AVG Internet Security 2011

Priručnik za korisnike

Revizija dokumenta 2011.21 (16.5.2011)

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

Ovo korisničko uputstvo sadrži sveobuhvatnu dokumentaciju za **AVG Internet Security 2011**.

Čestitamo vam na kupovini programa AVG Internet Security 2011!

AVG Internet Security 2011 predstavlja deo asortimana nagrađivanih AVG proizvoda, osmišljenih da bi ste vi mogli da budete bezbrižni, znajući da je vaš računar potpuno zaštićen. Kao i svi AVG proizvodi, **AVG Internet Security 2011** je redizajniran od samog temelja, kako bi se čuvena AVG zaštita obezbeđivala na nov, jednostavniji i efikasniji način. Vaš novi **AVG Internet Security 2011** proizvod odlikuje se svedenim interfejsom u kombinaciji sa agresivnijim i bržim skeniranjem. Radi veće praktičnosti, automatizovano je još nekoliko bezbednosnih funkcija, a dodate su i nove inteligentne korisničke opcije kako biste bezbednosne funkcije mogli da prilagodite svom načinu života. Nema više kompromisa po pitanju bezbednosti kako bi se pojednostavilo korišćenje!

Program AVG je osmišljen i razvijen kako bi zaštitio vaše računarske i mrežne aktivnosti. Uživajte u potpunoj zaštiti koju nudi AVG.

Sve ponude AVG proizvoda

- Zaštita koja je bitna za način na koji koristite vaš računar i Internet: bankarstvo i kupovina, surfovanje i pretraga, ćaskanje i e-pošta ili preuzimanje datoteka i društveno umrežavanje - AVG ima proizvod za zaštitu koji je po vašoj meri
- Zaštita bez muke kojoj veruje preko 110 miliona ljudi širom sveta i podsticana od strane globalne mreže izuzetno iskusnih istraživača
- Zaštita koja ima dvadesetočasovnu stručnu podršku

2. Zahtevi za instalaciju programa AVG

2.1. Podržani operativni sistemi

AVG Internet Security 2011 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 Zaštita identiteta nije podržana u operativnom sistemu Windows XP x64. Na ovom operativnom sistemu možete da instalirate AVG Internet Security 2011, ali bez komponente Zaštita identiteta.*

2.2. Minimalni i preporučeni hardverski zahtevi

Minimalni hardverski zahtevi za **AVG Internet Security 2011**:

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

Preporučeni hardverski zahtevi za **AVG Internet Security 2011**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM memorije
- 1400 MB slobodnog prostora na čvrstom disku (za instalaciju)

3. Opcije za instalaciju programa AVG

AVG se može instalirati putem instalacione datoteke koja se nalazi na instalacionom CD-u ili tako što ćete preuzeti najnoviju instalacionu datoteku sa AVG Web lokacije (http://www.avg.com/).

Pre nego što počnete da instalirate AVG, preporučujemo vam da posetite AVG Web lokaciju (http://www.avg.com/) da biste proverili da li postoji nova instalaciona datoteka. Na taj način ćete biti sigurni da ćete instalirati najnoviju verziju programa AVG Internet Security 2011.

Tokom procesa instalacije bićete upitani za broj licence/prodajni broj. Pre nego što započnete instalaciju, uverite se da je taj broj dostupan. Prodajni broj možete pronaći na pakovanju CD-a. Ako ste svoj primerak AVG programa kupili na mreži, broj licence dostavljen vam je e-poštom.

