešno identifikovanoj e-pošti nakon potvrde korisnika** (*podrazumevano uključeno*) – slanje informacija o e-porukama koje su pogrešno identifikovane kao bezvredne ili o bezvrednim porukama koje komponenta [Obrana od bezvredne pošte](#) nije otkrila. Pre slanja ovih informacija, od vas će se tražiti potvrda.
- **Dozvoli slanje anonimnih podataka o identifikovanim ili sumnjivim pretnjama** (*podrazumevano uključeno*) – slanje informacija o svakom sumnjivom ili dokazano opasnom kodu ili obrascu ponašanja (*može biti reč o virusu, špijunskom softveru ili zlonamernoj Web lokaciji kojoj pokušavate da pristupite*) koji bude otkriven na vašem računaru.
- **Dozvoli slanje anonimnih podataka o upotrebi proizvoda** (*podrazumevano uključeno*) – slanje osnovne statistike o upotrebi aplikacija, kao što je broj otkrivanja, pokrenutih skeniranja, uspešnih ili neuspešnih ažuriranja itd.

- **Dozvoli proveru otkrivenih pretnji „u oblaku“** (podrazumevano uključeno) – otkrivene pretnje će biti proverene kako bi se utvrdilo da li su zaista zaražene i kako bi se isključila mogućnost da dođe do potvrđenih grešaka.

Najčešće pretnje

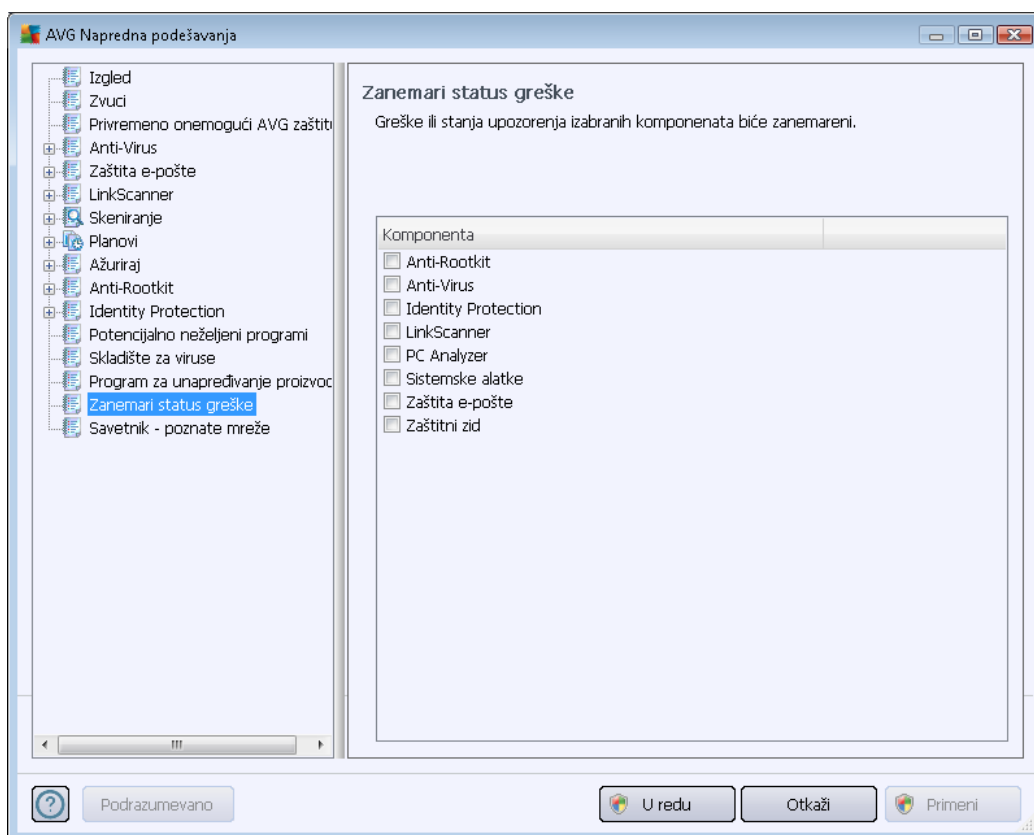
U današnje vreme, postoji mnogo više pretnji nego običnih virusa. Autori zlonamernih kodova i opasnih Web lokacija su vrlo domišljati i nove vrste pretnji se javljaju vrlo često, od kojih je velika većina na Internetu. Evo nekih od najčešćih:

- **Virus** je zlonamerni kôd koji se sam kopira i širi, a često se ne može primetiti sve dok ne počne da nanosi štetu računaru. Neki virusi predstavljaju ozbiljnu pretnju, jer brišu ili namerno menjaju datoteke na računaru, dok neki virusi izvršavaju naizgled neškodljive komande, kao što je reprodukcija neke melodije. Međutim, svi virusi su opasni zbog njihove osnovne sposobnosti da se umnožavaju - čak i jednostavan virus može veoma brzo zauzeti celu memoriju računara i izazvati pad sistema.
- **Crv** predstavlja potkategoriju virusa kojem, za razliku od običnih virusa, nije potreban „prenosilac“ - objekat za koje se mora prikazati; on se sam šalje na druge računare, obično e-poštom, pa često izaziva preopterećenje servera e-pošte i mrežnih sistema.
- **Špijunski softver** se obično definiše kao vrsta malvera (*malver = bilo kakav zlonamernan softver, uključujući i viruse*) koji obuhvata programe - najčešće Trojanske konje - čiji je cilj krađa ličnih informacija, lozinki, brojeva kreditnih kartica ili infiltriranje u računar i omogućavanje napadaču da ga daljinski kontroliše; naravno, sve to bez znanja i dozvole vlasnika računara.
- **Potencijalno neželjeni programi** su vrsta špijunskog softvera koji može, ali ne mora biti opasan po vaš računar. Konkretni primer Potencijalno neželjenog programa je adwer, softver koji distribuira reklame, obično preko iskačućih prozora, što je neprijatno, ali ne i štetno.
- **Kolačići za praćenje** takođe se mogu smatrati vrstom špijunskog softvera, pošto ove male datoteke, koje se čuvaju u Web pregledaču i automatski šalju „matičnoj“ Web lokaciji kada je ponovo posetite, mogu sadržati podatke o vašoj istoriji pregledanja Interneta i slične informacije.
- **Exploit program** je zlonamerni kôd koji iskorištava nedostatke ili propuste u operativnom sistemu, Internet pregledaču ili nekom drugom važnom programu.
- **Phishing** je pokušaj da se dođe do osetljivih ličnih podataka izigravajući poverljive i dobro poznate organizacije. Potencijalne žrtve se obično kontaktiraju masovnim e-porukama koje od njih traže da npr. ažuriraju podatke svog bankovnog računa. Da bi to uradili, nudi im se veza koja vodi do lažne Web lokacije banke.
- **Hoax poruke** su masovne e-poruke koje sadrže opasne, uznemiravajuće ili dosadne i beskorisne informacije. Mnoge od gore navedenih pretnji se šire putem hoax e-poruka.
- **Zlonamerne Web lokacije** su one koje namerno instaliraju zlonamerni softver na vašem računaru, a hakovane lokacije rade to isto, ali su u pitanju legitimne Web lokacije koje se zloupotrebljavaju kako bi zarazile posetioce.

Da biste bili zaštićeni od svih ovih različitih tipova pretnji, AVG Internet Security 2012 uključuje specijalizovane komponente. Kratak opis ovih komponenti potražite u poglavlju [Pregled komponenti](#).

10.15. Zanemari status greške

U dijalogu **Zanemarivanje statusa greške** možete označiti komponente za koje ne želite da budete obaveštavani:



Podrazumevano, na listi nije izabrana nijedna komponenta. To znači da ako se neka komponenta nađe u stanju greške, bićete odmah obavešteni putem:

- [ikone na sistemskoj paleti](#) – kada sve komponente programa AVG rade ispravno, ikona se prikazuje u četiri boje. Međutim, ako dođe do greške, ikona se prikazuje sa žutim znakom uzvika,
- tekstualnog opisa postojećeg problema u odeljku [Informacije o bezbednosnom statusu](#) u glavnom prozoru programa AVG

Možda će biti potrebno da u nekoj situaciji iz nekog razloga privremeno isključite komponentu (*to se ne preporučuje, trebalo bi da sve komponente stalno budu uključene i u podrazumevanoj konfiguraciji, ali postoji mogućnost da ih isključite*). U tom slučaju, ikona na sistemskoj paleti vas automatski obaveštava o statusu greške komponente. Međutim, u ovom konkretnom slučaju ne može se govoriti o stvarnoj grešci jer ste je namerno izazvali i svesni ste mogućeg rizika. Kada ikona



postane siva, nećete dobijati obaveštenja o mogućoj drugoj grešci koja se javila.

U tom slučaju, u gore navedenom dijalogu možete izabrati komponente koje mogu biti u stanju greške (*ili isključene*) i za koje ne želite da dobijate obaveštenja. Ista opcija (*Zanemari status komponente*) dostupna je za određene komponente i direktno u [pregledu komponenti u glavnom AVG prozoru](#).

10.16. Savetnik - poznate mreže

The [AVG savetnik](#) obuhvata funkciju koja nadgleda mreže sa kojima se povezujete i ako se pronade nova mreža (*sa imenom mreže koje se već koristilo, što može dovesti do zabune*), obavestiće vas i preporučiti vam da proverite bezbednost mreže. Ako zaključite da je mreža bezbedna za povezivanje, možete je takođe sačuvati na ovoj listi; [AVG savetnik](#) će u tom slučaju zapamtiti jedinstvene atribute mreže (*posebno MAC adresu*) i sledeći put neće prikazivati obaveštenje.

U ovom prozoru dijaloga možete proveriti koje ste mreže prethodno sačuvali kao poznate. Pojedinačne stavke možete izbrisati pritiskom na dugme **Ukloni**; data mreža će se tada ponovo smatrati nepoznatom i potencijalno nebezbednom.

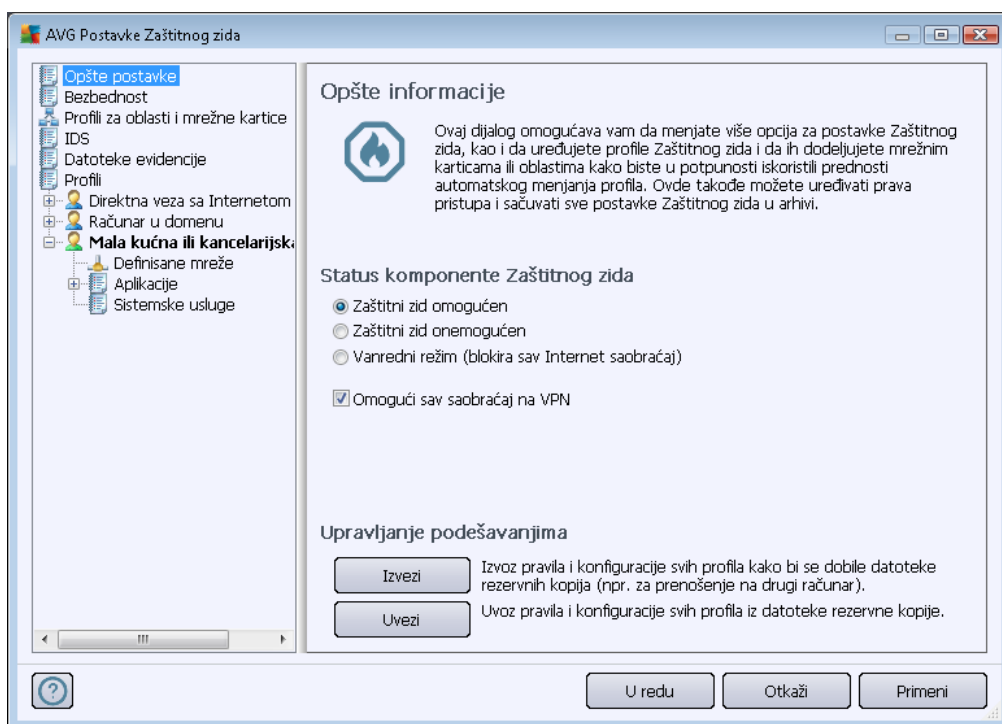
11. Podešavanja zaštitnog zida

Konfiguracija komponente [Zaštitni zid](#) otvara se u novom prozoru, a na raspolaganju vam je nekoliko dijaloga za podešavanje veoma naprednih parametara ove komponente.

Međutim, prodavac softvera je podesio sve AVG Internet Security 2012 komponente za postizanje optimalne performanse. Nemojte menjati podrazumevanu konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja bi trebalo da menjaju samo iskusni korisnici!

11.1. Opšte postavke

Dijalog **Opšte informacije** je podeljen na dva odeljka:



Status zaštitnog zida

U odeljku **Status zaštitnog zida** možete menjati status [Zaštitnog zida](#) prema potrebi:

- **Zaštitni zid omogućen** – izaberite ovu opciju da biste omogućili komunikaciju aplikacijama koje su označene kao „dozvoljene“ u skupu pravila definisanih za izabrani profil [zaštitnog zida](#).
- **Zaštitni zid je onemogućen** – ova opcija potpuno isključuje [Zaštitni zid](#), pa je sav mrežni saobraćaj dozvoljen, ali se ne proverava!
- **Hitni režim (blokira sav Internet saobraćaj)** – izaberite ovu opciju da biste blokirali sav saobraćaj na svim mrežnim portovima; [Zaštitni zid](#) je i dalje aktivan, ali je sav mrežni

saobraćaj obustavljen.

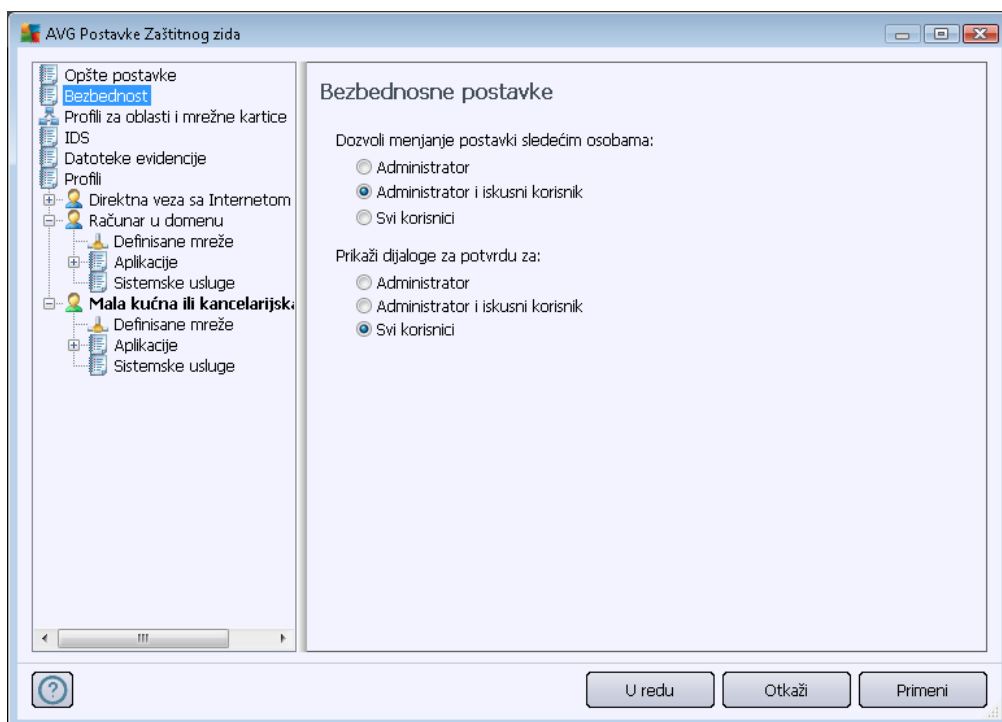
- **Omogući sav saobraćaj na VPN** (podrazumevano uključeno) – ako koristite VPN (Virtual Private Network) vezu, npr. za povezivanje sa kancelarijom od kuće, preporučujemo da označite izbor u ovom polju za potvrdu. **AVG Zaštitni zid** će automatski pretražiti vaše mrežne adaptere, pronaći one koji se koriste za VPN vezu i dozvoliti svim aplikacijama da se povežu na ciljnu mrežu (odnosi se samo na aplikacije kojima nije dodeljeno nijedno specifično pravilno zaštitnog zida). U standardnom sistemu sa uobičajenim mrežnim adapterima, ovaj jednostavan korak vam omogućava da ne morate da dodeljujete detaljna pravila svakoj aplikaciji koju želite da koristite preko VPN veze.

Napomena: Da biste omogućili VPN vezu, morate dozvoliti komunikaciju sledećim sistemskim protokolima: GRE, ESP, L2TP, PPTP. To možete uraditi u dijalogu [Sistemske usluge](#).

Upravljanje podešavanjima

U odeljku **Upravljanje podešavanjima** možete da **izvezete** ili **uvezete konfiguraciju Zaštitnog zida**, npr. izvezete definisana pravila [zaštitnog zida](#) i podešavanja u datoteke rezervne kopije ili da uvezete čitavu datoteku rezervne kopije.

11.2. Bezbednost



U dijalogu **Bezbednosne postavke** možete definisati opšta pravila ponašanja komponente [Zaštitni zid](#), bez obzira na to koji je profil izabran:

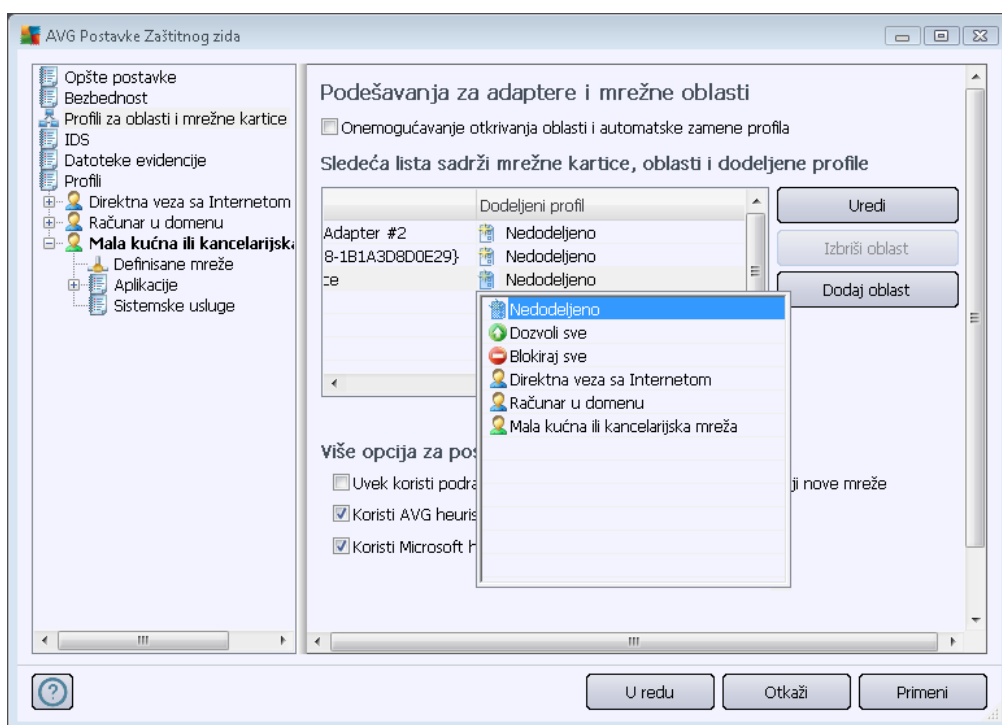
- **Dozvoli izmenu podešavanja za** - navedite kome je dozvoljeno da menja konfiguraciju [zaštitnog zida](#).
- **Prikaži dijaloge za potvrdu za** - navedite kome treba da se prikazuju dijalozi za potvrdu (dijalozi koji traže da se donese odluka u situaciji koju ne pokriva definisano pravilo [zaštitnog zida](#)).

U oba slučaja, određeno pravo možete dodeliti nekoj od sledećih korisničkih grupa:

- **Administrator** – u potpunosti kontroliše računar i ima pravo da svakog korisnika dodeli grupi sa posebno definisanim ovlašćenjima.
- **Administrator i iskusni korisnik** – administrator može svakog korisnika da dodeli određenoj grupi (*iskusni korisnik*), kao i da definiše ovlašćenja članova grupe.
- **Svi korisnici** – ostali korisnici koji nisu dodeljeni nijednoj određenoj grupi.

11.3. Profili za oblasti i adaptore

U dijalogima **Postavke za adaptore i mrežne oblasti** možete urediti postavke koje se tiču dodeljivanja definisanih profila određenim adapterima i mrežama:



- **Onemogućiti otkrivanje oblasti i automatsku zamenu profila** (podrazumevano isključeno) - jedan od definisanih profila se može dodeliti svakom tipu mrežnog interfejsa, odnosno svakoj oblasti. Ukoliko ne želite da definišete određene profile, koristiće se jedan



opšti profil. Međutim, ako želite da definišete profile i da ih dodelite određenim adapterima i oblastima, a kasnije iz nekog razloga poželite da privremeno promenite ove postavke, izaberite opciju **Onemogućiti otkrivanje oblasti i automatsku zamenu profila**.

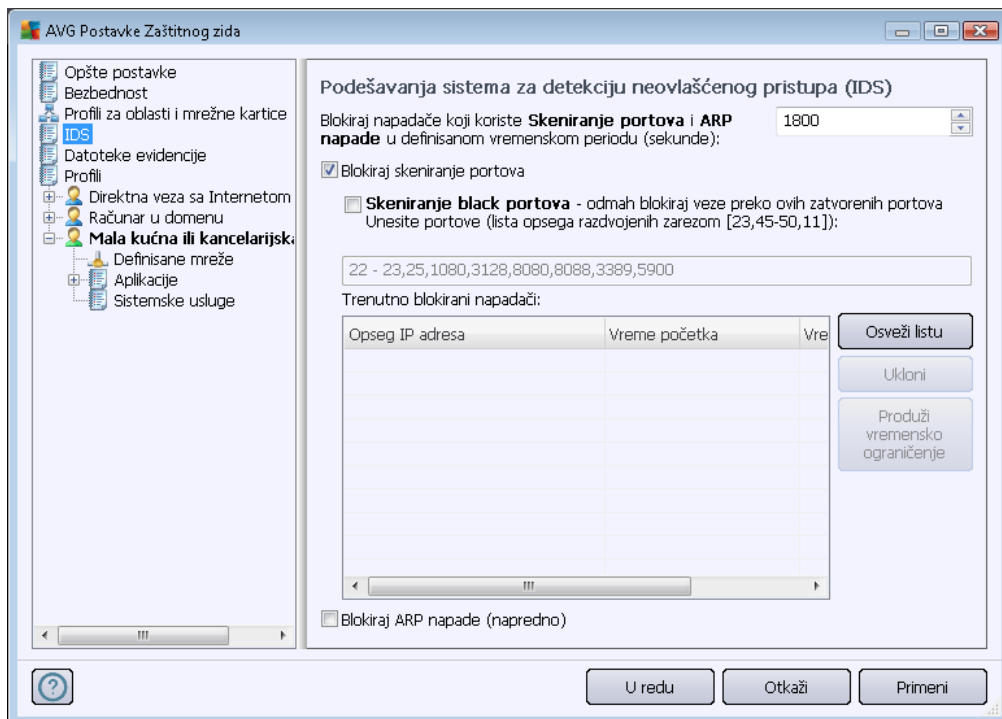
- **Lista adaptera, oblasti i dodeljenih profila** - na ovoj listi se nalazi pregled otkrivenih adaptera i oblasti. Svako od ovih stavki možete dodeliti određeni profil iz menija definisanih profila. Da biste otvorili ovaj meni, levim tasterom miša kliknite na odgovarajuću stavku na listi adaptera (u koloni „Dodeljeni profil“) i iz kontekstualnog menija izaberite profil.