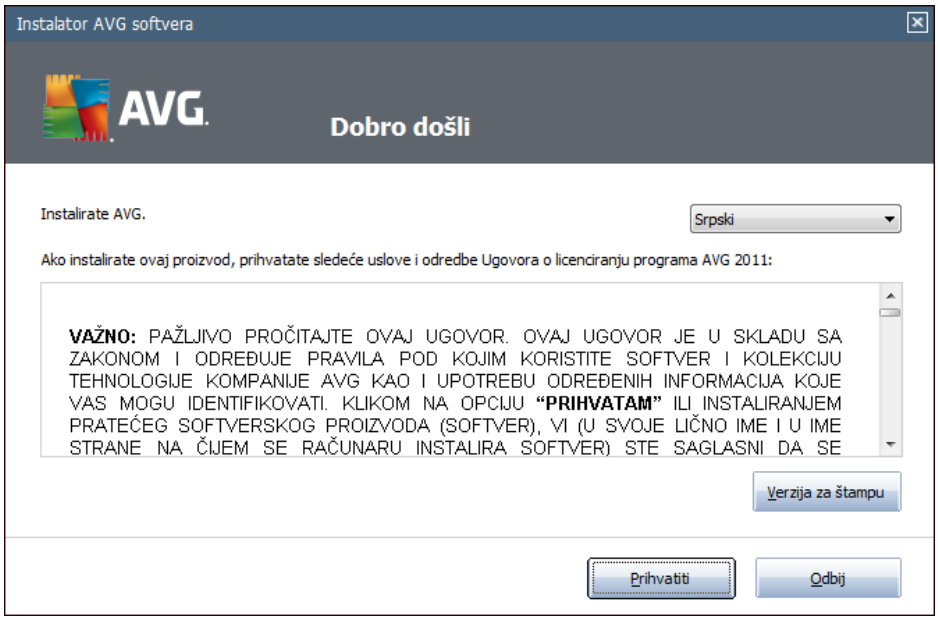
4. Proces instalacije programa AVG

Da biste instalirali **AVG Internet Security 2011** na svoj računar, potrebna vam je najnovija instalaciona datoteka. Možete da upotrebite instalacionu datoteku sa CD-a iz kompleta, ali postoji mogućnost da je zastarela. Zato vam preporučujemo da preuzmete najnoviju instalacionu datoteku sa mreže. Datoteku možete da preuzmete sa Web lokacije kompanije AVG (http://www.avg.com/), odeljak ***Centar za podršku / Preuzimanje.***

Instalaciju čini niz dijaloga sa kratkim opisom radnji koje bi trebalo da preduzmete u tom koraku. U nastavku teksta nalaze se objašnjenja svih dijaloga:

4.1. Dobro došli

Proces instalacije počinje prozorom ***Dobro došli*** . Ovde možete izabrati koji ćete jezik koristiti za proces instalacije i podrazumevani jezik AVG korisničkog interfejsa. U gornjem odeljku prozora nađite padajući meni sa spiskom jezika koje možete birati:



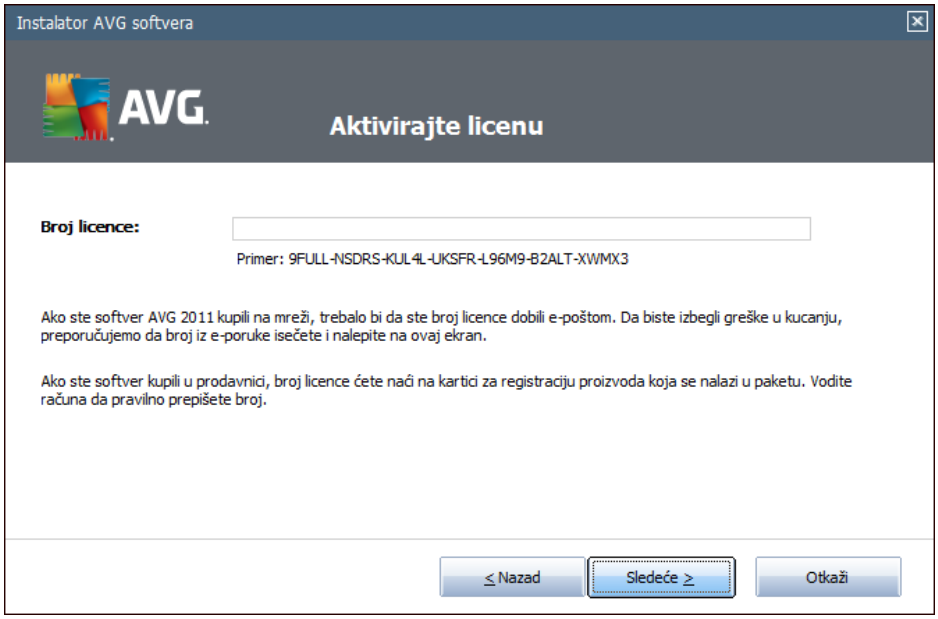
Pažnja: *Ovde je potrebno da izaberete jezik za proces instalacije. Jezik koji odaberete će biti instaliran kao podrazumevani jezik za AVG korisnički interfejs, zajedno sa engleskim koji se instalira automatski. Ukoliko želite da budu instalirani i drugi, dodatni jezici za korisnički interfejs, definišite ih u okviru jednog od sledećih dijaloga za podešavanje pod imenom* ***Prilagođene opcije****.*

Uz to, ovaj dijalog sadrži kompletnu verziju AVG ugovora o licenciranju. Molimo vas da ga pažljivo pročitate. 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.

4.2. Aktivirajte AVG licencu

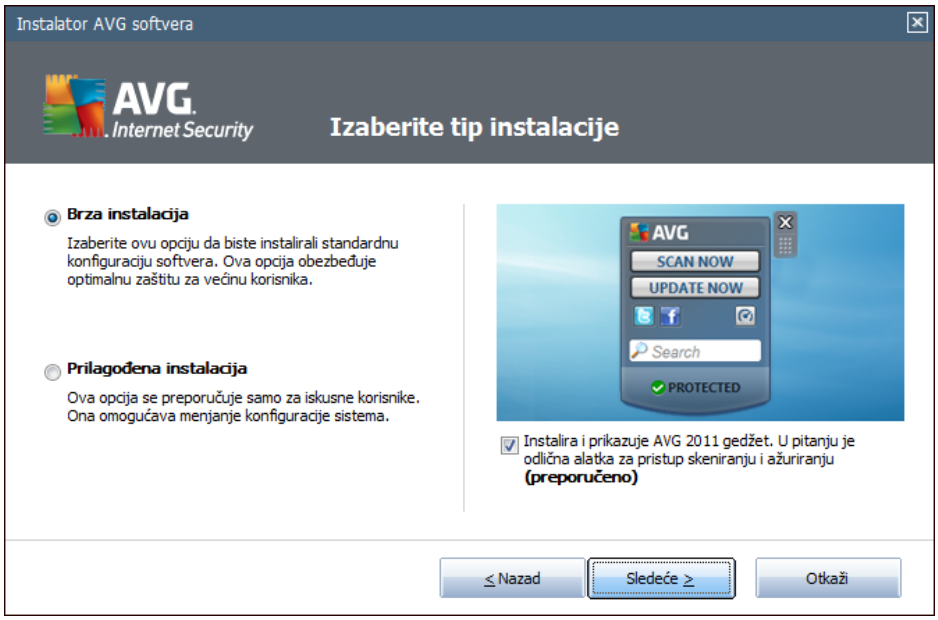
U dijalogu ***Aktivirajte vašu licencu*** pozivate se da unesete broj vaše licence u ponuđeno tekstualno polje.

Prodajni broj se nalazi na pakovanju CD-a u kutiji programa **AVG Internet Security 2011** . Broj licence će se nalaziti u potvrdnoj e-poruci koju ste dobili nakon kupovine programa **AVG Internet Security 2011** 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.



Pritisnite dugme ***Sledeće*** da biste nastavili sa procesom instalacije.