Napredna podešavanja

- **Uvek koristi podrazumevani profil i ne prikazuj dijalog o detekciji nove mreže** - kad god se vaš računar poveže na novu mrežu, [Zaštitni zid](#) će vas obavestiti i prikazati dijalog u kojem se od vas traži da izaberete tip mrežne veze i da joj dodelite [Profil zaštitnog zida](#). Ako ne želite da se ovaj dijalog prikazuje, označite ovo polje.
- **Koristi AVG heuristiku za otkrivanje novih mreža** - omogućava prikupljanje informacija o novoj otkrivenoj mreži pomoću AVG mehanizma (međutim, ova opcija je dostupna samo u operativnom sistemu Windows Vista i novijim verzijama).
- **Koristi Microsoft heuristiku za otkrivanje novih mreža** - omogućava uzimanje informacija o upravo otkrivenoj mreži iz Windows usluge (ova opcija je dostupna samo u operativnom sistemu Windows Vista i novijim verzijama).

11.4. IDS

IDS (Sistem za detekciju neovlašćenog pristupa) je posebna funkcija za analizu ponašanja, dizajnirana da prepozna i blokira sumnjive pokušaje komunikacije preko određenih portova na računaru. IDS parametre možete konfigurisati u dijalogu **Sistem za detekciju neovlašćenog pristupa (IDS) podešavanja**:



Dijalog **Podešavanja sistema za detekciju neovlašćenog pristupa** nudi sledeće opcije za konfiguraciju:

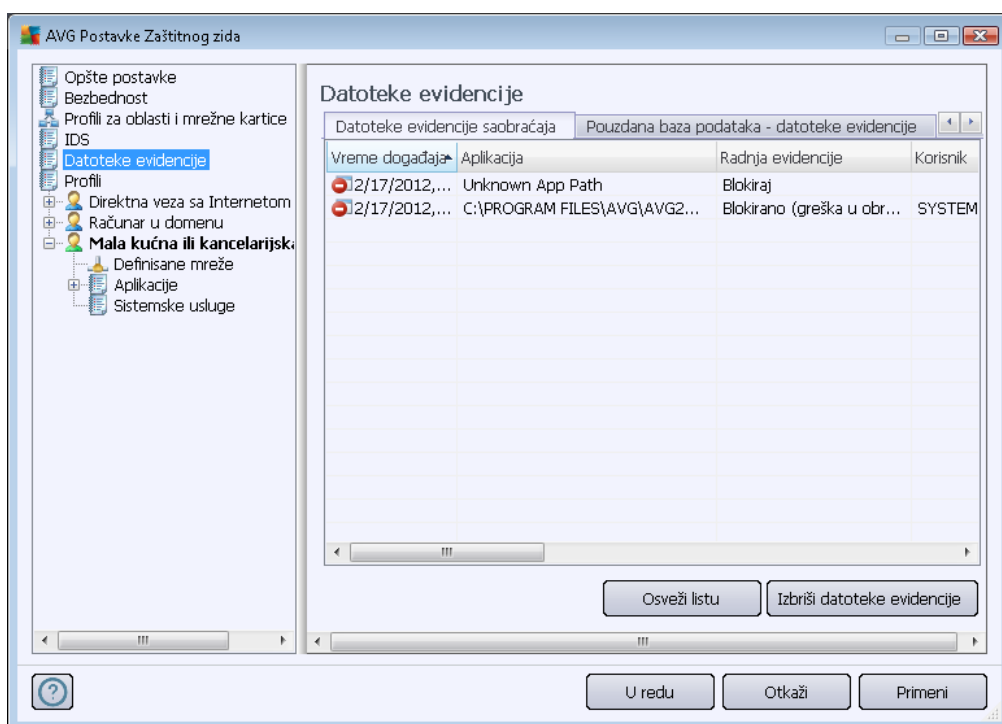
- **Blokiraj (skeniranje porta i ARP napadi) napadače u određenom vremenskom periodu** - ovde možete navesti koliko sekundi port treba da bude blokiran svaki put kada se na njemu otkrije sumnjivi pokušaj komunikacije. Podrazumevano, vremenski interval je podešen na 1800 sekundi (30 minuta).
- **Blokiraj skeniranje porta (podrazumevano uključeno)** – označite izbor u ovom polju za potvrdu da biste blokirali pokušaje komunikacije preko svih TCP i UDP portova koji potiču sa spoljašnjih računara. U slučaju takvih veza, dozvoljeno je pet pokušaja, dok će šesti pokušaj biti blokiran. Ova stavka je podrazumevano uključena i preporučuje se da zadržite ovo podešavanje. Ako ostavite opciju **Blokiraj skeniranje porta** uključenu, dostupna je dodatna detaljna konfiguracija (u suprotnom, sledeća stavka će biti deaktivirana):
 - **Blokiraj skeniranje porta** – označite izbor u polju za potvrdu da biste odmah blokirali sve pokušaje komunikacije preko portova navedenih u polju za tekst ispod. Pojedinačne portove ili opsege portova treba razdvojiti zarezima. Dostupna je i unapred definisana lista preporučenih portova ako želite da koristite ovu funkciju.
 - Trenutno blokirani napadači - ovaj odeljak navodi sve pokušaje komunikacije koje trenutno blokira **zaštitni zid**. Kompletna istorija blokiranih napada može se videti u dijalogu **Evidencije** (kartica „Evidencije skeniranja portova“).
- **Blokiraj ARP napade (napredno) (podrazumevano isključeno)** - označite ovu opciju da biste aktivirali blokiranje specijalnih tipova pokušaja komunikacije na lokalnoj mreži koje **IDS** otkrije kao potencijalno opasne. Primenjuje se vreme podešeno u okviru opcije **Blokiraj napadače u definisanom vremenskom periodu**. Preporučujemo da ovu funkciju koriste

samo iskusni korisnici, dobro upoznati sa tipom i nivoom rizika na lokalnoj mreži.

Kontrolna dugmad

- **Osveži listu** - pritisnite dugme da ažurirate listu (da uvrstite najnovije blokirane pokušaje)
- **Ukloni** - pritisnite da prekinete odabranu blokadu
- **Produženi rok** - pritisnite da produžite vremenski period blokade odabranog pokušaja. Otvoriće se novi dijalog sa dodatnim opcijama u kojem možete podesiti određeno vreme i datum ili neograničeno trajanje.

11.5. Datoteke evidencije



U dijalogu **Evidencija** možete da pregledate listu svih evidentiranih radnji i događaja komponente [Zaštitni zid](#) sa detaljnim opisom relevantnih parametara (vreme događaja, ime aplikacije, odgovarajuća radnja evidencije, korisničko ime, PID, smer saobraćaja, tip protokola, broj udaljenih i lokalnih portova, itd.) na četiri kartice:

- **Evidencija saobraćaja** - sadrži informacije o aktivnostima svih aplikacija koje su pokušale da se povežu sa mrežom.
- **Evidencija pouzdane baze podataka** - Pouzdana baza podataka je interna AVG baza podataka u kojoj se prikupljaju informacije o sertifikovanim i pouzdanim aplikacijama kojima se uvek može dozvoliti komunikacija na mreži. Kada aplikacija pokuša prvi put da se poveže sa mrežom (tj. kada za tu aplikaciju još nije definisano pravilo zaštitnog zida),

neophodno je da saznate da li toj aplikaciji treba dozvoliti mrežnu komunikaciju. AVG najpre pretražuje *pouzdanu bazu podataka* i ako se aplikacija nalazi u njoj, automatski će joj biti odobren pristup mreži. Tek nakon toga, pod uslovom da se u bazi podataka ne nalaze informacije o aplikaciji, od vas će se tražiti da u posebnom dijalogu odlučite da li želite da toj aplikaciji dozvolite pristup mreži.

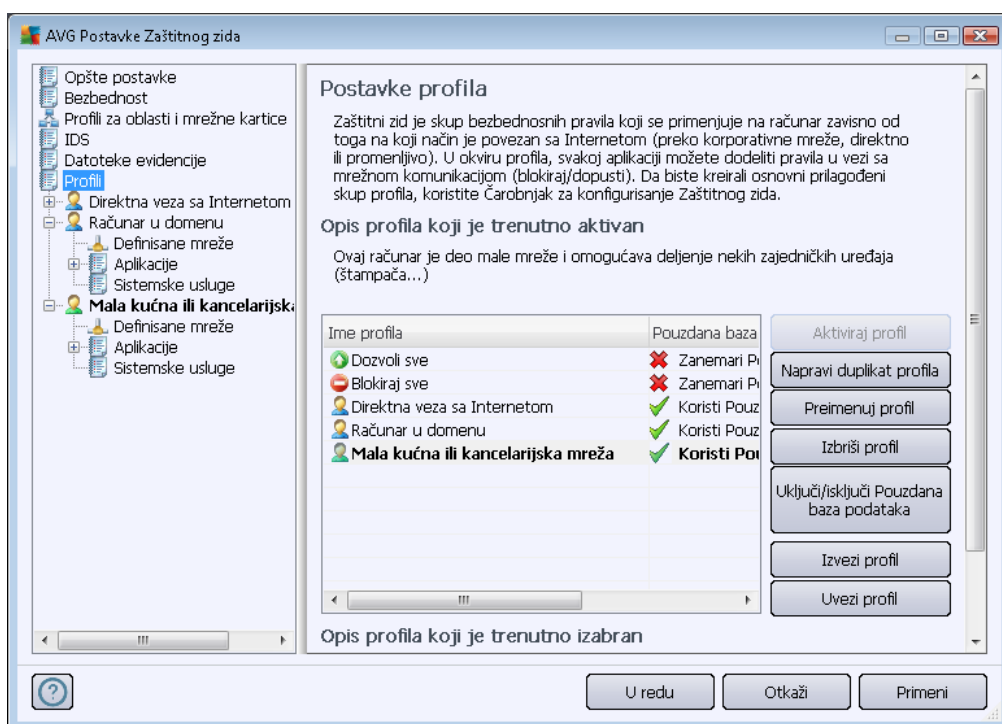
- **Evidencije skeniranja portova** - pruža evidencije svih aktivnosti [Sistema za detekciju neovlašćenog pristupa](#).
- **Evidencije ARP** - evidencione informacije oblokiranju posebnih vrsta pokušaja komunikacije u okviru lokalnih mreža ([Blokiraj ARP napade opcija](#)) detektovanih [Sistemom za detekciju neovlašćenog pristupa](#) kao potencijalno opasnih.

Kontrolna dugmad

- **Osveži listu** - svi evidentirani parametri mogu se rasporediti u skladu sa izabranim atributom: hronološki (*po datumima*) ili abecedno (*ostale kolone*) - jednostavno kliknite na odgovarajuće zaglavlje kolone. Upotrebite dugme **Osveži listu** da biste ažurirali informacije koje se trenutno prikazuju.
- **Izbriši evidencije** - kliknite da biste izbrisali sve stavke iz grafikona.

11.6. Profili

U dijalogu **Postavke profila** nalazi se lista svih dostupnih profila:





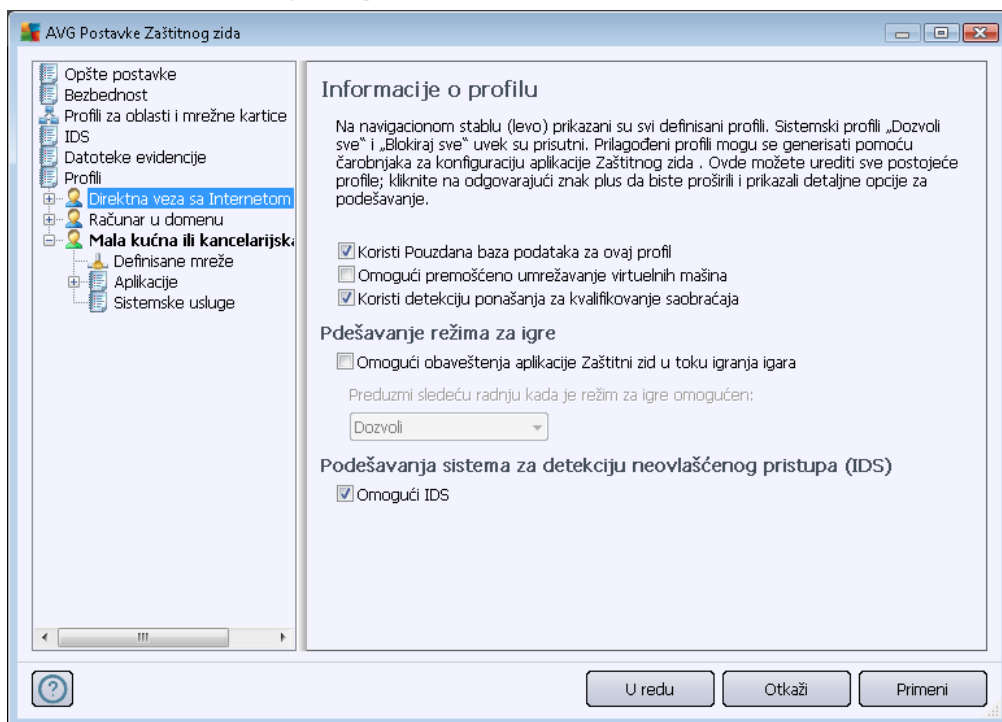
Sistemske profile (*Dozvoli sve*, *Blokiraj sve*) ne mogu se uređivati. Međutim, svi prilagođeni [profili](#) (*Direktno povezano sa Internetom*, *Računar u domenu*, *Mala kućna ili poslovna mreža*) mogu se uređivati direktno u ovom dijalogu pomoću sledeće kontrolne dugmadi:

- **Aktiviraj profil** - ovo dugme postavlja izabrani profil kao aktivan, što znači da će [zaštitni zid](#) koristiti konfiguraciju izabranog profila za kontrolisanje mrežnog saobraćaja.
- **Dupliraj profil** - kreira identičnu kopiju izabranog profila; kasnije možete urediti i preimenovati kopiju da biste kreirali novi profil na osnovu dupliranog originala.
- **Preimenuj profil** - dozvoljava vam da definišete novo ime za izabrani profil.
- **Izbriši profil** - briše izabrani profil sa liste.
- **Uključi/isključi pouzdanu bazu podataka** - za izabrani profil možete odlučiti da koristite informacije iz *pouzdanе baze podataka* (*Pouzdana baza podataka predstavlja AVG unutrašnju bazu podataka koja prikuplja podatke o pouzdanim i sertifikovanim aplikacijama kojima se uvek može dozvoliti komunikacija na mreži.*).
- **Izvezi profil** - snima konfiguraciju izabranog profila u datoteci koja će se sačuvati za moguću kasniju upotrebu.
- **Uvezi profil** - konfiguriše podešavanja izabranog profila na osnovu podataka izvezenih iz rezervne datoteke konfiguracije.

U donjem delu dijaloga nalazi se opis profila koji je trenutno izabran na gornjoj listi.

U zavisnosti od broja definisanih profila na listi u dijalogu **Profil**, menjaće se i struktura levog navigacionog menija. Za svaki definisani profil kreira se zasebna grana u okviru stavke **Profil**. Pojedinačne profile zatim možete uređivati u sledećim dijalozima (*koji su isti za sve profile*):

11.6.1. Informacije o profilu



Dijalog **Informacije o profilu** je prvi dijalog odeljka u kojem možete urediti konfiguraciju svakog profila u zasebnim dijalozima za svaki parametar profila.

- **Koristi pouzdanu bazu podataka za ovaj profil** (podrazumevano uključeno) - označite ovu opciju da biste aktivirali pouzdanu bazu podataka (tj. AVG unutrašnju bazu podataka koja prikuplja informacije o pouzdanoj i sertifikovanoj komunikaciji aplikacija na mreži. Ako za određenu aplikaciju još nije navedeno pravilo, neophodno je da saznate da li je toj aplikaciji moguće dozvoliti pristup mreži. AVG najpre pretražuje pouzdanu bazu podataka i ako se aplikacija nalazi u njoj, smatraće se bezbednom i biće joj dozvoljena komunikacija putem mreže. U suprotnom, od vas će se tražiti da odlučite da li aplikaciji treba dozvoliti komunikaciju putem mreže) za odgovarajući profil
- **Omogući premošćeno umrežavanje virtuelnih mašina** (podrazumevano isključeno) - označite ovu stavku da biste dozvolili virtuelnim mašinama u programu VMware da se direktno povezuju sa mrežom.
- **Koristi otkrivanje ponašanja za kvalifikaciju saobraćaja** (podrazumevano uključeno) - označite ovu opciju da biste [zaštitnom zidu](#) dozvolili da koristi funkcionalnost [zaštite identiteta](#) prilikom procenjivanja aplikacije - [Identity Protection](#) može da prepozna da li aplikacija ispoljava sumnjivo ponašanje ili da li joj se može verovati i dozvoliti da komunicira na mreži.

Podešavanja režima za igre

U odeljku **Podešavanja režima za igre** označavanjem odgovarajuće stavke možete odlučiti i potvrditi

da li želite da se informativne poruke [zaštitnog zida](#) prikazuju čak i kada su na računaru pokrenute aplikacije preko celog ekrana, (*obično su to igre, ali ovo se odnosi i na ostale aplikacije preko celog ekrana, npr. PPT prezentacije*), pošto informativne poruke mogu donekle da ometaju.

Ako izaberete opciju **Onemogućiti obaveštenja zaštitnog zida tokom igranja igara**, u padajućem meniju izaberite radnju koju treba preduzeti u slučaju da nova aplikacija za koju još nisu definisana pravila pokuša da komunicira putem mreže (*aplikacije za koje bi se obično pojavio upitni dijalog*), svim ovim aplikacijama može se dozvoliti ili blokirati pristup mreži.

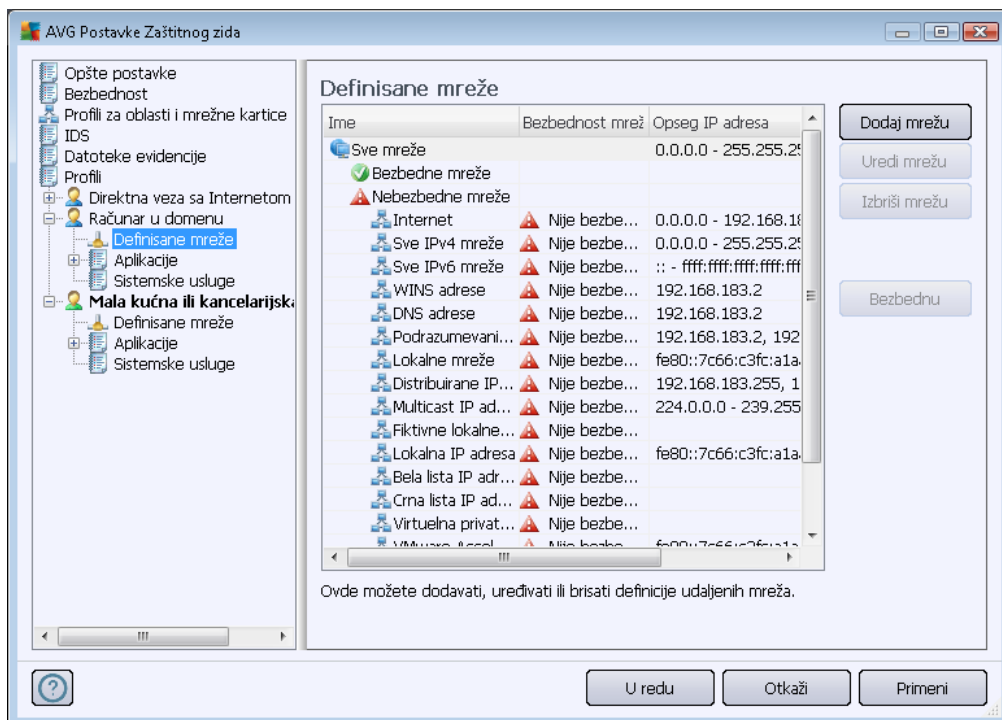
Sa uključenim režimom za igranje, svi planirani zadaci (*skeniranja, ažuriranja*) se odlažu dok se aplikacija ne zatvori.

Podešavanja sistema za detekciju neovlašćenog pristupa (IDS)

Označite izbor u polju za potvrdu **Omogući IDS** da biste aktivirali specijalno funkciju analize ponašanja namenjenu za identifikaciju i blokiranje sumnjivih pokušaja komunikacije preko određenih portova na računaru (*detalje o podešavanjima ove funkcije potražite u poglavlju [IDS](#) u ovom dokumentu*).

11.6.2. Definisane mreže

Dijalog **Definisane mreže** sadrži listu svih mreža na koje je povezan vaš računar.



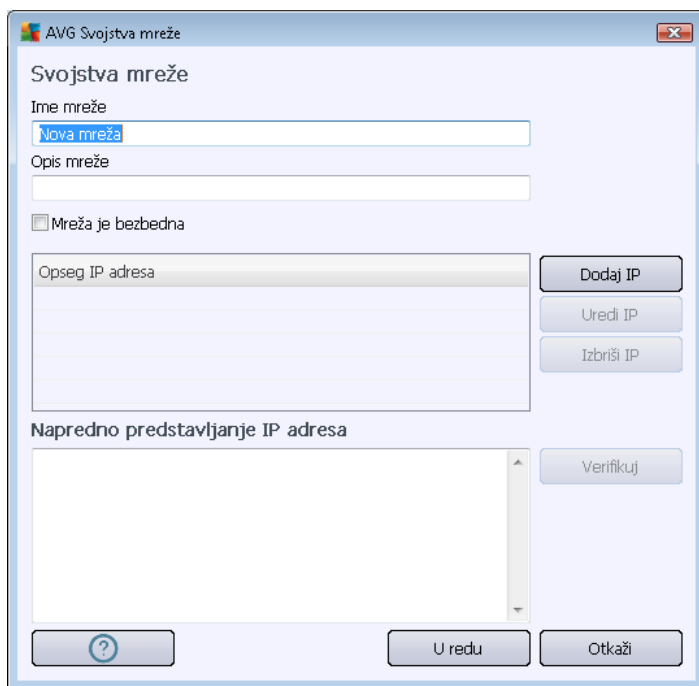
Lista pruža sledeće informacije o svakoj otkrivenoj mreži:

- **Mreže** - obezbeđuje listu imena svih mreža sa kojima je povezan računar.