4.3. Izaberite tip instalacije



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

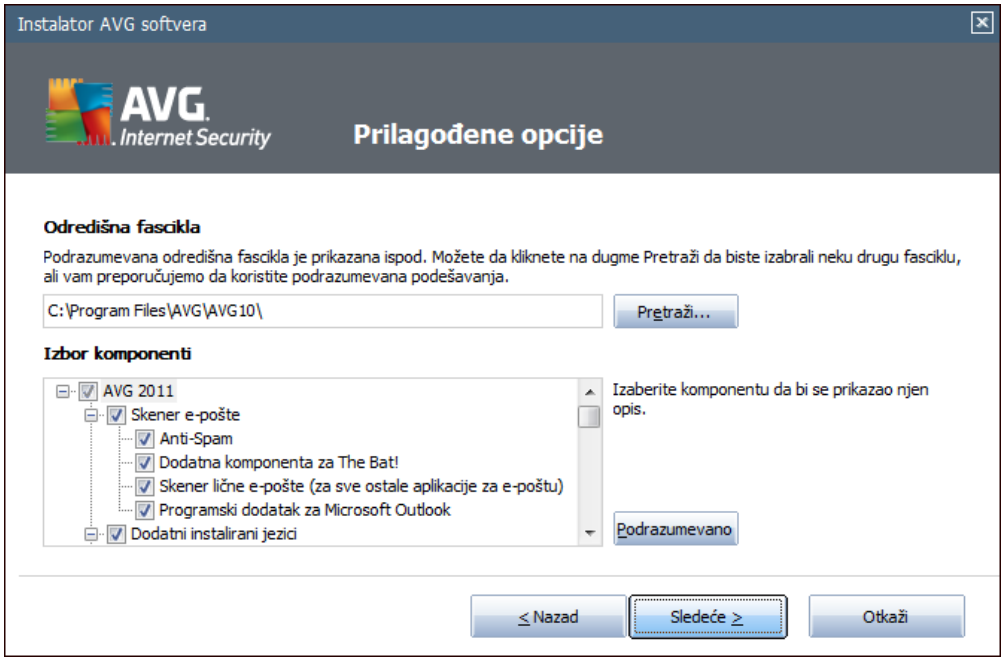
Većini korisnika se preporučuje da se drže standardne***Brze instalacije*** kojom će se program AVG instalirati u potpuno automatskom režimu sa postavkama koje je unapred definisao proizvođač softvera. Ova konfiguracija obezbeđuje maksimalnu bezbednost i optimalnu zauzetost resursa. Ako kasnije bude potrebno da promenite konfiguraciju, to ćete uvek moći da uradite direktno u aplikaciji AVG. Ukoliko ste odabrali opciju ***Brza instalacija*** , pritisnite dugme ***Dalje*** da nastavite ka sledećem dijalogu***Instaliraj AVG bezbednosnu traku sa alatkama***.

Prilagođenu instalaciju treba da koriste isključivo iskusni korisnici koji imaju dobar razlog da program AVG instaliraju sa nestandardnim postavkama, npr. u skladu sa specijalnim zahtevima sistema. Kada ste izabrali ovu opciju, pritisnite dugme ***Dalje*** da nastavite ka dijalogu ***Prilagođene opcije*** .

U desnom odeljku dijaloga možete naći polje za označavanje koje se odnosi na ***AVG gadžet*** (*koji je podržan u operativnim sistemima Windows Vista/Windows 7*). Ukoliko želite da instalirate ovaj gadžet, označite odgovarajuće polje. ***AVG gadžet***će tada biti pristupačan iz Windows bočne trake, čime se omogućava momentalni pristup najvažnijim funkcijama vašeg **AVG Internet Security 2011**, npr. skeniranjei ažuriranje.

4.4. Opcije prilagođavanja

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



Odredišna fascikla

U okviru ***Odredišna fascikla***odeljka dijaloga od vas se traži da označite lokaciju gde će **AVG Internet Security 2011** biti instaliran. Podrazumevano, AVG se instalira u fasciklu Programske datoteke na jedinici diska C:- Ako želite da promenite ovu lokaciju, kliknite na dugme ***Potraži*** da biste videli strukturu disk jedinice i izaberite odgovarajuću fasciklu.

Izbor komponenti

Odeljak***Izbor komponenti*** omogućava pregled svih **AVG Internet Security 2011** 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***.

Kliknite na dugme ***Dalje*** da biste nastavili.

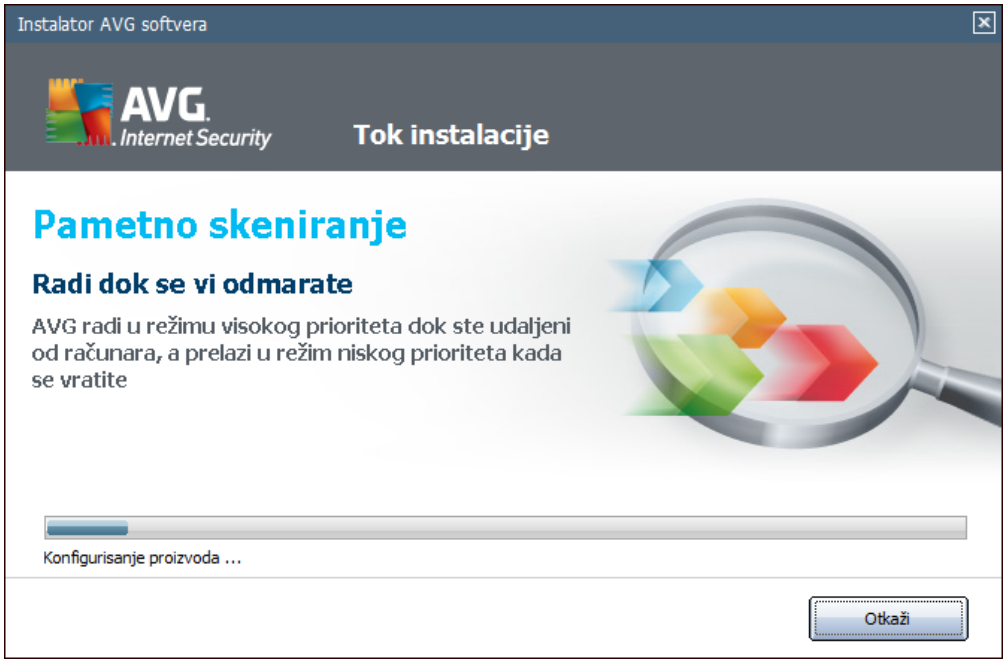
4.5. Instalirajte AVG bezbednosnu traku sa alatkama

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 novija verzija i Mozilla Firefox v. 3.0 ili novija verzija*) 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.

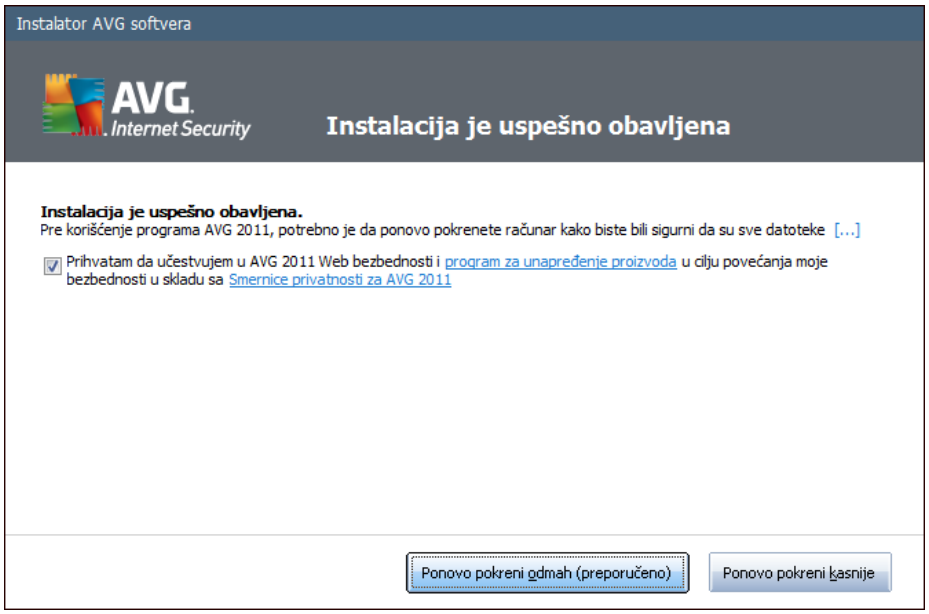
4.6. Tok instalacije

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



Kada se proces instalacije završi, bićete preusmereni na sledeći dijalog.

4.7. Instalacija je uspešno obavljena



Dijalog Instalacija je uspešno obavljena potvrđuje da je vaš **AVG Internet Security 2011** u

potpunosti instaliran i konfigurisan.

U ovom dijalogu unesite vaše kontakt podatke kako biste mogli da dobijate informacije i novosti u vezi sa proizvodom. Ispod obrasca za registraciju ćete naći sledeće dve opcije:

- ***Da, želim da budem informisan o novostima vezanim za bezbednost i AVG 2011 specijalnim ponudama putem e-pošte*** - označite ovo polje ako želite da budete informisani o novitetima iz sfere bezbednosti na Internetu i želite da dobijate informacije o specijalnim ponudama, unapređenjima i ažuriranjima, itd. u vezi sa AVG proizvodom

- ***Prihvatam da učestvujem u AVG 2011 web bezbednosti i Programu za unapređenje proizvoda ...*** - označite ovo polje da prihvatite učešće u Programu za unapređenje proizvoda (*za detalje videti poglavlje AVG Napredna podešavanja/Program za unapređenje proizvoda*) koji prikuplja anonimne informacije o detektovanim pretnjama u cilju povećanja nivoa opšte bezbednosti Interneta.