- **Bezbednost mreže** - podrazumevano, sve mreže se smatraju nebezbednim, pa mreže označavajte kao bezbedne samo ako imate potpuno poverenje u njih (*kliknite na stavku sa liste koja se odnosi na određenu mrežu i izaberite opciju „Bezbedna“ u kontekstualnom meniju*) - sve bezbedne mreže biće zatim uključene u grupu mreža sa kojima aplikacija može da komunicira sa pravilom za aplikacije postavljenim na opciju [Dozvoli kao bezbedno](#).
- **Opseg IP adresa** - mreže se otkrivaju automatski i navode se u obliku opsega IP adresa.

Kontrolna dugmad

- **Dodaj mrežu** - otvara dijalog **Svojstva mreže** u kojem možete urediti parametre nove mreže.



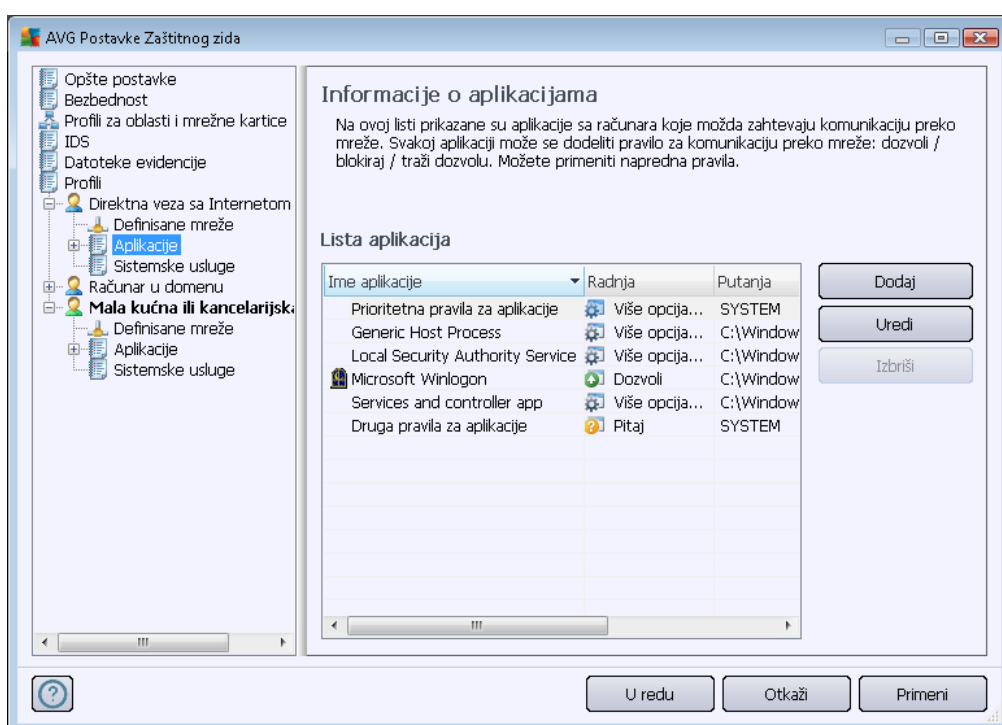
U ovom dijalogu možete navesti **Ime mreže**, uneti **Opis mreže** i eventualno je označiti kao bezbednu. Novu mrežu možete definisati ručno u samostalnom dijalogu koji se otvara ako kliknete na dugme **Dodaj IP** (takođe, **Uredi IP** / **Izbriši IP**); iz tog dijaloga možete navesti mrežu unošenjem njenog opsega IP adresa ili maske. Ako je potrebno definisati veliki broj mreža kao deo nove mreže, možete upotrebiti opciju **Napredno predstavljanje IP adresa**: unesite listu svih adresa u odgovarajuće polje za tekst (*podržani su svi standardni formati*) i pritisnite dugme **Verifikuj** da biste bili sigurni da je format prepoznat. Zatim pritisnite dugme **U redu** da biste potvrdili i sačuvali podatke.

- **Uredi mrežu** - otvara dijalog **Svojstva mreže** (*vidi iznad*) u kojem možete urediti parametre mreža koje ste već definisali (*ovaj dijalog je isti kao dijalog za dodavanje nove mreže, pogledajte opis u prethodnom pasusu*).
- **Izbriši mrežu** - uklanja informaciju o izabranoj mreži sa liste mreža.

- **Označi kao bezbednu** - podrazumevano, sve mreže se smatraju nebezbednim, pa mreže označavajte kao bezbedne pomoću ovog dugmeta samo ako imate potpuno poverenje u njih (*i obmuto, kada mrežu označite kao bezbednu, tekst na dugmetu se menja u „Označi kao nebezbednu“*).

11.6.3. Aplikacije

U dijalogu **Informacije o aplikaciji** navedene su sve instalirane aplikacije kojima može biti potrebna komunikacija preko mreže, zajedno sa ikonama za dodeljenu radnju:



Aplikacije na **listi aplikacija** su one koje je vaš računar otkrio (*i kojima je dodelio odgovarajuće radnje*). Mogu se koristiti sledeći tipovi radnji:

-  - Dozvoli komunikaciju sa svim mrežama
-  - Dozvoli komunikaciju samo sa mrežama koje su definisane kao bezbedne
-  - Blokiraj komunikaciju
-  - Prikaži traženje dijaloga (*korisnik će moći da odluči da li želi da dozvoli ili blokira komunikaciju kada aplikacija pokuša da komunicira putem mreže*)
-  - Definisana napredna podešavanja

Imajte u vidu da se detektuju samo već instalirane aplikacije, pa ćete, ako kasnije instalirate novu aplikaciju, morati da definišete pravila Zaštitnog zida za nju. Kada nova aplikacija prvi put pokuša da se poveže putem mreže, Zaštitni zid će podrazumevano automatski kreirati pravilo za tu aplikaciju u skladu sa Pouzdanom bazom podataka ili će vas pitati da li želite



da dozvolite ili blokirate komunikaciju. Ukoliko se radi o drugom slučaju, moći ćete da sačuvate svoj odgovor kao trajno pravilo (koje će biti navedeno u ovom dijalogu).

Naravno, pravila za novu aplikaciju možete i odmah definisati – u ovom dijalogu, pritisnite dugme **Dodaj** i unesite detalje o aplikaciji.

Osim aplikacija, na listi se nalaze i dve specijalne stavke:

- **Prioritetna pravila za aplikacije** (na vrhu liste) imaju prioritet i uvek se primenjuju pre pravila za pojedinačne aplikacije.
- **Druga pravila za aplikacije** (na dnu liste) koriste se kao „poslednja instanca“ ako ne važe pravila za pojedinačne aplikacije, npr. za nepoznatu i nedefinisanu aplikaciju. Izaberite radnju koja bi trebalo da se pokrene kada takva aplikacija pokuša da komunicira preko mreže:
 - *Blokiraj* – komunikacija će uvek biti blokirana.
 - *Dozvoli* – komunikacija će biti dozvoljena za sve mreže.
 - *Pitaj* – bićete pozvani da odlučite da li komunikaciju treba dozvoliti ili blokirati.

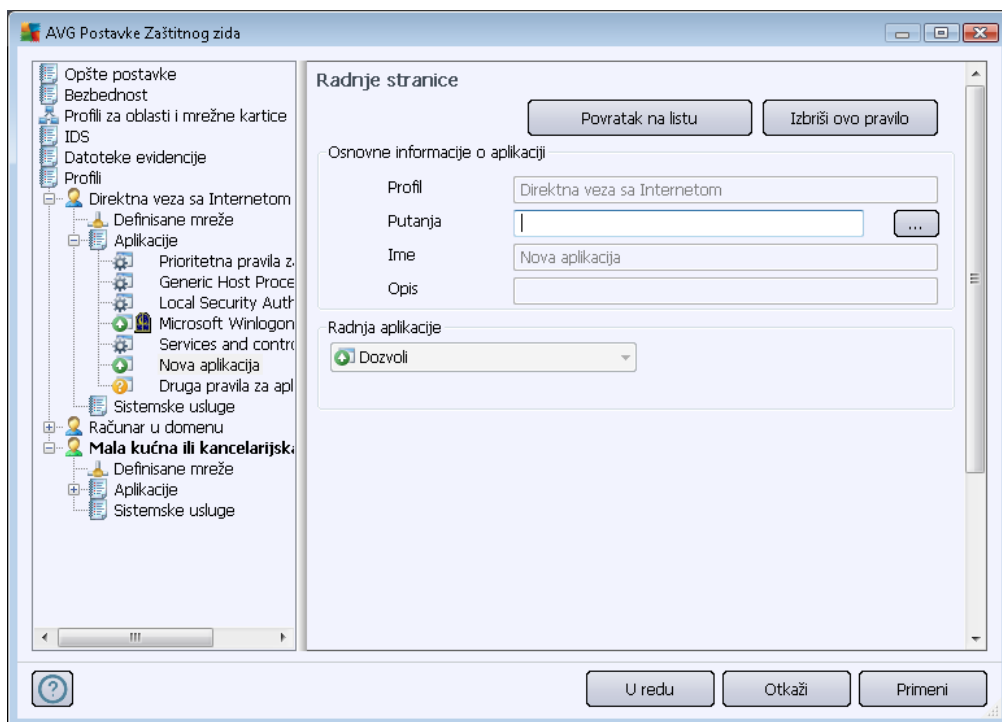
Ove stavke se podešavaju drugačije od ostalih aplikacija, a namenjene su isključivo za iskusne korisnike. Preporučujemo vam da ne menjate ova podešavanja!

Kontrolna dugmad

Listu možete urediti pomoću sledeće kontrolne dugmadi:

- **Dodaj** - otvara se prazan dijalog [Radnje na stranici](#) za definisanje novih pravila za aplikaciju.
- **Uredi** - otvara se isti dijalog [Radnje na stranici](#) u kojem se nalaze podaci za uređivanje postojećeg skupa pravila za aplikaciju.
- **Izbriši** - uklanja izabranu aplikaciju sa liste.

U dijalogu **Radnje na stranici** možete detaljno definisati podešavanja za određene aplikacije:



Kontrolna dugmad

Dva kontrolna dugmeta dostupna su na vrhu dijaloga:

- **Nazad na listu** - pritisnite ovo dugme da biste prikazali pregled svih definisanih pravila za aplikacije.
- **Izbriši ovo pravilo** - pritisnite ovo dugme da biste izbrisali trenutno prikazano pravilo za aplikacije. **Imajte u vidu da ovu radnju nije moguće opozvati!**

Osnovne informacije o aplikaciji

U ovom odeljku unesite **Ime** aplikacije, a opcionalno možete da unesete **Opis** (*kratak komentar o informacijama koje ste uneli*). U polje **Putanja** unesite punu putanju do aplikacije (*izvršne datoteke*) na disku; umesto toga, aplikaciju možete jednostavno da pronađete u strukturi stabla, tako što ćete kliknuti na dugme "...".

Radnja aplikacije

U padajućem meniju možete izabrati pravilo **zaštitnog zida** za aplikaciju, tj. šta bi **zaštitni zid** trebalo da preduzme kada aplikacija pokuša da komunicira preko mreže.

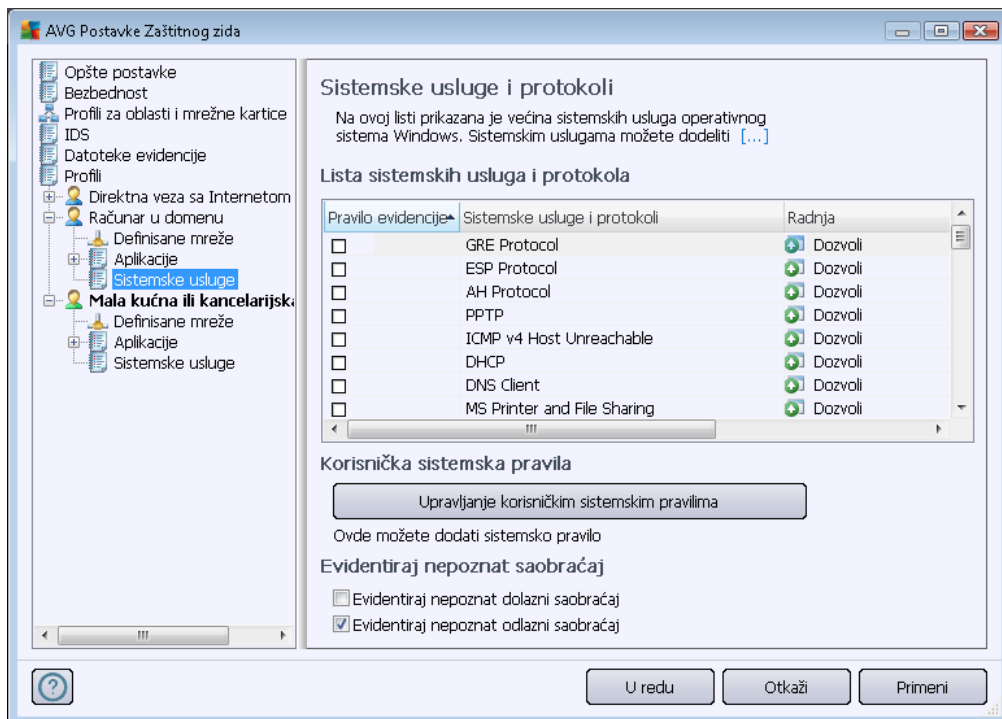


- **Dozvoli sve** - omogućava aplikaciji da komunicira preko svih definisanih mreža i adaptera, bez ikakvih ograničenja.
- **Dozvoli za bezbedne** - omogućava aplikaciji da komunicira samo preko onih mreža koje ste definisali kao bezbedne (*pouz dane*).
- **Blokiraj** - automatski zabranjuje komunikaciju; aplikaciji neće biti dozvoljeno da se poveže ni sa jednom mrežom.
- **Pitaj** - prikazuje dijalog koji vam omogućava da odlučite da li želite da dozvolite ili blokirate trenutni pokušaj komunikacije.
- **Napredna podešavanja** - prikazuje dodatne proširene i detaljne opcije podešavanja u donjem delu dijaloga u odeljku **Detaljna pravila za aplikaciju**. Detalji će se primenjivati prema redosledu na listi tako da ćete moći da koristite opcije **Premesti nagore** ili **Premesti nadole** da biste raspodelili pravila na listi po prioritetu. Nakon što kliknete na određeno pravilo sa liste, pregled detalja pravila prikazaće se u donjem delu dijaloga. Svaka vrednost koja je podvučena plavom bojom može se promeniti tako što ćete kliknuti na odgovarajući dijalog za podešavanje. Da biste izbrisali istaknuto pravilo, pritisnite dugme **Ukloni**. Da biste definisali novo pravilo, upotrebite dugme **Dodaj** da biste otvorili dijalog **Promeni detalje pravila** u kojem možete definisati sve potrebne detalje.

11.6.4. Sistemske usluge

Sva uređivanja u dijalogu „Sistemske usluge i protokoli“ namenjena su SAMO ISKUSNIM KORISNICIMA!

U dijalogu **Sistemske usluge i protokoli** su navedene standardne Windows sistemske usluge i protokoli koji možda zahtevaju komunikaciju putem mreže:



Lista sistemskih usluga i protokola

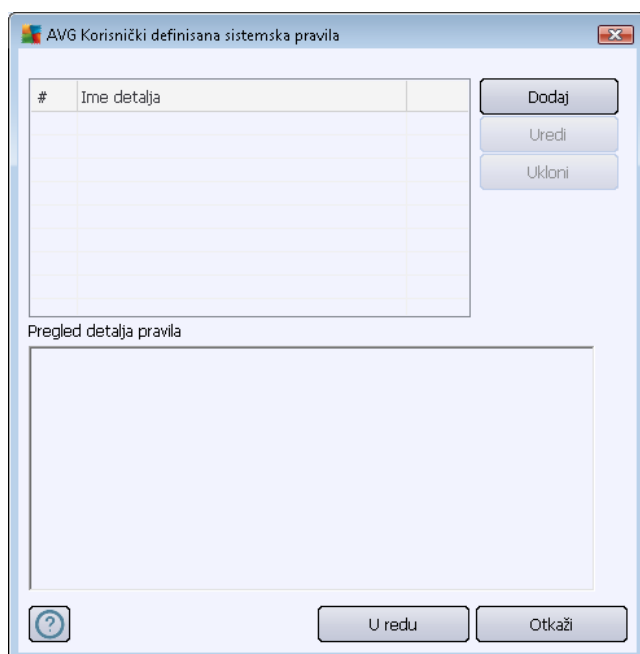
Grafikon se sastoji iz sledećih kolona:

- **Radnja pravila evidencije** - ovo polje vam omogućava da uključite snimanje svake primene pravila u [evidencijama](#).
- **Sistemske usluge i protokoli** - ova kolona prikazuje ime odgovarajuće sistemske usluge.
- **Radnja** - ova kolona prikazuje ikonu za dodeljenu radnju:
 -  Dozvoli komunikaciju sa svim mrežama
 -  Dozvoli komunikaciju samo sa mrežama koje su definisane kao Bezbedne
 -  Blokiraj komunikaciju
- **Mreže** - ova kolona navodi na koju se određenu mrežu odnosi sistemsko pravilo.

Da biste uredili postavke bilo koje stavke na listi (*uključujući dodeljene radnje*), kliknite desnim tasterom miša na stavku i izaberite opciju **Uredi**. **Sistemska pravila bi trebalo da uređuju samo napredni korisnici, a strogo se preporučuje da se ne uređuju!**

Korisnički definisana sistemska pravila

Da biste otvorili novi dijalog za definisanje sopstvenog sistemskog pravila (*pogledajte sliku ispod*), kliknite na dugme **Upravljanje korisničkim sistemskim pravilima**. U gornjem delu dijaloga **Korisnički definisana sistemska pravila** se prikazuje pregled svih detalja trenutno izmenjenog sistemskog pravila, a u donjem delu se prikazuje izabrani detalj. Korisnički definisana pravila mogu se uređivati, dodavati ili brisati pomoću odgovarajućeg dugmeta. Pravila koje je definisao proizvođač mogu se samo uređiti:



Imajte u vidu da su detaljna podešavanja pravila napredna, pre svega namenjena za administratore mreže kojima je potrebna potpuna kontrola nad konfiguracijom zaštitnog zida. Ako niste upoznati sa tipovima protokola za komunikaciju, brojevima mrežnih portova, definicijama IP adresa itd., ne menjajte ove postavke! Ukoliko je zaista potrebno da promenite konfiguraciju, pogledajte datoteke pomoći u odgovarajućem dijalogu da biste saznali više informacija.

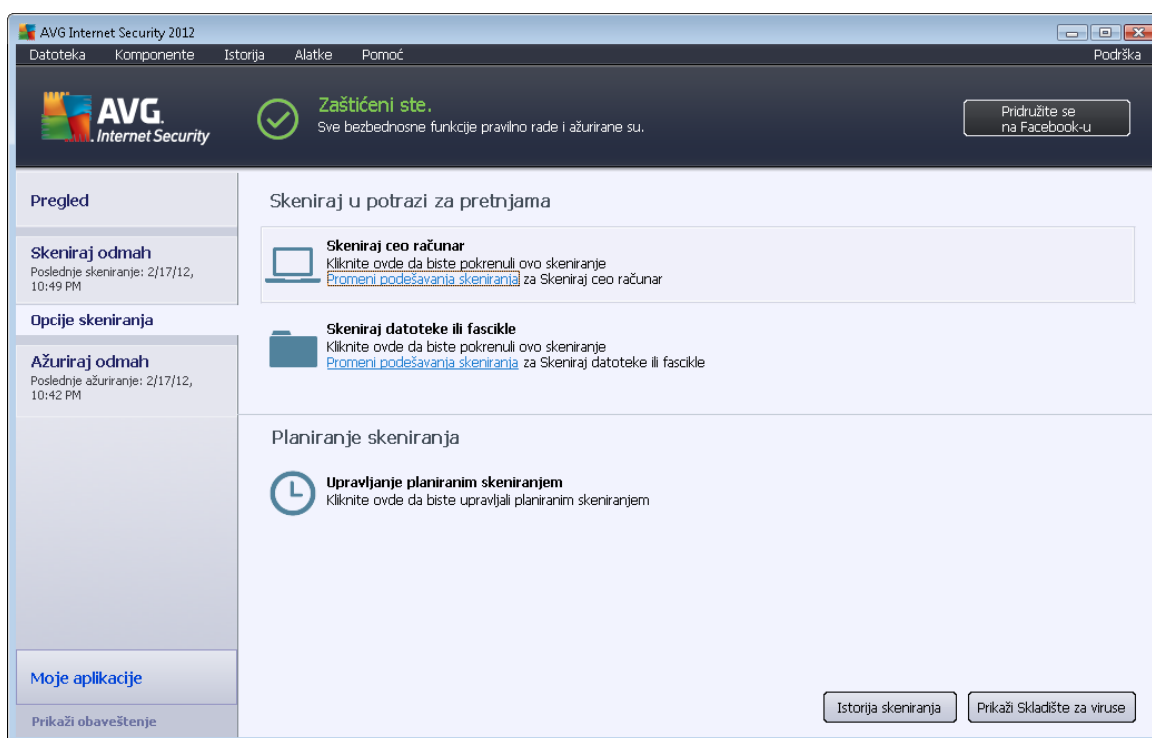
Evidentiraj nepoznat saobraćaj

- **Evidentiraj nepoznati dolazni saobraćaj** (*podrazumevano isključeno*) – označite izbor u polju za potvrdu da biste u [evidencijama](#) snimali svaki nepoznati spoljni pokušaj povezivanja sa vašim računarom.
- **Evidentiraj nepoznati odlazni saobraćaj** (*podrazumevano uključeno*) – označite izbor u polju za potvrdu da biste u [evidencijama](#) snimali svaki nepoznati pokušaj povezivanja sa spoljnom lokacijom sa vašeg računara.

12. Skeniranje programom AVG

Podrazumevano, **AVG Internet Security 2012** ne pokreće nikakvo skeniranje zato što bi nakon početnog skeniranja trebalo u potpunosti da vas štite stalne komponente programa **AVG Internet Security 2012** koje su uvek u pripravnosti i ne dozvoljavaju zlonamernom kodu da pristupi vašem računaru. Naravno, možete [da isplanirate skeniranje](#) u redovnim intervalima ili ručno pokrenete skeniranje u skladu sa potrebama.

12.1. Interfejs za skeniranje



AVG interfejsu za skeniranje možete pristupiti putem **brze veze** [Opcije skeniranja](#). Kliknite na ovu vezu da biste prešli na dijalog **Skeniraj u potrazi za pretnjama**. U tom dijalogu nalaze se sledeći elementi:

- pregled [unapred definisanih skeniranja](#) - tri vrste skeniranja koje je definisao prodavac softvera mogu se koristiti odmah, na zahtev ili planirano:
 - [Skeniranje celog računara](#)
 - [Skeniraj određene datoteke ili fascikle](#)
- [Odeljak „Planiranje skeniranja“](#) u kojem po potrebi možete definisati nove testove i kreirati nove planove.

Kontrolna dugmad



U interfejsu za testiranje dostupna su sledeća kontrolna dugmad:

- **Istorija skeniranja** - prikazuje dijalog [Pregled rezultata skeniranja](#) sa celokupnom istorijom skeniranja
- **Prikaži Skladište za viruse** - otvara novi prozor u kojem se nalazi [Skladište za viruse](#) - karantin za detektovane zaraze.

12.2. Unapred definisana skeniranja

Jedna od glavnih funkcija programa **AVG Internet Security 2012** je skeniranje na zahtev. Testovi na zahtev su dizajnirani da skeniraju različite delove računara uvek kada postoji sumnja da je moglo doći do zaraze virusom. U svakom slučaju se preporučuje da se testovi redovno izvršavaju čak i kada mislite da nema virusa na računaru.

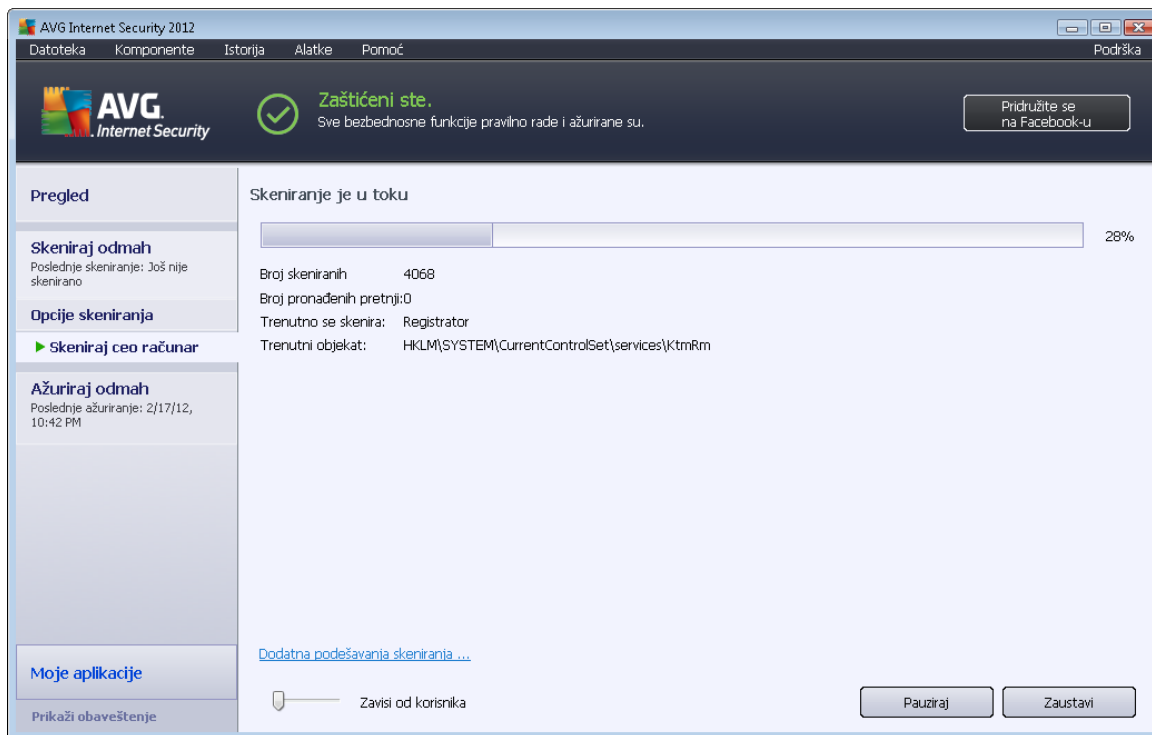
U **AVG Internet Security 2012** naći ćete dve vrste skeniranja koje je unapred definisao distributer softvera:

12.2.1. Skeniranje celog računara

Skeniraj ceo računar - skeniranje celog računara kako bi se proverilo da li sadrži viruse i/ili potencijalno neželjene programe. Ovaj test će skenirati sve čvrste diskove na računaru, detektovati i oporaviti sve pronađene viruse ili ukloniti zaraženu datoteku i premestiti je u [Skladište za viruse](#). Skeniranje celog računara trebalo bi da se zakaže na radnoj stanici barem jednom nedeljno.

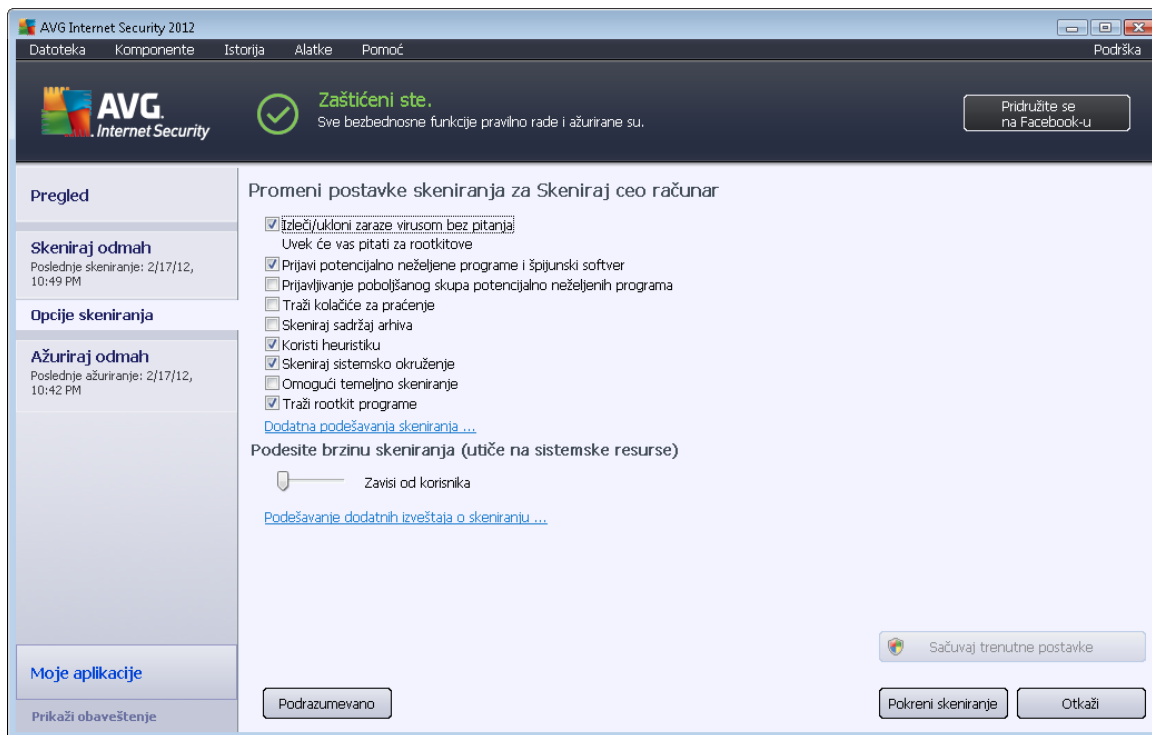
Pokretanje skeniranja

Skeniranje celog računara može se pokrenuti neposredno iz [interfejsa za skeniranje](#), tako što ćete kliknuti na ikonu tog skeniranja. Za ovaj tip skeniranja nije potrebno konfigurisati dodatne postavke, a skeniranje će odmah početi u okviru dijaloga **Skeniranje je u toku** (pogledajte snimak ekrana). Skeniranje se može privremeno prekinuti (**Pauziraj**) ili otkazati (**Zaustavi**) ako je potrebno.



Uređivanje konfiguracije skeniranja

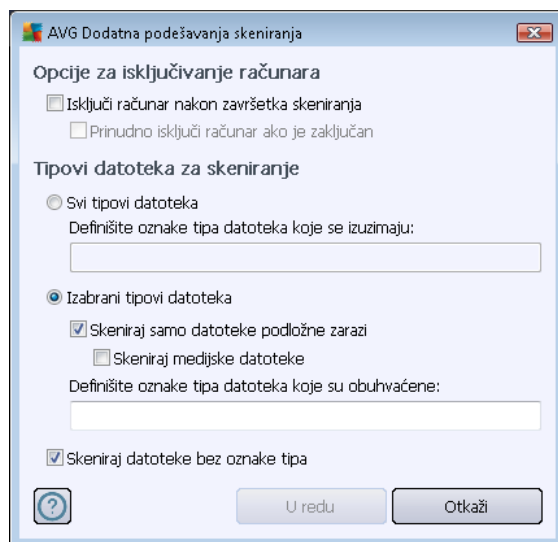
Na raspolaganju vam je opcija za uređivanje unapred podešenih podešavanja za **Skeniranje celog računara**. Pritisnite vezu **Promeni podešavanja skeniranja** da odete na dijalog **Promeni podešavanja skeniranja za skeniranje celog računara** (može se pristupiti iz [interfejsa skeniranja](#) putem veze **Promeni podešavanja skeniranja za Skeniranje celog računara). **Preporučuje se da zadržite podrazumevana podešavanja, osim ako nemate dobar razlog da ih menjate!****



- **Parametri skeniranja** - na listi parametara za skeniranje po potrebi možete uključiti/isključiti pojedinačne parametre:
 - **Izleči/ukloni virusnu infekciju bez upita** (*podrazumevano uključeno*): ako tokom skeniranja bude otkriven virus, moguće ga je automatski izlečiti ukoliko je dostupan lek. Ukoliko zaraženu datoteku nije moguće automatski izlečiti, ona će biti premeštena u [Skladište za viruse](#).
 - **Prijavi potencijalno neželjene programe i pretnje špijunskog softvera** (*podrazumevano uključeno*) - označite izbor da biste aktivirali mašinu za [zaštitu od špijunskog softvera](#) i skenirali u potrazi za špijunskim softverom, kao i za virusima. Špijunski softver se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.
 - **Prijavi poboljšani skup potencijalno neželjenih programa** (*podrazumevano isključeno*) - označite radi detekcije proširenog paketa špijunskih programa: programi koji su potpuno u redu i bezopasni kada ih kupite direktno od proizvođača, ali se kasnije mogu iskoristiti u zlonamernu svrhu. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
 - **Skeniraj kolačiće za praćenje** (*podrazumevano isključeno*) - ovaj parametar komponente [Antispajver](#) definiše da bi tokom skeniranja trebalo otkrivati kolačiće; (*HTTP kolačići služe za proveru identiteta, praćenje i održavanje određenih informacija o korisnicima, kao što su omiljene web lokacije ili sadržaj njihovih*

elektronskih korpi za kupovinu).

- **Skeniraj sadržaj arhiva** (podrazumevano isključeno) - ovaj parametar definiše da bi tokom skeniranja trebalo proveravati sve datoteke koje se nalaze unutar arhiva, npr. ZIP, RAR, ...
 - **Koristi heuristiku** (podrazumevano uključeno) - heuristička analiza (*dinamička emulacija naredbi skeniranih objekata u virtuelnom računarskom okruženju*) biće jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja.
 - **Skeniraj sistemsko okruženje** (podrazumevano uključeno) - skeniranje će obuhvatiti i sistemske oblasti vašeg računara.
 - **Omogući temeljno skeniranje** (podrazumevano isključeno) - u posebnim situacijama (*ako sumnjate da je vaš računar zaražen*), možete označiti ovu opciju da aktivirate najtemeljnije algoritme za skeniranje, koji će skenirati čak i one oblasti na računaru koji se teško mogu zaraziti, radi predostrožnosti. Ipak, zapamtite da ovaj metod prilično dugo traje.
 - **Skeniraj u potrazi za rootkit programima** (podrazumevano uključeno) - [Anti-Rootkit](#) skeniranje na računaru pretražuje moguće rootkit programe, tj. programe i tehnologije koji mogu pokriti aktivnost malvera na računaru. Ako se otkrije rootkit program, to ne znači da je vaš računar zaražen. U nekim slučajevima, određeni upravljački programi ili delovi običnih aplikacija mogu biti pogrešno protumačeni kao rootkit programi.
- **Dodatne postavke skeniranja** - ovaj link otvara novi dijalog **Dodatne postavke skeniranja** u kojem možete da navedete sledeće parametre:



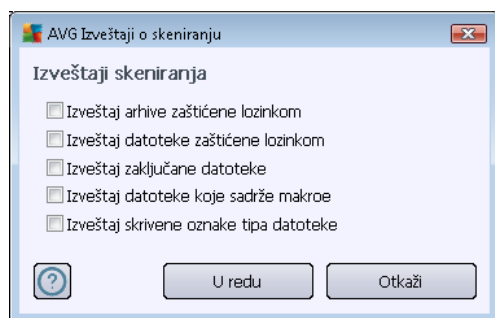
- **Opcije za isključivanje računara** - odlučite da li želite da se računar automatski isključi kada se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Isključi računar nakon završetka skeniranja**), aktiviraće se nova opcija koja omogućava da se računar isključi čak i ako je trenutno zaključan (**Prinudno isključi računar ako**

je zaključan).

- **Tipovi datoteka za skeniranje** - uz to treba da odlučite da li želite da se skeniraju:

- **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka koji se neće skenirati tako što ćete navesti listu oznaka tipa datoteke razdvojenih zarezima koje ne treba skenirati;
- **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteke možete označiti datoteke koje treba uvek skenirati.
- Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.

- **Podešavanje brzine skeniranja** - možete da koristite klizač da izmenite prioritet procesa skeniranja. Vrednost ove opcije podrazumevano je postavljena na nivo automatske zauzetosti resursa koja *zavisi od korisnika*. Takođe, proces skeniranja možete usporiti, što znači da će zauzetost sistemskih resursa biti manja (*korisno ako morate da radite na računaru, a nije vam važno koliko će skeniranje trajati*), a možete ga i ubrzati, što zahteva više sistemskih resursa (*npr. kada se privremeno udaljite od računara*).
- **Podešavanje dodatnih izveštaja o skeniranju** - ovaj link otvara novi dijalog **Izveštaji skeniranja** u kojem možete da izaberete koji tip pronađenog sadržaja će se prijavljivati:



Upozorenje: Ova podešavanja skeniranja ista su kao parametri najnovijeg definisanog skeniranja - kao što je opisano u poglavlju [AVG skeniranje / Planiranje skeniranja/ Kako skenirati](#). Ako odlučite da promenite podrazumevanu konfiguraciju opcije **Skeniraj ceo računar**, nove postavke možete sačuvati kao podrazumevanu konfiguraciju koja će se koristiti za svako buduće skeniranje celog računara.

12.2.2. Skeniraj određene datoteke ili fascikle

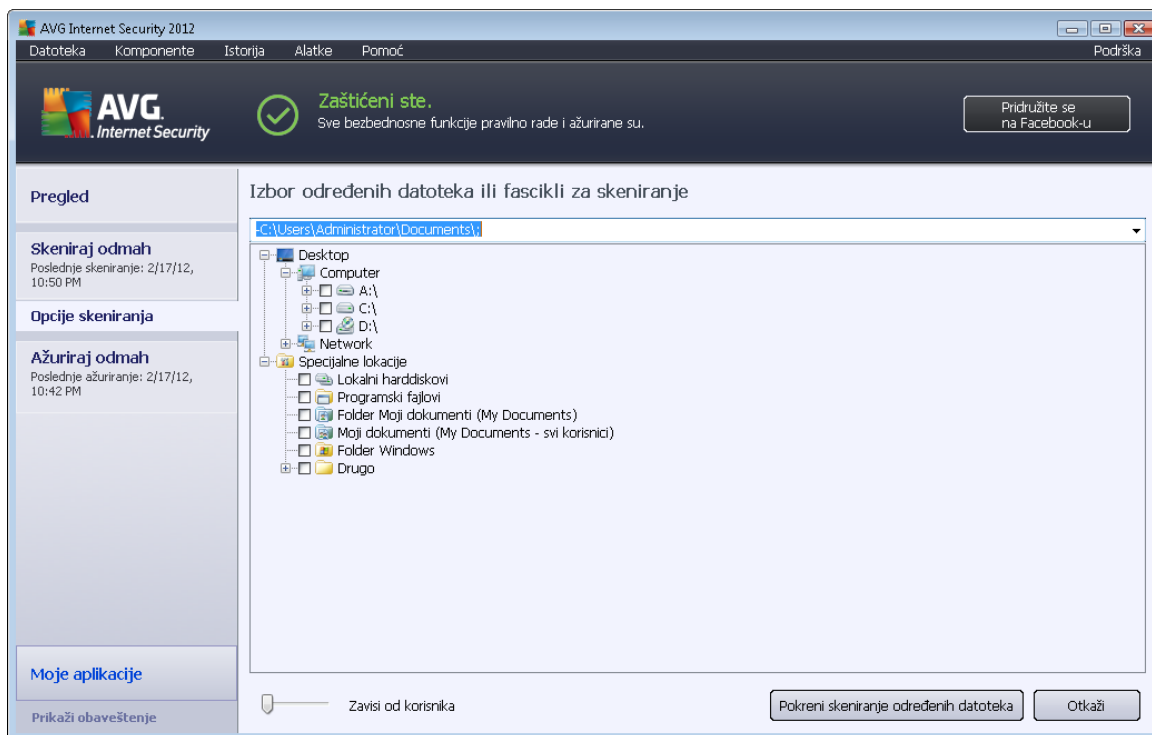
Skeniraj određene datoteke ili fascikle - skeniranje samo onih oblasti računara koje ste izabrali za skeniranje (*izabrane fascikle, čvrsti diskovi, diskete, kompakt diskovi itd.*). Tok skeniranja u slučaju detekcije virusa i tretiranje virusa isti su kao kod skeniranja celog računara: pronađeni virusi se uklanjaju iz datoteke ili premeštaju u [Skladište za viruse](#). Skeniranje datoteka ili fascikli možete koristiti da biste kreirali sopstvene testove i planove skeniranja u skladu sa vašim potrebama.

Pokretanje skeniranja

Skeniranje datoteka ili fascikli može se pokrenuti neposredno iz [interfejsa za skeniranje](#) tako što ćete kliknuti na ikonu tog vida skeniranja. Otvoriće se nov dijalog po imenu **Izbor određenih datoteka ili fascikli za skeniranje**. U prikazu stabla računara možete izabrati fascikle koje želite da skenirate. Putanja do izabranih fascikli automatski će se generisati i pojaviti se u polju za tekst u gornjem delu ovog dijaloga.

Takođe postoji mogućnost skeniranja određene fascikle, ali ne i njenih potfascikli; da biste to učinili, unesite znak minus „-“ ispred automatski generisane putanje (*vidi snimak ekrana*). Da biste celu fasciklu izuzeli iz skeniranja, koristite „!“ parametar.

Konačno, da biste pokrenuli skeniranje, pritisnite dugme **Pokreni skeniranje**; sam proces skeniranja je u suštini isti kao [Skeniranje celog računara](#).

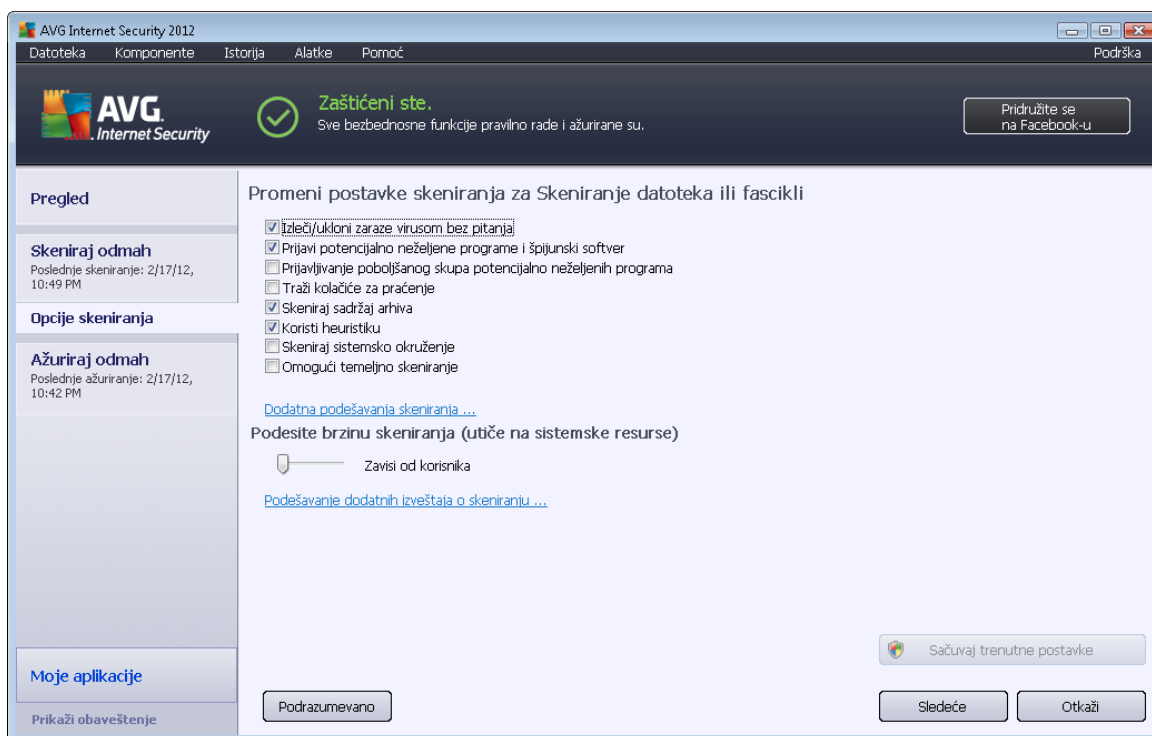


Uređivanje konfiguracije skeniranja

Imate mogućnost uređivanja unapred definisanih podešavanja za **Skeniranje datoteka ili fascikli**.

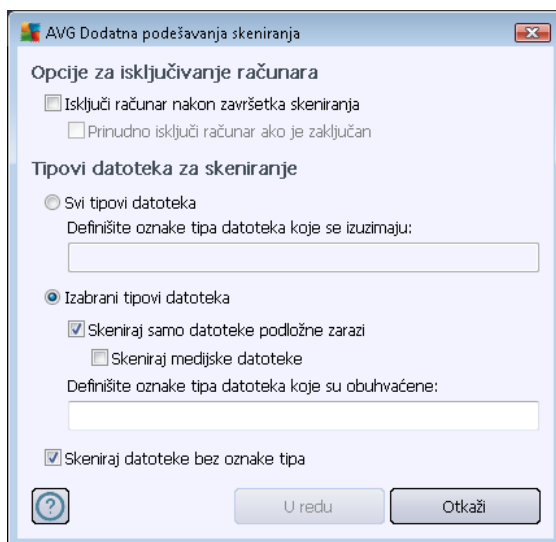


Pritisnite link **Promeni podešavanja skeniranja** da biste otvorili dijalog **Promeni podešavanja skeniranja za Skeniranje datoteka ili fascikli**. **Preporučuje se da zadržite podrazumevana podešavanja, osim ako nemate dobar razlog da ih menjate!**



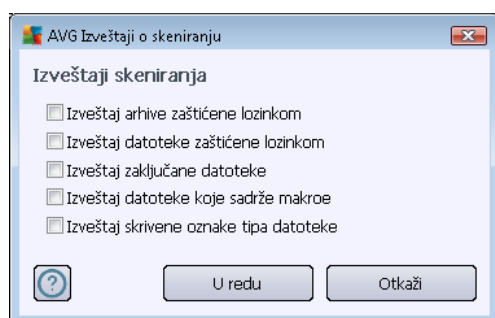
- **Parametri skeniranja** - na listi parametara za skeniranje po potrebi možete uključiti/isključiti pojedinačne parametre:
 - **Izleči/ukloni virusnu infekciju bez upita** (podrazumevano uključeno): ako tokom skeniranja bude otkriven virus, moguće ga je automatski izlečiti ukoliko je dostupan lek. Ukoliko zaraženu datoteku nije moguće automatski izlečiti, ona će biti premeštena u [Skladište za viruse](#).
 - **Prijavi potencijalno neželjene programe i pretnje špijunskog softvera** (podrazumevano uključeno) - označite radi aktivacije [Antispajver](#) mehanizma i skeniranja u potrazi za špijunskim programima kao i virusima. Špijunski softver se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.
 - **Prijavi poboljšani skup potencijalno neželjenih programa** (podrazumevano isključeno) - označite radi detekcije proširenog paketa špijunskih programa: programi koji su potpuno u redu i bezopasni kada ih kupite direktno od proizvođača, ali se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.