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***.

> ***Napomena:*** *Ukoliko koristite AVG poslovnu licencu i u slučaju da ste prethodno odabrali da se instalira stavka Daljinske administracije (videti Prilagođene opcije), dijalog Instalacija je uspešno obavljena pojaviće se sa sledećim interfejsom:*
>
> *Morate da odredite parametre AVG centra za podatke - unesite niz za vezu u AVG centar za podatke u formi server:port. Ako te informacije trenutno nisu dostupne, ostavite ovo polje praznim, a konfiguraciju možete kasnije podesiti u dijalogu* ***Napredna podešavanja / Daljinska administracija****. Za detaljne informacije o AVG daljinskoj administraciji pročitajte korisničko uputstvo za AVG Business izdanje; može se preuzeti sa AVG Web lokacije (http://www.avg.com/).*

5. Nakon instalacije

5.1. Registracija proizvoda

Kada završite instalaciju programa **AVG Internet Security 2011**, registrujte svoj proizvod na Web lokaciji kompanije AVG (http://www.avg.com/), stranica ***Registracija*** (*sledite uputstva koja se nalaze na stranici*). Nakon registracije, imaćete pun pristup AVG korisničkom nalogu, AVG informativnom biltenu i drugim uslugama koje su dostupne isključivo registrovanim korisnicima.

5.2. Pristup korisničkom interfejsu

AVG korisničkom interfejsu možete pristupiti na nekoliko načina:

- dvaput kliknite na***AVG ikonu u sistemskoj traci***
- dvaput kliknite na AVG ikonu na radnoj površini
- dvaput kliknite na statusnu liniju koja se nalazi u donjem odeljku***AVG gadžet*** (*ukoliko je instaliran; podržano na OS Windows Vista/ Windows 7*)
- iz menija ***Start/Programi/AVG 2011/AVG korisnički interfejs***
- iz***AVG trake sa alatkama***putem opcije***Pokreni AVG***

5.3. Skeniranje celog računara

Postoji potencijalni rizik da je vaš računar zaražen virusom pre instalacije programa **AVG Internet Security 2011**. Zato je potrebno da pokrenete ***Skeniranje celog računara***, kako biste bili sigurni da računar nije zaražen.

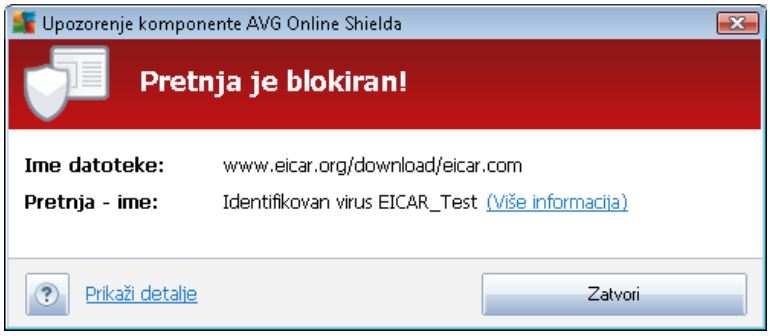
Uputstva za ***Skeniranje celog računara*** potražite u poglavlju ***Skeniranje programom AVG***.

5.4. Eicar test

Da biste potvrdili da je **AVG Internet Security 2011** 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. Čim potvrdite preuzimanje datoteke za testiranje, ***Online Shield*** će 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*** detektovati „virus“ kada pokušate da je otpakujete. **Ako AVG ne identifikuje probnu datoteku EICAR kao virus, trebalo bi da ponovo proverite konfiguraciju programa!**