- **Skeniraj kolačiće za praćenje** (podrazumevano isključeno) - ovaj parametar komponente [Antispajver](#) definiše da bi trebalo da kolačići budu otkriveni; (*HTTP kolačići služe za proveru identiteta, praćenje i održavanje određenih informacija o korisnicima, kao što su omiljene Web lokacije ili sadržaj njihovih elektronskih korpi za kupovinu*).
 - **Skeniraj sadržaj arhiva** (podrazumevano uključeno) - ovaj parametar definiše da bi tokom skeniranja trebalo proveravati sve datoteke, pa čak i one koje se nalaze unutar arhiva, npr. ZIP, RAR, ...
 - **Koristi heuristiku** (podrazumevano uključeno) - heuristička analiza (*dinamička emulacija naredbi skeniranih objekata u virtuelnom računarskom okruženju*) biće jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja.
 - **Skeniraj sistemsko okruženje** (podrazumevano isključeno) - skeniranje će obuhvatiti i sistemske oblasti vašeg računara.
 - **Omogući temeljno skeniranje** (podrazumevano isključeno) - u posebnim situacijama (*ako sumnjate da je vaš računar zaražen*), možete označiti ovu opciju da aktivirate najtemeljnije algoritme za skeniranje, koji će skenirati čak i one oblasti na računaru koji se teško mogu zaraziti, radi predostrožnosti. Ipak, zapamtite da ovaj metod prilično dugo traje.
- **Dodatne postavke skeniranja** - ova veza otvara novi dijalog **Dodatne postavke skeniranja** u kojem možete da navedete sledeće parametre:



- **Opcije za isključivanje računara** - odlučite da li želite da se računar automatski isključi kada se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Isključi računar nakon završetka skeniranja**), aktiviraće se nova opcija koja omogućava da se računar isključi čak i ako je trenutno zaključan (**Prinudno isključi računar ako je zaključan**).
- **Tipovi datoteka za skeniranje** - uz to treba da odlučite da li želite da se skeniraju:

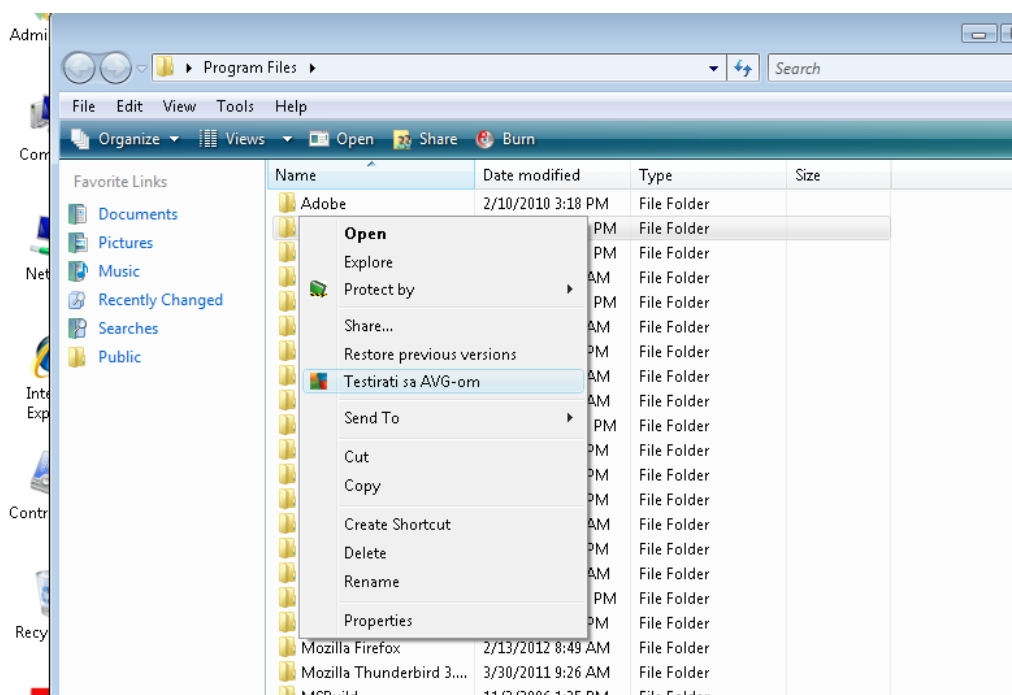
- **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka koji se neće skenirati tako što ćete navesti listu oznaka tipa datoteke razdvojenih zarezima koje ne treba skenirati;
- **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteke možete označiti datoteke koje treba uvek skenirati.
- Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.
- **Prioritet procesa skeniranja** - pomoću klizača možete promeniti prioritet procesa skeniranja. Vrednost ove opcije podrazumevano je postavljena na nivo automatske zauzetosti resursa koja *zavisi od korisnika*. Takođe, proces skeniranja možete usporiti, što znači da će zauzetost sistemskih resursa biti manja (*korisno ako morate da radite na računaru, a nije vam važno koliko će skeniranje trajati*), a možete ga i ubrzati, što zahteva više sistemskih resursa (*npr. kada se privremeno udaljite od računara*).
- **Podešavanje dodatnih izveštaja o skeniranju** - ovaj link otvara dijalog **Izveštaji skeniranja** u kojem možete izabrati koji tip pronađenog sadržaja će se prijavljivati:



Upozorenje: Ova podešavanja skeniranja ista su kao parametri najnovijeg definisanog skeniranja - kao što je opisano u poglavlju [AVG skeniranje / Planiranje skeniranja/ Kako skenirati](#). Ako odlučite da izmenite podrazumevanu konfiguraciju opcije **Skeniraj određene datoteke ili fascikle**, nova podešavanja možete sačuvati kao podrazumevanu konfiguraciju koja će se koristiti za svako buduće skeniranje datoteka ili fascikli. Takođe, ova konfiguracija će se koristiti kao predložak za sva nova planirana skeniranja ([sva prilagođena skeniranja zasnivaju se na trenutnoj konfiguraciji opcije Skeniranje datoteka ili fascikli](#)).

12.3. Skeniranje u programu Windows Explorer

Pored unapred definisanog skeniranja celog računara ili izabranih oblasti na njemu, **AVG Internet Security 2012** nudi i opciju brzog skeniranja određenog objekta direktno iz programa Windows Explorer. Ako želite da otvorite nepoznatu datoteku, a niste sigurni u njen sadržaj, možda ćete želeći da je skenirate na zahtev. Pratite sledeće korake:



- U programu Windows Explorer markirajte datoteku (*ili fasciklu*) koju želite da proverite
- Desnim tasterom miša kliknite na taj objekat da bi se otvorio kontekstualni meni
- Izaberite opciju **Skeniraj programom** da bi program AVG skenirao željenu datoteku **AVG Internet Security 2012**

12.4. Skeniranje komandne linije

U programu **AVG Internet Security 2012** postoji opcija za pokretanje skeniranja iz komandne linije. Ovu opciju možete koristiti npr. na serverima ili pri kreiranju grupne skripte koja će se automatski pokretati zajedno sa računarom. Iz komandne linije možete pokrenuti skeniranje sa većinom parametara koji su ponuđeni u AVG grafičkom korisničkom interfejsu.

Da biste pokrenuli AVG skeniranje iz komandne linije, pokrenite sledeću komandu u fascikli u kojoj je instaliran program AVG:

- **avgscanx** za 32-bitne operative sisteme
- **avgscana** za 64-bitne operative sisteme



Sintaksa komande

Sintaksa komandi je sledeća:

- **avgscanx /parametar** ... npr. **avgscanx /comp** za skeniranje celog računara
- **avgscanx /parametar /parametar** .. ako se koristi više parametara koji se ređaju jedan za drugim, a odvojeni su razmakom i kosom crtom
- ako je potrebno uneti određenu vrednost za parametar (npr. parametar **/scan** koji zahteva informacije o tome koje će se oblasti računara skenirati, pa je potrebno da unesete tačnu putanju do izabranog odeljka), vrednosti su odvojene tačkom i zarezom, npr.: **avgscanx /scan=C:\;D:**

Parametri skeniranja

Za prikazivanje celog pregleda dostupnih parametara otkucajte odgovarajuću komandu zajedno sa parametrom **/?** ili **/HELP** (npr. **avgscanx /?**). Jedini obavezni parametar je **/SCAN** kojim se određuju oblasti računara koje se skeniraju. Za detaljnije objašnjenje opcija pogledajte [pregled parametara komandne linije](#).

Da biste pokrenuli skeniranje, pritisnite taster **Enter**. U toku skeniranja, proces možete zaustaviti ako pritisnete kombinaciju tastera **Ctrl+C** ili **Ctrl+Pause**.

Pokretanje skeniranja iz komandne linije pomoću grafičkog interfejsa

Kada pokrenete računar u Windows bezbednom režimu, postoji i mogućnost pokretanja skeniranja iz komandne linije pomoću grafičkog interfejsa. Sâmo skeniranje se pokreće iz komandne linije, a dijalog **Sastavljač komandne linije** vam omogućava da navedete većinu parametara za skeniranje u komfornom grafičkom okruženju.

Budući da je ovaj dijalog dostupan samo u Windows bezbednom režimu, njegovo detaljno objašnjenje potražite u datoteci pomoći koja se otvara direktno iz dijaloga.

12.4.1. Parametri za skeniranje iz komandne linije

Sledi lista svih dostupnih parametara za skeniranje iz komandne linije:

- **/SCAN** [Skeniranje datoteka ili fascikli](#) **/SCAN=putanja;putanja** (npr. **/SCAN=C:\;D:**)
- **/COMP** [Skeniranje celog računara](#)
- **/HEUR** Koristi [heurističku analizu](#)
- **/EXCLUDE** Izuzmi putanju ili datoteke iz skeniranja



- **/@** Komandna datoteka /ime datoteke/
- **/EXT** Skeniraj ove oznake tipa /na primer, EXT=EXE,DLL/
- **/NOEXT** Ne skeniraj ove oznake /na primer, NOEXT=JPG/
- **/ARC** Skeniraj archive
- **/CLEAN** Automatski očisti
- **/TRASH** Premesti zaražene datoteke u [Skladište za viruse](#)
- **/QT** Brzi test
- **/LOG** Generiši datoteku sa rezultatima skeniranja
- **/MACROW** Prijavi makroe
- **/PWDW** Prijavi datoteke zaštićene lozinkom
- **/ARCBOMBSW** Izvesti o arhivama-bombama (*više puta komprimovane arhive*)
- **/IGNLOCKED** Zanimari zaključane datoteke
- **/REPORT** Izveštaj upiši u datoteku /ime datoteke/
- **/REPAPPEND** Dodaj u datoteku izveštaja
- **/REPOK** Prijavi da su datoteke koje nisu zaražene u redu
- **/NOBREAK** Onemogući prekidanje pomoću tastera CTRL-BREAK
- **/BOOT** Omogući MBR/BOOT proveru
- **/PROC** Skeniraj aktivne procese
- **/PUP** Izvesti o „[Potencijalno neželjenim programima](#)”
- **/PUPEXT** Izvesti o poboljšanom skupu [potencijalno neželjenih programa](#)
- **/REG** Skeniraj registrator
- **/COO** Skeniraj kolačiće
- **/?** Prikaži pomoć za ovu temu
- **/HELP** Prikaži pomoć za ovu temu
- **/PRIORITY** *Podesi prioritet skeniranja /Nizak, automatski, visok/ (pogledajte [Napredna podešavanja / Skeniranje](#))*



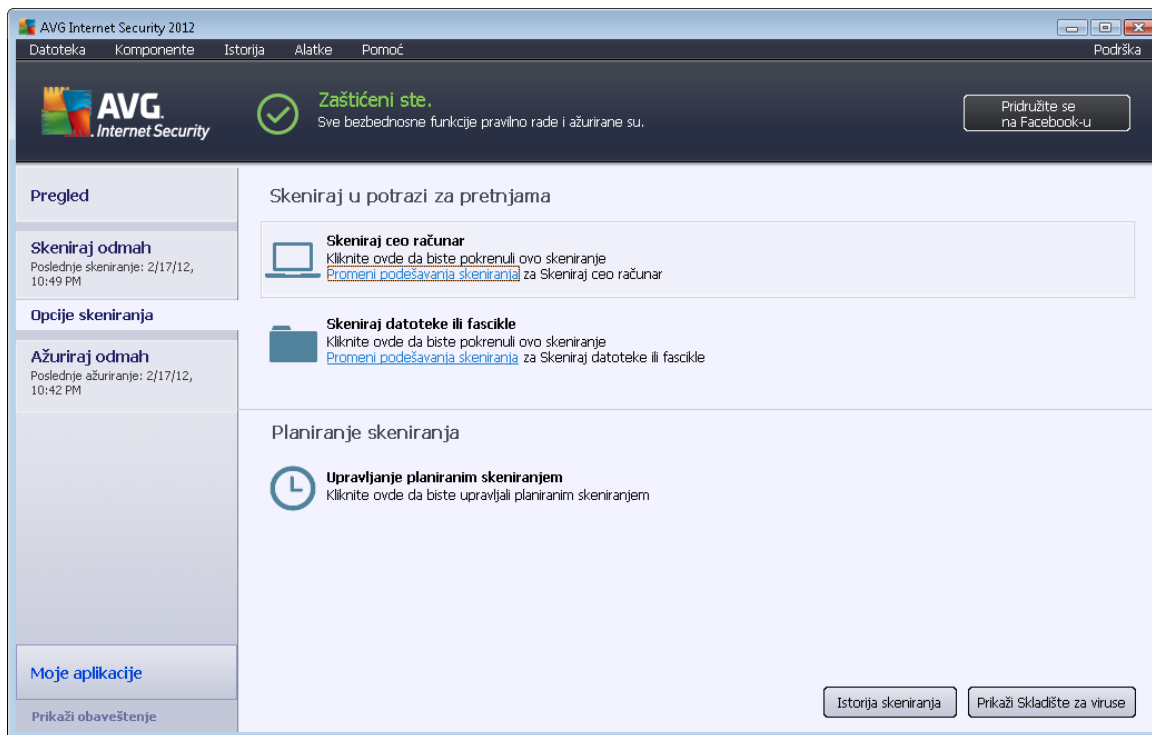
- **/SHUTDOWN** Isključi računar nakon završetka skeniranja
- **/FORCESHUTDOWN** Prinudno isključi računar nakon završetka skeniranja
- **/ADS** *Skeniraj alternativne tokove podataka (samo u NTFS sistemu)*
- **/HIDDEN** Izvesti o datotekama sa skrivenim oznakama tipa datoteka
- **/INFECTABLEONLY** Skeniraj samo datoteke sa oznakama tipa datoteka koje se mogu zaraziti
- **/THOROUGHSCAN** Omogući temeljno skeniranje
- **/CLOUDCHECK** Proveri da li postoje potvrđene greške
- **/ARCBOMBSW** Prijavi ponovo zapakovane datoteke arhive

12.5. Planiranje skeniranja

Program **AVG Internet Security 2012** vam omogućava da pokrenete skeniranje na zahtev (na primer, kada sumnjate da je infekcija prenesena na vaš računar) ili na osnovu plana. Preporučuje se da skeniranje obavljate po planu: na taj način možete biti sigurni da će vaš računar biti zaštićen od mogućnosti zaraze, a nećete morati da brinete ni o tome da li je potrebno pokrenuti skeniranje i kada.

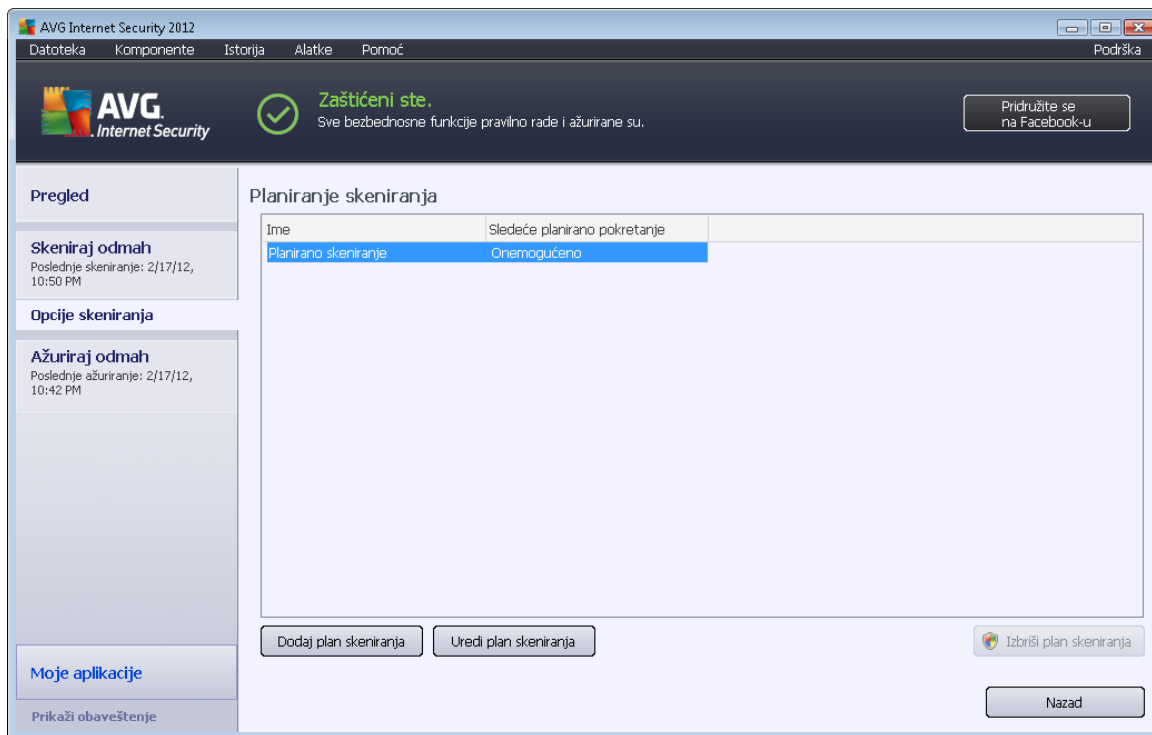
Trebalo bi redovno da pokrećete opciju [Skeniraj ceo računar](#), bar jednom nedeljno. Međutim, ako je moguće, pokrenite skeniranje celog računara jednom dnevno - kao što je podešeno u podrazumevanoj konfiguraciji plana za skeniranje. Ako računar držite stalno uključen, možete napraviti plan za skeniranje van radnih sati. Ako ponekad isključujete računar, zakažite skeniranje [po pokretanju računara, nakon propuštenog zadatka skeniranja](#).

Da biste kreirali novi plan skeniranja, pogledajte [AVG interfejs za skeniranje](#) pa u donjem delu pronađite odeljak **Plan skeniranja**:



Planiranje skeniranja

Kliknite na grafičku ikonu u odeljku **Planiranje skeniranja** da biste otvorili novi dijalog **Planiranje skeniranja** u kojem možete pronaći listu svih trenutno planiranih skeniranja:

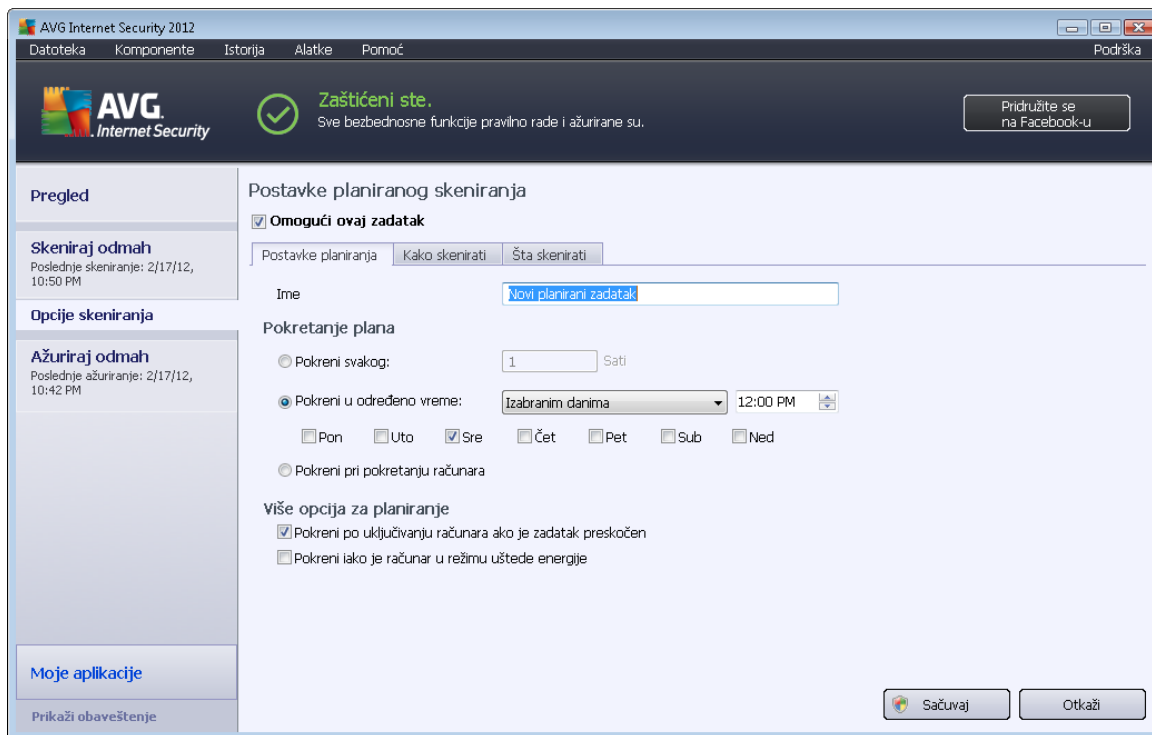


Možete da uredite / dodate skeniranja pomoću sledećih kontrolnih dugmadi:

- **Dodaj plan skeniranja** - služi za otvaranje kartice **Podešavanja planiranja** u dijalogu [Podešavanja za planiranje skeniranja](#). U ovom dijalogu možete navesti parametre za novodefinisani test.
- **Uredi plan skeniranja** - ovo dugme možete koristiti samo ako ste prethodno izabrali postojeći test iz liste planiranih testova. U tom slučaju dugme će biti aktivno i moći ćete da kliknete na njega da biste prešli na karticu [Podešavanja planiranja](#) u dijalogu **Podešavanja za planiranje skeniranja**. Parametri izabranog testa već su navedeni i moguće ih je urediti.
- **Izbriši plan skeniranja** - ovo dugme možete koristiti samo ako ste prethodno izabrali postojeći test iz liste planiranih testova. Ovaj test je moguće izbrisati iz liste tako što ćete kliknuti na kontrolno dugme. Međutim, možete uklanjati samo sopstvene testove; nije moguće izbrisati unapred definisani **Plan skeniranja celog računara** iz podrazumevanih podešavanja.
- **Nazad** - povratak u [AVG interfejs za skeniranje](#)

12.5.1. Postavke planiranja

Ako želite da isplanirate novi test i njegovo redovno pokretanje, otvorite dijalog **Postavke planiranog testa** (kliknite na dugme **Dodaj plan skeniranja** u dijalogu **Planiranje skeniranja**). Ovaj dijalog je podeljen u tri kartice: **Podešavanja planiranja** (pogledajte sliku ispod; podrazumevana kartica na koju ćete podrazumevano biti preusmereni), [Kako skenirati](#) i [Šta skenirati](#).



Na kartici **Podešavanja planiranja** možete prvo označiti/ponišiti izbor stavke **Omogući ovaj zadatak** da biste jednostavno deaktivirali zakazani test, a kasnije ga možete uključiti po potrebi.

Zatim imenujte način skeniranja koji kreirate i zakazujete. Unesite željeno ime u polje za tekst pored stavke **Ime**. Nastojte da koristite kratka, opisna i prikladna imena za načine skeniranja, kako biste kasnije lakše mogli da ih razlikujete jedne od drugih.

Primer: Nije dobro nazvati skeniranje „Novo skeniranje“ ili „Moje skeniranje“, pošto ta imena ne opisuju ono što se tim skeniranjem proverava. S druge strane, primer dobrog opisnog imena bio bi „Skeniranje sistemskih oblasti“ itd. Takođe, nije obavezno da u imenu skeniranja navedete da li je u pitanju skeniranje celog računara ili samo određenih datoteka ili fascikli - vaši načini skeniranja uvek će predstavljati određenu verziju skeniranja određenih datoteka ili fascikli.

U ovom dijalogu možete definisati sledeće parametre skeniranja:

- **Pokretanje plana** - navedite vremenske intervale za pokretanje novog plana skeniranja. Vremenski interval je moguće definisati uzastopnim pokretanjem skeniranja nakon određenog vremenskog perioda (**Pokreni svakih ...**), definisanjem tačnog datuma i vremena (**Pokreni u određeno vreme ...**) ili definisanjem događaja sa kojim bi trebalo povezati pokretanje skeniranja (**Radnja zasnovana na pokretanju računara**).
- **Napredne opcije za planiranje** - u ovom odeljku možete definisati pod kojim se okolnostima skeniranje pokreće/ne pokreće ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

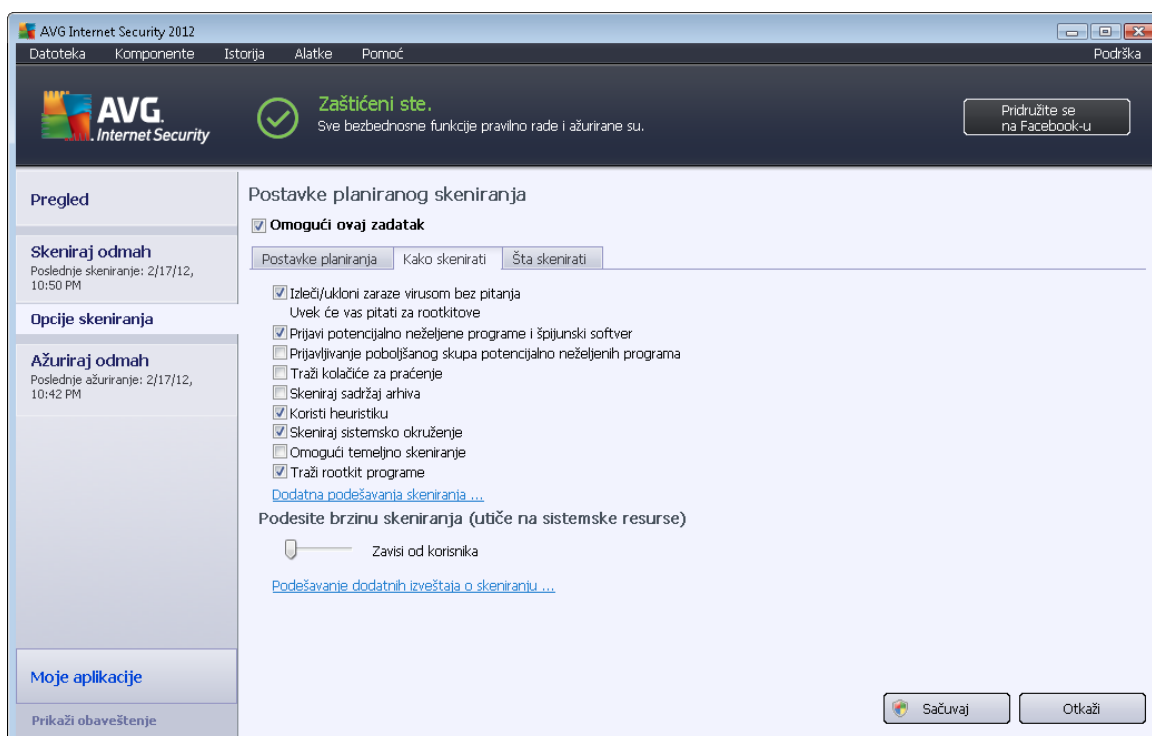
Kontrolna dugmad u dijalogu Podešavanja za planirano skeniranje



Dva kontrolna dugmeta dostupna su na sve tri kartice dijaloga **Podešavanja za planirano skeniranje** („[Podešavanja planiranja](#)“, „[Kako skenirati](#)“ i „[Šta skenirati](#)“) i ona imaju istu funkcionalnost, bez obzira na kojoj se kartici trenutno nalazite:

- **Sačuvaj** - čuva sve promene koje ste napravili na ovoj kartici ili na bilo kojoj drugoj kartici u ovom dijalogu i vraća vas na [podrazumevani dijalog AVG interfejsa za skeniranje](#). Stoga, ako želite da konfigurišete parametre testiranja na svim karticama, pritisnite ovo dugme da ih sačuvate tako nakon što ste uneli sve željene postavke.
- **Otkazi** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na [podrazumevani dijalog AVG interfejsa za skeniranje](#).

12.5.2. Kako skenirati



Na kartici **Kako skenirati** pronaći ćete listu parametara za skeniranje koje je moguće opcionalno uključiti ili isključiti. Većina parametara je podrazumevano uključena i primenjivaće se tokom skeniranja. Ukoliko nemate određen razlog da promenite te postavke, preporučuje se da zadržite unapred definisanu konfiguraciju:

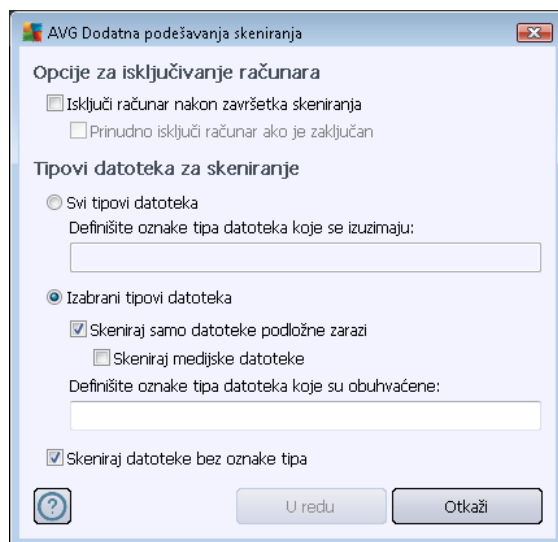
- **Izleči/ukloni virusnu infekciju bez upita** (podrazumevano uključeno): ako tokom skeniranja bude otkriven virus, moguće ga je automatski izlečiti ukoliko je dostupan lek. U slučaju da zaraženu datoteku nije moguće automatski izlečiti ili ako odlučite da isključite ovu opciju, nakon otkrivanja virusa dobićete obaveštenje, pa ćete morati da odlučite šta želite da uradite sa tom datotekom. Preporučena radnja je da zaraženu datoteku premestite u [Skladište za viruse](#).
- **Prijavi potencijalno neželjene programe i pretnje špijunskog softvera** (podrazumevano uključeno): označite radi aktivacije [Antispajver](#) mehanizma i skeniranja u potrazi za

špijunskim programima, kao i virusima. Špijunski softver se ne može sa sigurnošću svrstati u kategoriju malvera: iako obično predstavlja bezbednosni rizik, neki od ovih programa se mogu namerno instalirati. Preporučujemo vam da ova funkcija bude uključena, jer povećava bezbednost računara.

- **Prijavi poboljšani skup potencijalno neželjenih programa** (podrazumevano isključeno): označite radi detekcije proširenog paketa špijunskih programa: programi koji su potpuno u redu i bezopasni kada ih kupite direktno od proizvođača, ali se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Skeniraj kolačiće za praćenje** (podrazumevano isključeno): ovaj parametar komponente [Antispajver](#) definiše da bi tokom skeniranja trebalo otkrivati kolačiće (*HTTP kolačići služe za proveru identiteta, praćenje i održavanje određenih informacija o korisnicima, kao što su omiljene Web lokacije ili sadržaj njihovih elektronskih korpi za kupovinu*).
- **Skeniraj unutar arhiva** (podrazumevano isključeno): ovim parametrom se definiše da bi skeniranje trebalo da obuhvati sve datoteke, čak i ako su one zapakovane u nekom tipu arhive, npr. ZIP, RAR, ...
- **Koristi heuristiku** (podrazumevano uključeno): heuristička analiza (*dinamička emulacija naredbi skeniranih objekata u virtuelnom računarskom okruženju*) biće jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja.
- **Skeniraj sistemsko okruženje** (podrazumevano uključeno): skeniranje će obuhvatiti i sistemske oblasti vašeg računara.
- **Omogući temeljno skeniranje** (podrazumevano isključeno) - u posebnim situacijama (*ako sumnjate da je vaš računar zaražen*) možete označiti ovu opciju da aktivirate najtemeljnije algoritme za skeniranje, koji će skenirati čak i one oblasti na računaru koji se teško mogu zaraziti, radi predostrožnosti. Ipak, zapamtite da ovaj metod prilično dugo traje.
- **Skeniraj u potrazi za rootkit programima** (podrazumevano uključeno): [Anti-Rootkit](#) skeniranje na računaru pretražuje moguće rootkit programe, tj. programe i tehnologije koji mogu pokriti aktivnost malvera na računaru. Ako se otkrije rootkit program, to ne znači da je vaš računar zaražen. U nekim slučajevima, određeni upravljački programi ili delovi običnih aplikacija mogu biti pogrešno protumačeni kao rootkit programi.

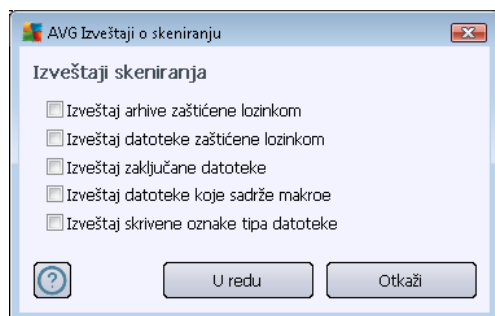
Potom možete da promenite konfiguraciju skeniranja na sledeći način:

- **Dodatne postavke skeniranja** - ovaj link otvara novi dijalog **Dodatne postavke skeniranja** u kojem možete da navedete sledeće parametre:



- **Opcije za isključivanje računara** - odlučite da li želite da se računar automatski isključi kada se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Isključi računar nakon završetka skeniranja**), aktiviraće se nova opcija koja omogućava da se računar isključi čak i ako je trenutno zaključan (**Prinudno isključi računar ako je zaključan**).
- **Tipovi datoteka za skeniranje** - uz to treba da odlučite da li želite da se skeniraju:
 - **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka koji se neće skenirati tako što ćete navesti listu oznaka tipa datoteke razdvojenih zarezima koje ne treba skenirati;
 - **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteke možete označiti datoteke koje treba uvek skenirati.
 - Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.
- **Podesi željenu brzinu završetka skeniranja** - možete da koristite klizač da izmenite prioritete procesa skeniranja. Vrednost ove opcije podrazumevano je postavljena na nivo automatske zauzetosti resursa koja *zavisí od korisnika*. Takođe, proces skeniranja možete usporiti, što znači da će zauzetost sistemskih resursa biti manja (*korisno ako morate da radite na računaru, a nije vam važno koliko će skeniranje trajati*), a možete ga i ubrzati, što zahteva više sistemskih resursa (*npr. kada se privremeno udaljite od računara*).

- **Podešavanje dodatnih izveštaja o skeniranju** - ovaj link otvara novi dijalog **Izveštaji skeniranja** u kojem možete da izaberete koji tip pronađenog sadržaja će se prijavljivati:

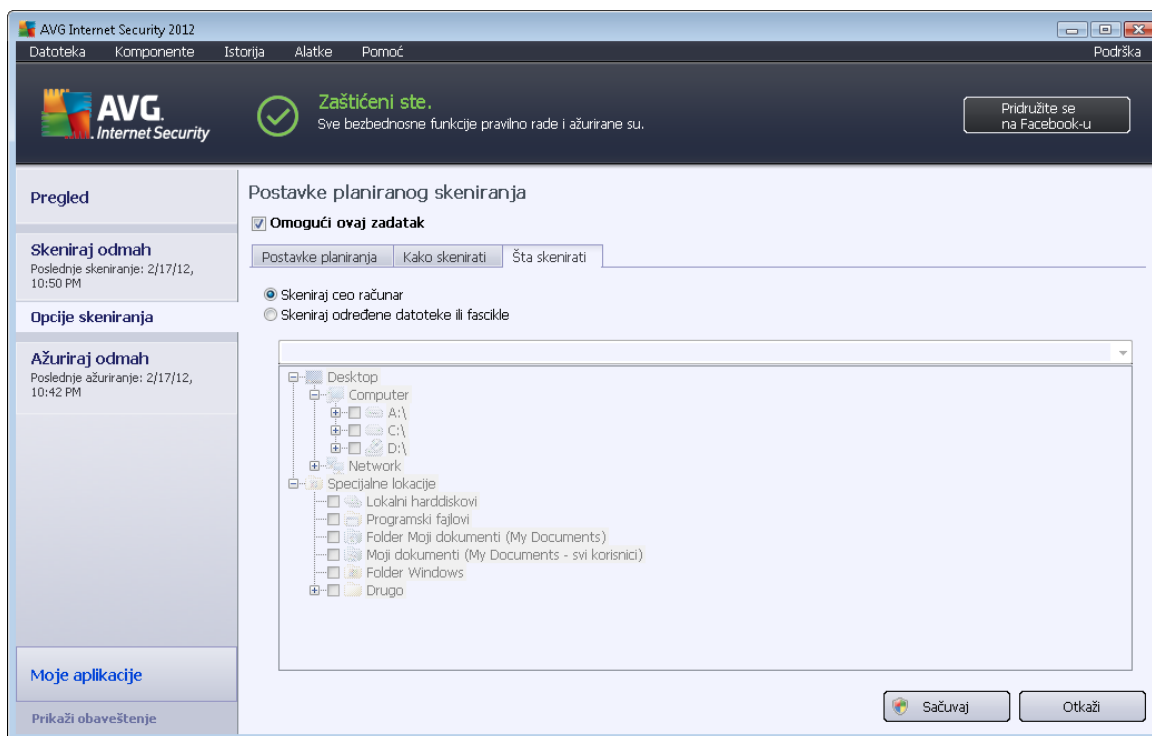


Kontrolna dugmad

Dva kontrolna dugmeta su dostupna na sve tri kartice dijaloga **Podešavanja za planirano skeniranje** („[Podešavanja planiranja](#)“, „[Kako skenirati](#)“ i „[Šta skenirati](#)“) i ona imaju istu funkcionalnost bez obzira na to na kojoj se kartici nalazite:

- **Sačuvaj** - čuva sve promene koje ste napravili na ovoj kartici ili na bilo kojoj drugoj kartici u ovom dijalogu i vraća vas na [podrazumevani dijalog AVG interfejsa za skeniranje](#). Stoga, ako želite da konfigurišete parametre testiranja na svim karticama, pritisnite ovo dugme da ih sačuvate tako nakon što ste uneli sve željene postavke.
- **Otkazi** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na [podrazumevani dijalog AVG interfejsa za skeniranje](#).

12.5.3. Šta skenirati



Na kartici **Šta skenirati**, možete definisati da li želite da zakažete [skeniranje celog računara](#) ili [skeniranje datoteka ili fascikli](#).

Ukoliko izaberete da želite da skenirate određene datoteke ili fascikle, u donjem delu ovog dijaloga prikazaće se prikaz strukture u obliku stabla u kome možete da izaberete fascikle koje želite da skenirate (*proširujte stavke tako što ćete kliknuti na znak sve dok ne pronađete fasciklu koju želite da skenirate*). Možete izabrati više fascikli tako što ćete označiti odgovarajuća polja. Izabrane fascikle pojaviće se u polju za tekst na vrhu dijaloga, a istorija izabranog skeniranja biće sačuvana u padajućem meniju za buduću upotrebu. Umesto toga, možete ručno uneti punu putanju do željene fascikle (*ako unesete više putanja, morate ih razdvojiti tačkom i zarezom, bez dodatnog razmaka između*).

U prikazu strukture u obliku stabla takođe možete da vidite granu **Posebne lokacije**. U nastavku sledi lista lokacija koje će se skenirati kada potvrdite izbor u odgovarajućem polju za potvrdu:

- **Lokalni čvrsti diskovi** - svi čvrsti diskovi na vašem računaru
- **Programske datoteke**
 - C:\Program Files\
 - u 64-bitnoj verziji C:\Program Files (x86)
- **Fascikla My Documents**



- za Win XP: C:\Documents and Settings\Default User\My Documents\
- za Windows Vista/7: C:\Users\user\Documents\

- **Deljena dokumenta**

- za Win XP: C:\Documents and Settings\All Users\Documents\
- za Windows Vista/7: C:\Users\Public\Documents\

- **Fascikla Windows** - C:\Windows\

- **Drugo**

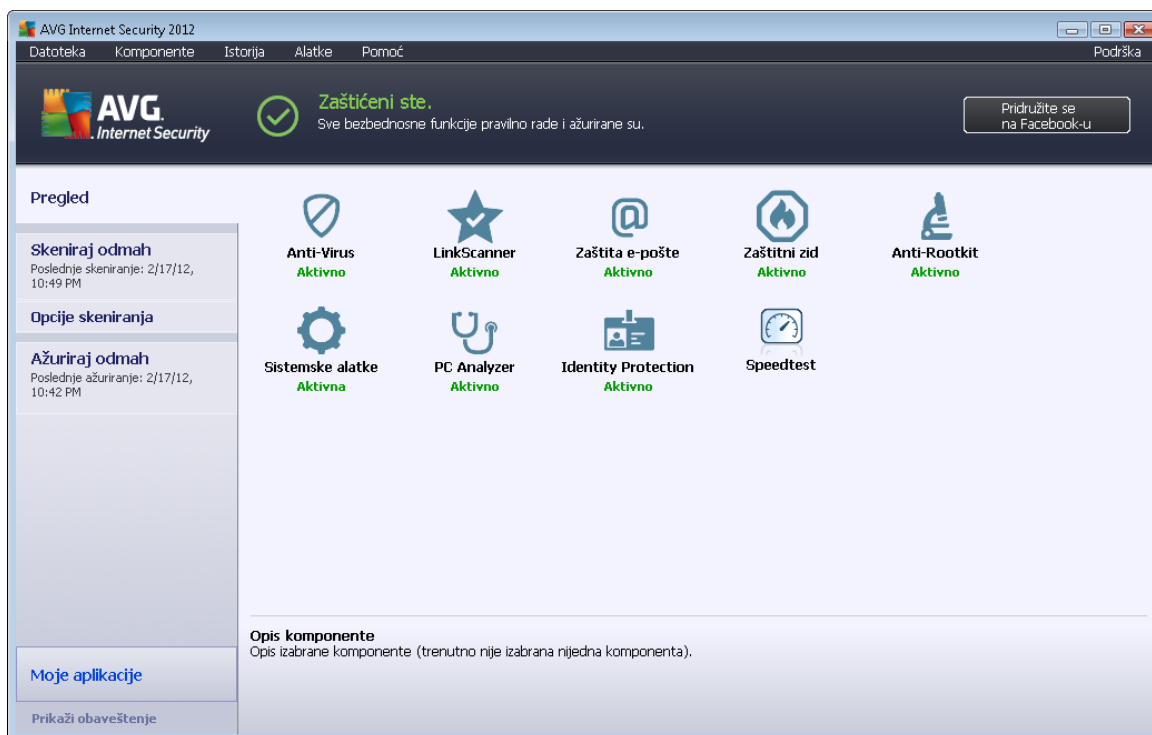
- *Sistemska disk jedinica* - čvrsti disk na kojem je instaliran operativni sistem (obično C:)
- *Sistemska fascikla* - C:\Windows\System32\
- *Fascikla za privremene datoteke* - C:\Documents and Settings\User\Local\ (Windows XP); ili C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- *Privremene Internet datoteke* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); ili C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

Kontrolna dugmad

Ista dva kontrolna dugmeta dostupna su na sve tri kartice dijaloga **Podešavanja planiranog skeniranja** ([Podešavanja planiranja](#), [Kako skenirati](#) i [Šta skenirati](#)):

- **Sačuvaj** - čuva sve promene koje ste napravili na ovoj kartici ili na bilo kojoj drugoj kartici u ovom dijalogu i vraća vas na [podrazumevani dijalog AVG interfejsa za skeniranje](#). Stoga, ako želite da konfigurirate parametre testiranja na svim karticama, pritisnite ovo dugme da ih sačuvate tako nakon što ste uneli sve željene postavke.
- **Otkazi** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na [podrazumevani dijalog AVG interfejsa za skeniranje](#).

12.6. Pregled rezultata skeniranja



Dijalogu **Pregled rezultata skeniranja** moguće je pristupiti iz [AVG interfejsa za skeniranje](#) pomoću dugmeta **Istorija skeniranja**. Dijalog sadrži listu svih prethodno pokrenutih skeniranja i informacije o njihovim rezultatima:

- **Ime** - odredište za skeniranje; to može biti ime nekog od [unapred definisanih skeniranja](#) ili ime koje ste dodelili sopstvenom [planiranom skeniranju](#). Svako ime sadrži i ikonu koja ukazuje na rezultat skeniranja:

 - zelena ikona ukazuje na to da tokom skeniranja nije otkrivena infekcija

 - plava ikona ukazuje na to da je tokom skeniranja otkrivena infekcija, ali je zaraženi objekat automatski uklonjen

 - crvena ikona upozorava na to da je tokom skeniranja otkrivena infekcija i da je nije bilo moguće ukloniti!