5.5. Podrazumevana AVG konfiguracija

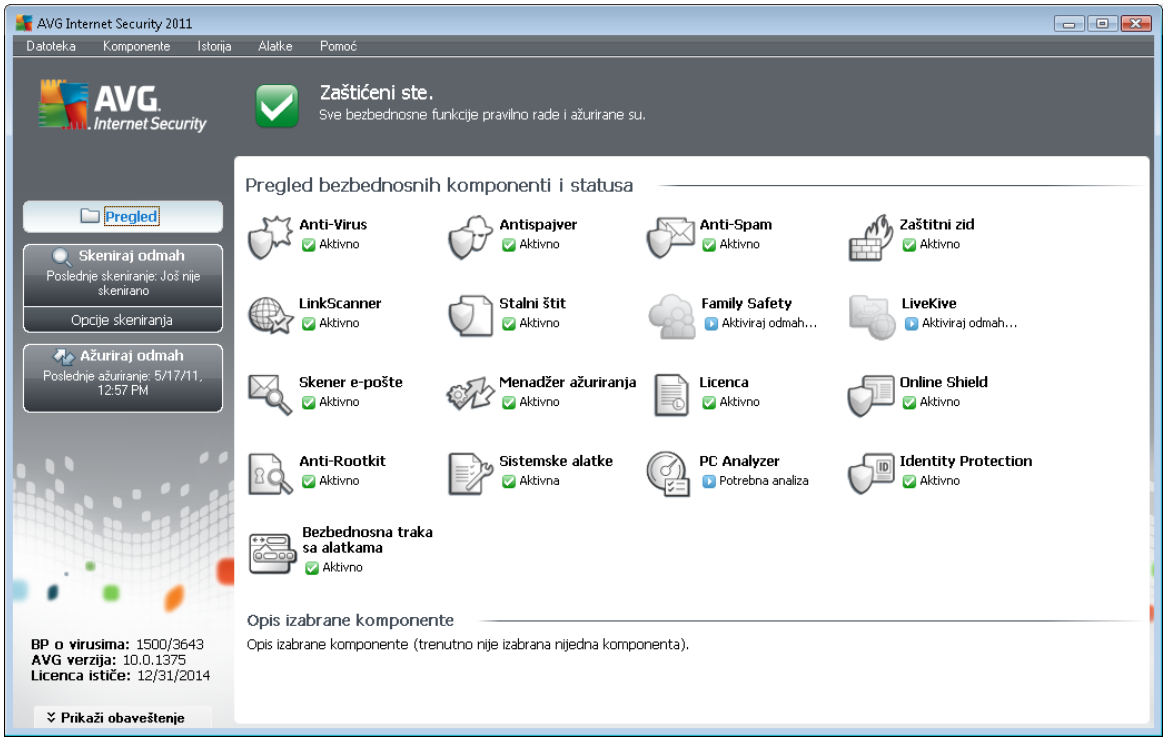
Podrazumevanu konfiguraciju (*tj. način na koji je aplikacija podešena odmah nakon instalacije*) programa **AVG Internet Security 2011** podesio je proizvođač softvera kako bi sve komponente i funkcije bile podešene tako da se postignu optimalne performanse.

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.

6. AVG korisnički interfejs

AVG Internet Security 2011 se otvara sa glavnim prozorom:



Glavni prozor je podeljen na nekoliko odeljaka:

- ***Sistemski meni*** *(gornja sistemska linija u prozoru)* je standardni element za navigaciju koji vam omogućava da pristupite svim AVG komponentama, uslugama i funkcijama - detalji>>
- ***Informacije o bezbednosnom statusu*** *(gornji deo prozora)* sadrži informacije o trenutnom statusu programa AVG - detalji>>
- ***Brze veze*** *(leva strana prozora)* omogućavaju vam da brzo pristupite najvažnijim AVG zadacima i onima koji se najčešće koriste - detalji>>
- ***Pregled komponenti*** *(središnji deo prozora)* sadrži pregled instaliranih AVG komponenata - detalji>>
- ***Statistika*** *(donji levi deo prozora)* sadrži sve statističke podatke u vezi sa radom programa - detalji>>
- ***Ikona sistemske palete*** *(donji desni ugao ekrana, na sistemskoj paleti)* označava trenutni status programa AVG - detalji>>
- ***AVG gadžet*** *(Windows bočna traka, podržano u Windows Vista/7)* omogućava brz pristup AVG skeniranju i ažuriranju - detalji>>

6.1. 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 2011**. Pomoću sistemskog menija možete pristupiti određenim AVG komponentama, funkcijama i uslugama.