Svaka ikona može biti prikazana u celosti ili presečena na pola - ikone koje su predstavljene u celosti predstavljaju skeniranja koja su ispravno dovršena; presečena ikona ukazuje na to da je skeniranje otkazano ili prekinuto.

Napomena: Detaljne informacije o svakom skeniranju potražite u dijalogu [Rezultati skeniranja](#) kojem možete pristupiti pomoću dugmeta **Prikaži detalje** (u donjem delu ovog dijaloga).

- **Vreme početka** - datum i vreme pokretanja skeniranja



- **Vreme završetka** - datum i vreme završetka skeniranja
- **Testirani objekti** - broj objekata koji su pregledani tokom skeniranja
- **Zaraze** - broj otkrivenih/uklonjenih virusa
- **Špijunski softver** - broj otkrivenih/uklonjenih špijunskih programa
- **Upozorenja** - broj detektovanih [sumnjivih objekata](#)
- **Rootkit programi** - broj detektovanih [rootkit programa](#)
- **Informacije o evidenciji skeniranja** - informacije u vezi sa tokom skeniranja i rezultatima (uobičajeno po završetku ili po prekidanju)

Kontrolna dugmad

Kontrolna dugmad za dijalog **Pregled rezultata skeniranja** su:

- **Prikaži detalje** - kliknite na ovo dugme da biste se prebacili u dijalog [Rezultati skeniranja](#) i videli detaljne podatke o izabranom skeniranju
- **Izbriši rezultat** - kliknite na ovo dugme da biste uklonili izabranu stavku iz pregleda rezultata skeniranja
- **Nazad** - služi za vraćanje na podrazumevani dijalog [AVG interfejsa za skeniranje](#)

12.7. Detalji rezultata skeniranja

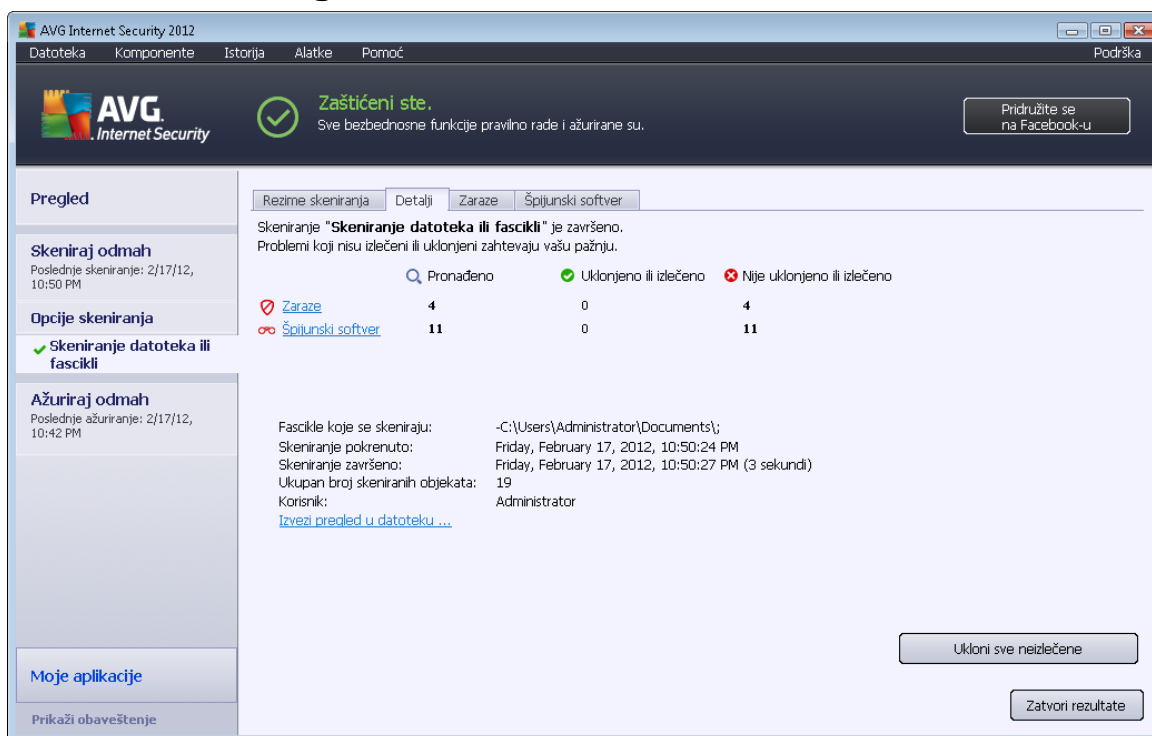
Ako u dijalogu [Pregled rezultata skeniranja](#) izaberite određeni način skeniranja, moći ćete da kliknete na dugme **Prikaži detalje** kako biste prešli u dijalog **Rezultati skeniranja** koji sadrži detaljne informacije o toku i rezultatu izabranog načina skeniranja. Ovaj dijalog je podeljen na nekoliko kartica:

- [Pregled rezultata](#) - ova kartica se sve vreme prikazuje, a sadrži statističke podatke o toku skeniranja
- [Zaraze](#) - ova kartica se prikazuje samo ako je u toku skeniranja detektovana zaraza virusom
- [Špijunski softver](#) - ova kartica se prikazuje samo ako je u toku skeniranja detektovan špijunski softver
- [Upozorenja](#) - ova kartica se prikazuje ako su, na primer, tokom skeniranja otkriveni kolačići
- [Rootkit programi](#) – ova kartica se prikazuje samo ako se tokom skeniranja detektuju rootkit programi
- [Informacije](#) - ova kartica se prikazuje samo ako su detektovane određene potencijalne pretnje koje ne spadaju u gornje kategorije; ova kartica sadrži poruku upozorenja u vezi sa pronađenom datotekom. Ovde ćete takođe pronaći informacije o objektima koji se ne mogu



skenirati (npr. archive zaštićene lozinkim).

12.7.1. Kartica Pregled rezultata



Na kartici **Rezultati skeniranja** nalaze se detaljni statistički podaci o:

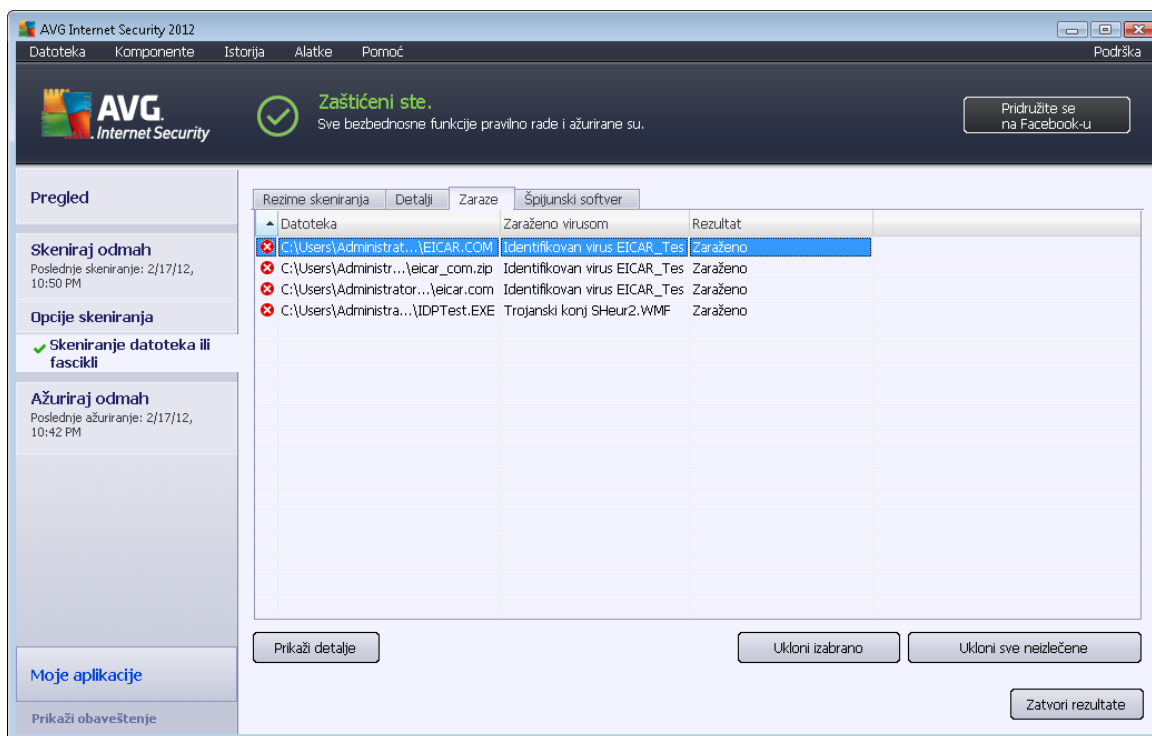
- otkrivenim zarazama virusom / špijunskim softverom
- uklonjenim zarazama virusom / špijunskim softverom
- broju zaraza virusom / špijunskim softverom koji se ne mogu ukloniti ili oporaviti

Osim toga, tu su i informacije o datumu i tačnom vremenu pokretanja skeniranja, ukupnom broj skeniranih objekata, trajanju skeniranja i broj grešaka koje su se javile u toku skeniranja.

Kontrolna dugmad

U ovom dijalogu nalazi se samo jedno kontrolno dugme: Dugme **Zatvori** služi za povratak u dijalog [Pregled rezultata skeniranja](#).

12.7.2. Kartica Zaraze



Kartica **Zaraze** prikazuje se u dijalogu **Rezultati skeniranja** samo ako je zaraza virusom detektovana u toku skeniranja. Kartica je podeljena na tri odeljka i pruža sledeće informacije:

- **Datoteka** - potpuna putanja do originalne lokacije zaraženog objekta
- **Zaraze** - ime detektovanog virusa (*detaljne informacije o konkretnim virusima potražite u [Enciklopediji virusa](#) na mreži*)
- **Rezultat** - definiše trenutni status zaraženog objekta koji je detektovan u toku skeniranja:
 - **Zaraženo** - zaraženi objekat je detektovan i ostavljen na originalnoj lokaciji (*na primer, ako ste [isključili opciju automatskog oporavka](#) u posebnim podešavanjima skeniranja*)
 - **Izlečeno** - zaraženi objekat je automatski izlečen i ostavljen je na originalnoj lokaciji
 - **Premešteno u skladište virusa** - zaraženi objekat je premešten u [Skladište virusa](#)
 - **Izbrisan** - zaraženi objekat je izbrisan
 - **Dodato u PUP izuzetke** - pronađeni objekat je prepoznat kao izuzetak i dodat na listu izuzetaka od potencijalno neželjenih programa (*koju ste podesili u dijalogu [Izuzeci od potencijalno neželjenih programa](#) u okviru naprednih podešavanja*)
 - **Zaključana datoteka - nije testirano** - pronađeni objekat je zaključan, pa ga AVG

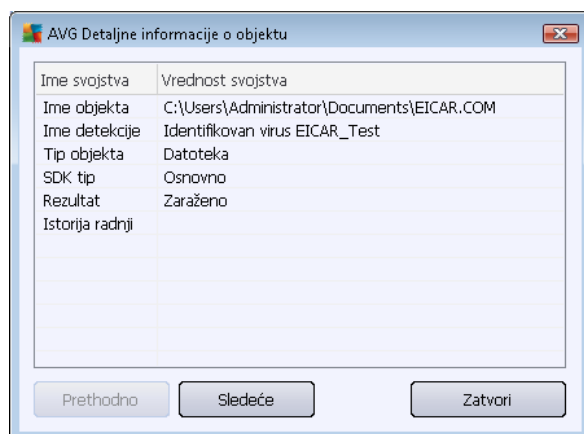
ne može skenirati

- **Potencijalno opasan objekat** - objekat je prepoznat kao potencijalno opasan, ali ne i zaražen (*npr. možda sadrži makroe*); ovu informaciju treba shvatiti samo kao upozorenje
- **Da bi se operacija dovršila, potrebno je da ponovo pokrenete računar** - nije moguće ukloniti zaraženi objekat, morate ponovo da pokrenete računar da biste ga uklonili

Kontrolna dugmad

U ovom dijalogu dostupna su tri kontrolna dugmeta:

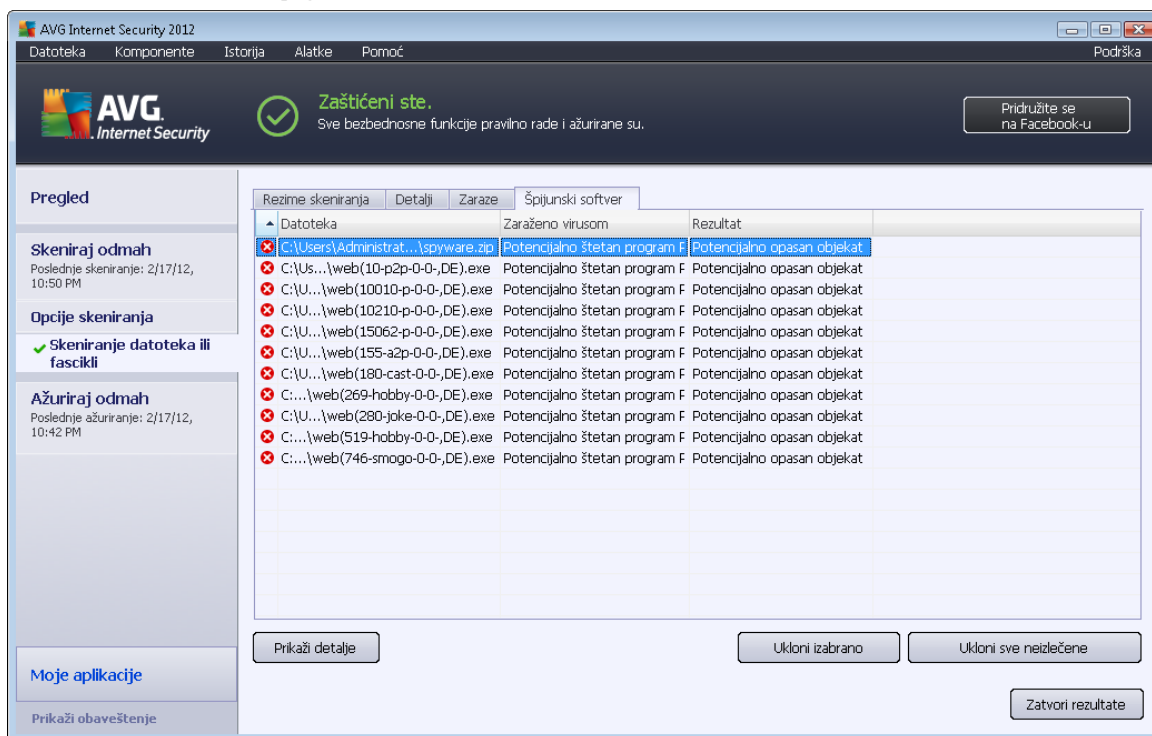
- **Vidi detalje** - dugme otvara novi prozor dijaloga nazvan **Detaljne informacije o objektu**:



U ovom dijalogu možete naći detaljne informacije o detektovanom zaraznom objektu (*npr. naziv i lokaciju zaraženog objekta, tip objekta, SDK tip, nalaz detekcije i istoriju radnji povezanih sa detektovanim objektom*). Pomoću dugmadi **Prethodno** / **Sledeće** možete prikazati informacije o željenim rezultatima. Pomoću dugmeta **Zatvori** možete zatvoriti dijalog.

- **Ukloni odabrano** - koristite ovo dugme da premestite odabrani nalaz u [Skladište virusa](#)
- **Ukloni sve neizlečeno** - ovo dugme briše sve nalaze koji se ne mogu izlečiti ili premestiti u [Skladište virusa](#)
- **Zatvori rezultate** - služi za zatvaranje pregleda detaljnih informacija i vraćanje u dijalog [Pregled rezultata skeniranja](#)

12.7.3. Kartica Špijunski softver



Kartica **Špijunski softver** prikazuje se u dijalogu **Rezultati skeniranja** samo ako je tokom skeniranja otkriven špijunski softver. Kartica je podeljena na tri odeljka i pruža sledeće informacije:

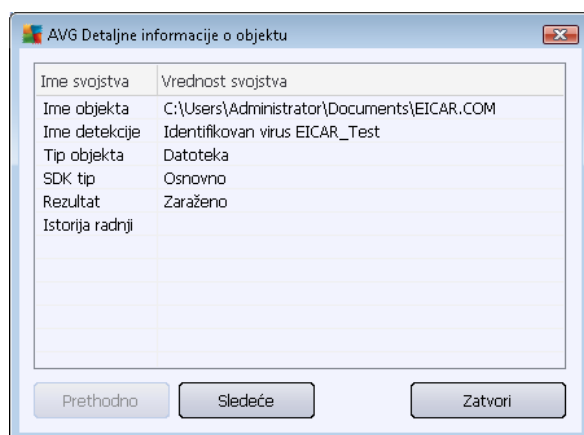
- **Datoteka** - potpuna putanja do originalne lokacije zaraženog objekta
- **Zaraze** - ime otkrivenog špijunskog softvera (*detalje o određenim virusima potražite u [Enciklopediji virusa](#) na mreži*)
- **Rezultat** - definiše trenutni status objekta koji je otkriven tokom skeniranja:
 - **Zaraženo** - zaraženi objekat je detektovan i ostavljen na originalnoj lokaciji (*na primer, ako ste [isključili opciju automatskog oporavka](#) u posebnim podešavanjima skeniranja*)
 - **Izlečeno** - zaraženi objekat je automatski izlečen i ostavljen je na originalnoj lokaciji
 - **Premešteno u skladište virusa** - zaraženi objekat je premešten u [Skladište virusa](#)
 - **Izbrisan** - zaraženi objekat je izbrisan
 - **Dodato u PUP izuzetke** - pronađeni objekat je prepoznat kao izuzetak i dodat na listu izuzetaka od potencijalno neželjenih programa (*koju ste podesili u dijalogu [Izuzeci od potencijalno neželjenih programa](#) u okviru naprednih podešavanja*)
 - **Zaključana datoteka - nije testirano** - objekat je zaključan pa AVG ne može da ga skenira

- **Potencijalno opasan objekat** - objekat je označen kao potencijalno opasan, ali nije zaražen (na primer, možda sadrži makroe); ovo je samo upozorenje
- **Da bi se operacija dovršila, potrebno je da ponovo pokrenete računar** - nije moguće ukloniti zaraženi objekat, morate da ponovo pokrenete računar da biste ga uklonili

Kontrolna dugmad

U ovom dijalogu dostupna su tri kontrolna dugmeta:

- **Vidi detalje** - dugme otvara novi prozor dijaloga nazvan **Detaljne informacije o objektu**:



U ovom dijalogu možete naći detaljne informacije o detektovanom zaraznom objektu (npr. naziv i lokaciju zaraženog objekta, tip objekta, SDK tip, nalaz detekcije i istoriju radnji povezanih sa detektovanim objektom). Pomoću dugmadi **Prethodno** / **Sledeće** možete prikazati informacije o željenim rezultatima. Pomoću dugmeta **Zatvori** možete zatvoriti ovaj dijalog.

- **Ukloni odabrano** - koristite ovo dugme da premestite odabrani nalaz u [Skladište virusa](#)
- **Ukloni sve neizlečeno** - ovo dugme briše sve nalaze koji se ne mogu izlečiti ili premestiti u [Skladište virusa](#)
- **Zatvori rezultate** - služi za zatvaranje pregleda detaljnih informacija i vraćanje u dijalog [Pregled rezultata skeniranja](#)

12.7.4. Kartica Upozorenja

Na kartici **Upozorenja** prikazane su informacije o „sumnjivim“ objektima (*najčešće datotekama*) koji su detektovani u toku skeniranja. Nakon detekcije komponentom Stalni štit, pristup tim datotekama je blokiran. Najčešći primeri za te objekte su: skrivene datoteke, kolačići, sumnjivi ključevi registratora, dokumenti ili arhive zaštićeni lozinkom itd. Te datoteke ne predstavljaju direktnu pretnju po vaš računar ili bezbednost. Informacije o tim datotekama obično su korisne ako se na računaru otkrije adware ili špijunski softver. Ako u rezultatima testa postoje samo upozorenja koja je otkrio **AVG Internet Security 2012**, nije potrebna nikakva radnja.



Ovo je kratak opis najčešćih primera takvih objekata:

- **Skrivene datoteke** - skrivene datoteke podrazumevano nisu vidljive u operativnom sistemu Windows, pa neki virusi ili druge pretnje mogu pokušati da izbegnu otkrivanje, tako što se smeštaju u datoteke sa ovim atributom. Ako **AVG Internet Security 2012** prijavi skrivenu datoteku za koju sumnjate da je zlonamerna, možete je premestiti u [skladište za viruse](#).
- **Kolačići** - kolačići su datoteke u formatu čistog teksta koje koriste Web lokacije za skladištenje specifičnih informacija o korisniku koje se kasnije koriste za učitavanje prilagođenog rasporeda Web lokacije, automatsko popunjavanje korisničkog imena itd.
- **Sumnjivi ključevi registratora** - određeni tipovi malvera skladište svoje informacije u registrator operativnog sistema Windows kako bi se one učitale prilikom pokretanja sistema ili kako bi proširili svoj efekat na operativni sistem.

12.7.5. Kartica Rootkit programi

Kartica **Rootkit programi** prikazuje informacije o rootkit programima otkrivenim tokom anti-rootkit skeniranja uključenog u [Skeniranje celog računara](#).

[Rootkit](#) je program osmišljen da preuzme potpunu kontrolu nad računarskim sistemom bez dozvole vlasnika sistema i administratora kojima je dozvoljen pristup. Pristup hardveru nije potreban jer je cilj rootkit programa da preuzme kontrolu nad operativnim sistemom koji je instaliran na hardveru. Rootkit programi najčešće prikrivaju svoje prisustvo na sistemu pomoću subverzije ili izbegavanja standardnih mehanizama za zaštitu operativnog sistema. Ti programi najčešće spadaju u red trojanskih konja, pa su u stanju da prevare korisnike kako bi poverovali da ih mogu bezbedno pokrenuti na sistemu. Tehnike kojima se to postiže obuhvataju prikrivanje aktivnih procesa kako ih ne bi videli programi za nadgledanje ili sakrivanje datoteka ili sistemskih podataka od operativnog sistema.

U osnovi ova kartica izgleda isto kao kartica [Zaraze](#) ili kartica [Špijunski softver](#).

12.7.6. Kartica Informacije

Na kartici **Informacije** nalaze se podaci o pronađenim objektima koji se ne mogu definisati kao zaraze virusom, špijunski softver itd. Ne mogu se obeležiti kao definitivno opasne, ali je potrebno da obratite pažnju na njih. **AVG Internet Security 2012** skeniranje može da otkrije datoteke koje možda nisu zaražene, ali su sumnjive. Za takve datoteke prikazuje se [Upozorenje](#) ili Informacija.

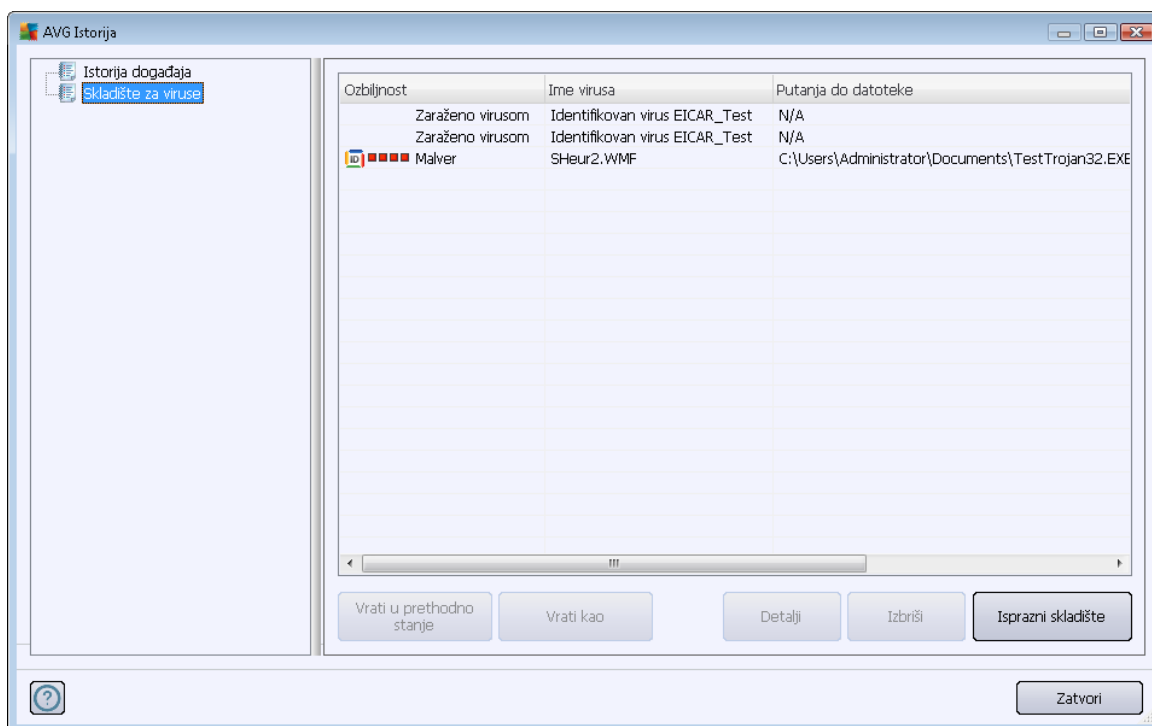
Ozbiljnost **Informacije** može da se prijavi iz nekog od sledećih razloga:

- **Zapakovan za izvršavanje** - datoteka je zapakovana jednim od manje uobičajenih programa za zapakivanje što može ukazati na pokušaj da se spreči skeniranje ovakve datoteke. Međutim, ne ukazuje svako otkrivanje ovakve datoteke na virus.
- **Rekurzivno zapakovan za izvršavanje** - slično kao gore navedeno samo što se manje sreće kod uobičajenog softvera. Takve datoteke su sumnjive i trebalo bi da razmislite o njihovom uklanjanju ili slanju na analizu.
- **Arhiva ili dokument zaštićen lozinkom** - datoteke zaštićene lozinkom ne može skenirati **AVG Internet Security 2012** (ili uopšte bilo koji drugi program za zaštitu od malvera).



- **Dokument sa makroima** - otkriveni dokument sadrži makroe koji mogu biti zlonamerni.
- **Skrivene oznake tipa datoteke** - datoteke sa skrivenim oznakama tipa datoteke mogu npr. izgledati kao datoteka slike, ali su u stvari izvršne datoteke (npr. *slika.jpg.exe*). Druga oznaka tipa datoteke podrazumevano nije vidljiva u operativnom sistemu Windows i **AVG Internet Security 2012** prijavljuje takve datoteke da bi se sprečilo njihovo slučajno otvaranje.
- **Neodgovarajuća putanja datoteke** - ako se neka važna sistemska datoteka pokreće sa putanje koja nije podrazumevana (npr. *winlogon.exe* se pokreće iz fascikle koja nije Windows fascikla), će prijaviti to neslaganje. **AVG Internet Security 2012** U nekim slučajevima, virusi koriste imena standardnih sistemskih procesa kako bi sakrili svoje prisustvo u sistemu.
- **Zaključana datoteka** - prijavljena datoteka je zaključana i ne može je skenirati **AVG Internet Security 2012**. To obično znači da neku datoteku neprekidno koristi sistem (npr. *datoteka virtuelne memorije*).

12.8. Skladište za viruse



Kartica Skladište za viruse predstavlja bezbedno okruženje za upravljanje sumnjivim/zaraženim objektima koji su otkriveni tokom AVG testova. Ako se tokom skeniranja pronađe zaraženi objekat, a AVG program ne može automatski da ga oporavi, od vas će se tražiti da odlučite šta ćete uraditi sa sumnjivim objektom. Preporučeno rešenje jeste da premestite objekat u **Skladište za viruse** radi njegovog daljeg tretiranja. Osnovna svrha **Skladišta za viruse** je čuvanje izbrisanih datoteka na određeni vremenski period, kako biste bili sigurni da vam više neće biti potrebne na prvobitnoj lokaciji. Ukoliko primetite da odsustvo datoteke izaziva probleme, možete poslati tu datoteku na



analizu ili možete da je vratite na prvobitnu lokaciju.

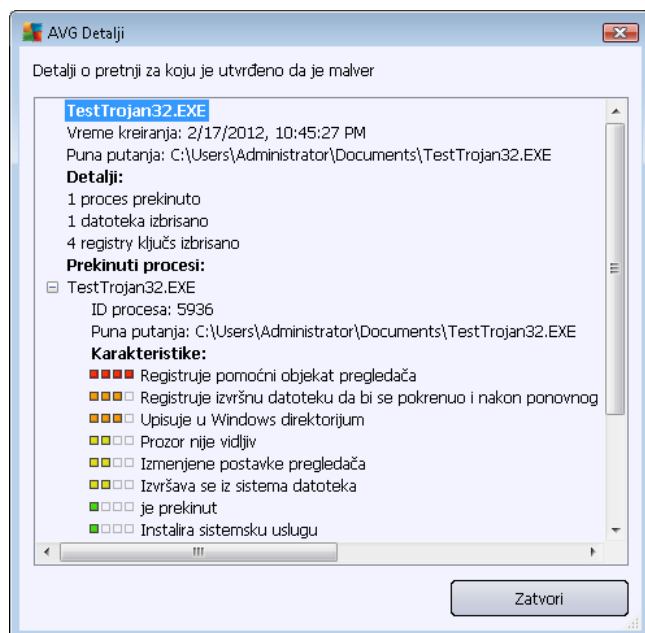
Interfejs komponente **Skladište za viruse** otvara se u novom prozoru i sadrži pregled informacija o zaraženim objektima koji su stavljeni u karantin.

- **Ozbiljnost** - ako ste odlučili da instalirate komponentu [Identity Protection](#) u okviru programa **AVG Internet Security 2012**, u ovom odeljku će se nalaziti grafički prikaz pronađene pretnje na skali od četiri nivoa, od bezopasne (■□□□) pa do veoma opasne (■□■□), kao i informacije o tipu zaraze (*na osnovu njene zarazne moći, objekti na listi mogu biti zaraženi ili potencijalno zaraženi*)
- **Ime virusa** - navodi ime detektovane zaraze na osnovu [Enciklopedije virusa](#) (*na mreži*)
- **Putanja do datoteke** - puna putanja do originalne lokacije detektovane zarazne datoteke
- **Originalno ime objekta** – svi detektovani objekti navedeni na grafikonu označeni su standardnim imenom koje im daje AVG tokom procesa skeniranja. Ukoliko je objekat imao neko određeno originalno ime koje je poznato (*npr. ime priloga e-poruke koje ne odgovara stvarnom sadržaju priloga*), ono će biti navedeno u ovoj koloni.
- **Datum skladištenja** - datum i vreme kada je sumnjiva datoteka detektovana i premeštena u Skladište za viruse

Kontrolna dugmad

U interfejsu komponente **Skladište za viruse** dostupna su sledeća kontrolna dugmad:

- **Vrati u prethodno stanje** - vraća zaraženu datoteku na originalnu lokaciju na disku
- **Vrati kao** – zaražena datoteka se premešta u izabranu fasciklu
- **Detalji** – ovo dugme se odnosi samo na pretnje koje je otkrila komponenta [Identity Protection](#). Kada kliknete na njega, prikazuje se pregled detalja o pretnji (*datoteke/procesi koji su ugroženi, karakteristike procesa itd.*). Imajte u vidu da je ovo dugme aktivno samo za stavke koje je otkrila komponenta „Identity Protection“!



- **Izbriši** - potpuno i nepovratno uklanjanje zaražene datoteke iz **Skladišta za viruse**
- **Isprazni skladište za viruse** - uklanja iz **Skladišta za viruse** sadržajkompletno. Kada uklonite datoteke iz **Skladišta za viruse**, one su nepovratno uklonjenje sa diska (*nisu premeštene u korpu za otpatke*).



13. Ažuriranje programa AVG

Nijedan bezbednosni softver ne može garantovati pouzdanu zaštitu od raznih vrsta pretnji ako se redovno ne ažurira! Kreatori virusa stalno traže nove propuste u softveru i operativnim sistemima koje mogu da iskoriste. Svakodnevno se pojavljuju novi virusi, novi malver, novi napadi sa mreže. Zato proizvođači softvera redovno izdaju sadržaje za ažuriranje i bezbednosne zakrpe za ispravljanje otkrivenih propusta u bezbednosti.

Imajući u vidu sve nove računarske pretnje koje se pojavljuju i brzinu kojom se šire, apsolutno je neophodno redovno ažurirati **AVG Internet Security 2012**. Najbolje rešenje je držati se podrazumevanih podešavanja programa u kojima je konfigurisano automatsko ažuriranje. Imajte u vidu da ako baza podataka virusa programa **AVG Internet Security 2012** nije ažurirana, program neće moći da otkrije najnovije pretnje!

Od ključnog je značaja da redovno ažurirate program AVG! Ažuriranje osnovnih definicija virusa trebalo bi da se obavlja svakodnevno, ako je moguće. Manje hitno ažuriranje programa može se obavljati jednom nedeljno.

13.1. Pokretanje ažuriranja

Da bi se obezbedila maksimalna dostupna bezbednost, **AVG Internet Security 2012** je podrazumevano podešen da traži novo ažuriranje na svaka četiri časa. Pošto se AVG ažuriranje ne objavlja po nekom fiksnom planu, već kao reakcija na količinu i ozbiljnost novih pretnji, ova provera je izuzetno važna da biste se uverili da je AVG baza podataka o virusima u svakom trenutku ažurirana.

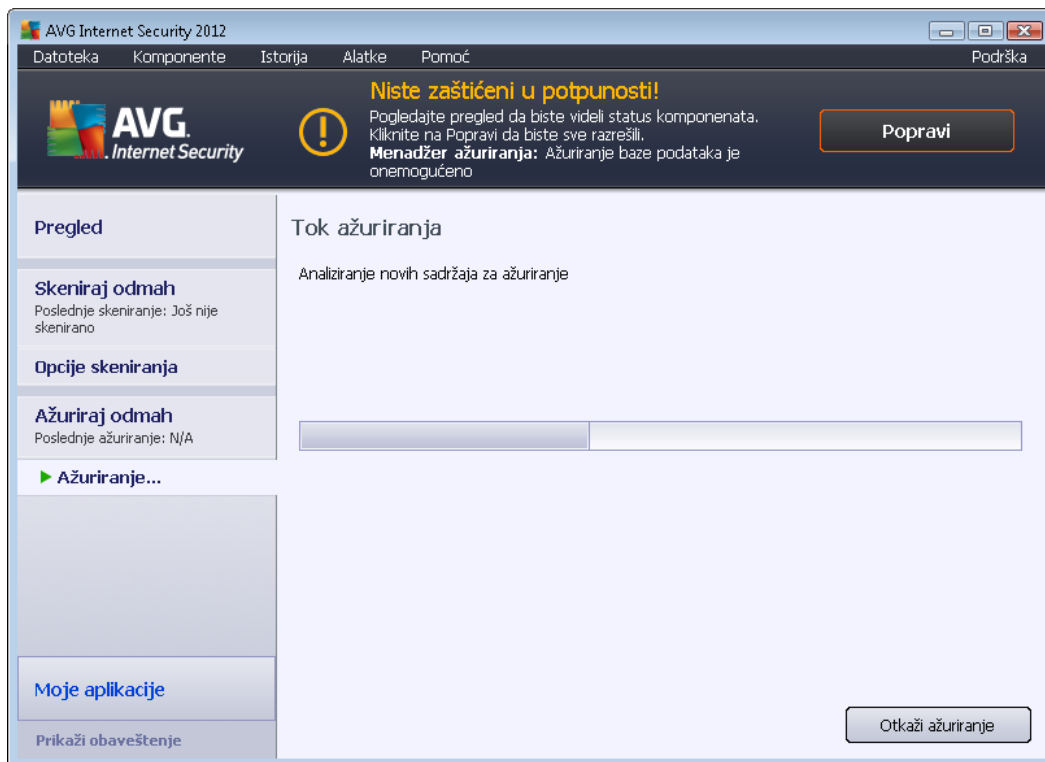
Ako želite da smanjite broj pokretanja ažuriranja, možete podesiti sopstvene parametre pokretanja. Međutim, preporučuje se da ažuriranje pokrećete makar jednom dnevno! Konfiguracija se može urediti u odeljku [Napredna podešavanja/Planiranja](#), konkretno u sledećim dijalozima:

- [Plan ažuriranja definicija](#)
- [Plan ažuriranja programa](#)
- [Plan ažuriranja komponente Odbrana od bezvredne pošte](#)

U slučaju da želite odmah da proverite nove datoteke za ažuriranje, koristite brzu vezu [Ažuriraj odmah](#) u glavnom korisničkom interfejsu. Ova veza je dostupna u svakom trenutku iz bilo kojeg dijaloga u [korisničkom interfejsu](#).

13.2. Tok ažuriranja

Kada pokrenete ažuriranje, AVG će prvo proveriti da li su dostupne nove datoteke za ažuriranje. Ako jesu, **AVG Internet Security 2012** pokreće preuzimanje datoteka za ažuriranje, a zatim i sam proces ažuriranja. Tokom procesa ažuriranja bićete preusmereni na interfejs za **Ažuriranje** gde možete videti grafički prikaz toka procesa, kao i pregled odgovarajućih statističkih parametara (*veličina datoteke za ažuriranje, preuzeti podaci, brzina preuzimanja, proteklo vreme, ...*):



Napomena: pre svakog pokretanja ažuriranja AVG programa kreira se tačka vraćanja sistema. U slučaju da proces ažuriranja otkáže i operativni sistem padne, uvek ga možete vratiti u originalnu konfiguraciju iz ove tačke. Ovoj opciji se pristupa putem Windows menija: Start / Svi programi / Pribor / Sistemske alatke / Vraćanje sistema. Preporučuje se samo za iskusne korisnike!

13.3. Nivoi ažuriranja

AVG Internet Security 2012 nudi izbor od dva nivoa ažuriranja:

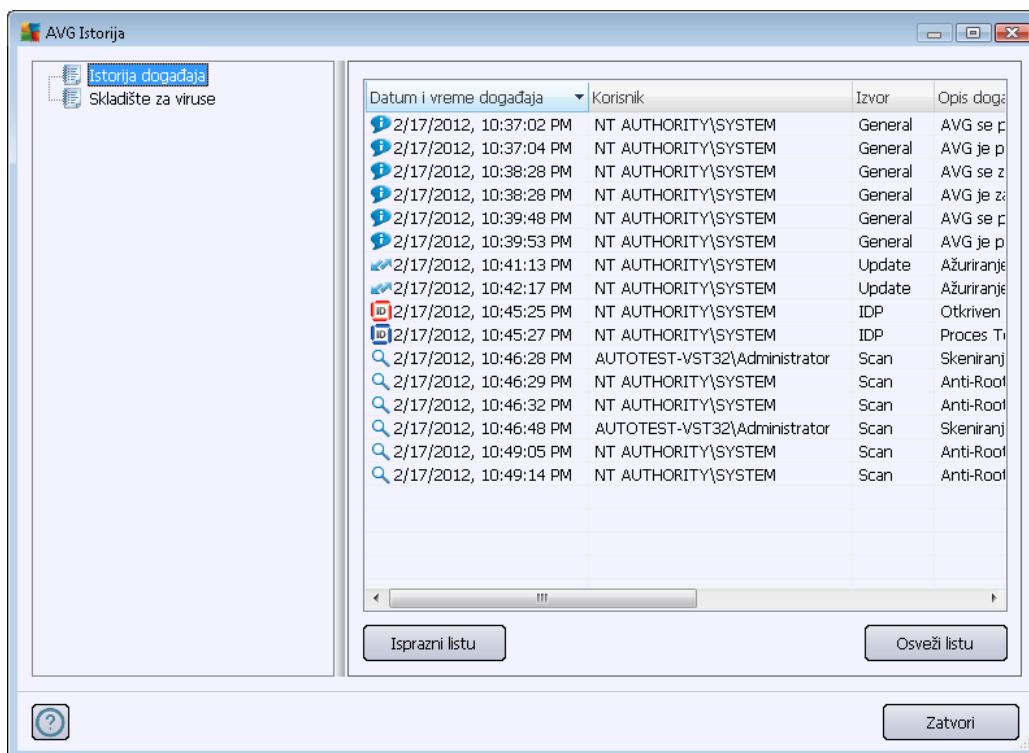
- **Ažurirane definicije** sadrže promene neophodne za pouzdanu zaštitu od virusa, neželjene pošte i malvera. Ono obično ne sadrži promene koda i ažurira samo bazu podataka definicija. Ovu ispravku bi trebalo primeniti čim postane dostupna.
- **Ažuriranje programa** sadrži različite promene, ispravke i poboljšanja za program.

Prilikom [planiranja ažuriranja](#), moguće je definisati specifične parametre za oba nivoa ažuriranja:

- [Plan ažuriranja definicija](#)
- [Plan ažuriranja programa](#)

Napomena: Ako dođe do podudaranja u vremenu planiranog ažuriranja programa i planiranog skeniranja, proces ažuriranja ima veći prioritet, pa će skeniranje biti prekinuto.

14. Istorija događaja



Dijalogu **Istorija** se može pristupiti iz [sistemskog menija](#) putem stavke **Istorija/Evidencija istorije događaja**. U ovom dijalogu se nalazi rezime važnih događaja do kojih je došlo tokom rada programa **AVG Internet Security 2012**. **Istorija** beleži sledeće tipove događaja:

- Informacije o ispravkama za AVG aplikaciju
- Informacije o početku, završetku ili zaustavljanju skeniranja (*uključujući automatski izvršene testove*)
- Informacije o događajima povezanim sa otkrivanjem virusa (*pomoću komponente [Stalni štiti](#) ili [skeniranjem](#)*), uključujući lokaciju događaja
- Druge važne događaje

Za svaki događaj, navode se sledeće informacije:

- **Datum i vreme događaja** daje tačan datum i vreme događaja
- **Korisnik** navodi ime korisnika koji je trenutno prijavljen u vreme događaja
- **Izvor** daje informacije o izvornoj komponenti ili drugom delu AVG sistema koji je aktivirao događaj
- **Opis događaja** daje rezime događaja



Kontrolna dugmad

- ***Isprazni listu*** – kliknite na dugme da biste izbrisali sve stavke sa liste događaja
- ***Osveži listu*** – kliknite na dugme da biste ažurirali sve stavke sa liste događaja

15. Najčešća pitanja i tehnička podrška

Ako budete imali prodajne ili tehničke probleme u vezi sa aplikacijom **AVG Internet Security 2012**, postoji nekoliko načina na koje možete potražiti pomoć. Izaberite neku od sledećih opcija:

- **Pronalaženje podrške:** direktno iz AVG aplikacije možete doći do stranice posvećene podršci za korisnike na AVG Web lokaciji (<http://www.avg.com/>). Izaberite stavku glavnog menija **Pomoć / Pronalaženje podrške** da biste bili preusmereni na AVG Web lokaciju sa dostupnim stranicama podrške. Da biste nastavili, sledite uputstva na Web stranici.
- **Podrška (veza u glavnom meniju):** Meni aplikacije AVG (na vrhu glavnog korisničkog interfejsa) sadrži vezu **Podrška** koja otvara novi dijalog sa svim tipovima informacija koje vam mogu biti potrebne pri pokušaju pronalaženja pomoći. Dijalog uključuje osnovne podatke o instaliranom AVG programu (verzija programa/baze podataka), detalje o licenci i listu brzih veza za podršku:



- **Rešavanje problema u datoteci pomoći:** novi odeljak **Rešavanje problema** je dostupan direktno u datoteci pomoći uključenoj u **AVG Internet Security 2012** (da biste otvorili datoteku u pomoći, pritisnite taster **F1** u bilo kom dijalogu u aplikaciji). Ovaj odeljak obezbeđuje listu situacija do kojih najčešće dolazi kada korisnik želi da potraži profesionalnu pomoć za tehnički problem. Izaberite situaciju koja najbolje opisuje vaš problem i kliknite na nju da biste otvorili detaljna uputstva koja vode do rešavanja problema.
- **Centar za podršku AVG Web lokacije:** Alternativno tome, možete da potražite rešenje za problem na AVG Web lokaciji (<http://www.avg.com/>). U odeljku **Centar za podršku** možete da pronađete strukturirani pregled tematskih grupa koje obrađuju prodajne i tehničke probleme.
- **Najčešća pitanja:** Na AVG Web lokaciji (<http://www.avg.com/>) takođe možete da pronađete



zaseban i bogato strukturirani odeljak sa najčešćim pitanjima. Ovom odeljku se može pristupiti preko opcije menija **Centar za podršku/Najčešća pitanja**. Još jednom, sva pitanja su na dobro organizovan način podeljena na kategorije prodaje, tehničkih pitanja i virusa.

- **Osnovni podaci o virusima i pretnjama:** posebno poglavlje AVG Web lokacije (<http://www.avg.com/>) je posvećeno problemima u vezi sa virusima (*Web stranici se pristupa iz glavnog menija putem opcije Pomoć / Osnovni podaci o virusima i pretnjama*). U meniju, izaberite stavku **Centar za podršku/Osnovni podaci o virusima i pretnjama** da biste otišli na stranicu koja obezbeđuje strukturirani pregled informacijau vezi sa sa pretnjama na mreži. Takođe možete da pronađete uputstva za uklanjanje virusa, špijunskog softvera i savete o tome kako da budete zaštićeni.
- **Forum za diskusiju:** Možete da koristite i forum za diskusiju AVG korisnika na adresi <http://forums.avg.com>.