Sistemski meni ima pet glavnih odeljaka:

6.1.1. Datoteka

- ***Izađi*** - zatvaranje **AVG Internet Security 2011** korisničkog interfejsa. Međutim, aplikacija AVG će i dalje raditi u pozadini, pa će vaš računar biti zaštićen!

6.1.2. 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*** obezbeđuje zaštitu vašeg računara od virusa koji pokušavaju da prodru u njega - detalji >>
- ***Antispajver*** obezbeđuje da vaš računar bude zaštićen od spajvera i advera - detalji >>
- ***Odbrana od neželjene pošte*** proverava sve dolazne e-poruke i označava neželjenu e-poštu kao NEŽELJENU - detalji >>
- ***Zaštitni zid*** kontroliše način na koji računar razmenjuje podatke sa drugim računarima na Internetu ili lokalnoj mreži - detalji >>
- ***Skener linkova*** proverava rezultate pretrage koji se prikazuju u pregledaču Interneta - detalji >>
- ***Skener e-pošte*** proverava dolaznu i odlaznu poštu u potrazi za virusima - detalji >>
- ***Family Safety*** pomaže vam da nadgledate aktivnosti dece na mreži i štiti ih od neprikladnog sadržaja Web lokacija - detalji >>
- ***LiveKive*** omogućava automatsko pravljenje rezervnih kopija vaših podataka na mreži - detalji >>
- ***Stalni štit*** radi u pozadini i skenira datoteke prilikom njihovog kopiranja, otvaranja ili čuvanja - detalji >>
- ***Upravljanje ažuriranjem*** upravlja ažuriranjem programa AVG - detalji >>
- Υ οδελφκυ ***Licenca*** se prikazuje broj licence, tip licence i datum njenog isteka - detalji >>

- ***Online Shield*** skenira sve podatke koje preuzima pregledač Weba - detalji >>
- ***Anti-Rootkit*** detektuje programe i tehnologije čiji je cilj da kamufliraju zlonamerni softver - detalji >>
- ***Sistemski alati*** nudi detaljan pregled AVG okruženja i informacije o operativnom sistemu - detalji >>
- ***PC Analyzer*** analizator pruža informacije o statusu vašeg računara - detalji >>
- ***Zaštita identiteta*** - komponenta protiv zlonamernog softvera fokusirana na sprečavanje kradljivaca identiteta da ukradu vaše lične digitalne dragocenosti - detalji >>
- ***Bezbednosna traka sa alatkama*** omogućava vam da koristite željene AVG funkcije direktno iz Internet pregledača - detalji >>
- ***Daljinska administracija*** prikazuje se samo u okviru verzija iz serije AVG Business Edition, u slučaju da ste označili tokom procesa instalacije da želite da instalirate ovu komponentu

6.1.3. 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***
- ***Detekcija od strane skenera e-pošte*** – otvara se dijalog sa pregledom priloga e-poruka koje je kao opasne detektovala komponenta ***Skener e-pošte***
- ***Stavke koje je pronašao Online Shield*** – otvaranje dijaloga sa pregledom pretnji koje je detektovao ***Online Shield***
- ***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 2011** radnji
- ***Zaštitni zid*** - otvara interfejs za podešavanje zaštitnog zida na kartici ***Datoteke evidencije*** sa detaljnim pregledom svih radnji komponente Zaštitni zid.

6.1.4. Alatke

- ***Skeniraj računar*** - prelazak u AVG interfejs za skeniranjei pokretanje skeniranja celog računara.
- ***Skeniraj izabranu fasciklu*** - prelazak u AVG interfejs za skeniranje, nakon čega sa

prikaza vašeg računara u obliku stabla možete izabrati datoteke i fascikle koje želite da skenirate.

- ***Skeniraj datoteku*** – omogućava vam da pokrenete test pojedinačne datoteke na zahtev tako što ćete je izabrati sa prikaza vaše disk jedinice u obliku stabla.

- ***Ažuriranje*** – automatsko pokretanje procesa ažuriranja za **AVG Internet Security 2011**.

- ***Ažuriranje iz direktorijuma*** - pokretanje procesa ažuriranja na osnovu 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*** – otvaranje dijaloga ***AVG napredna podešavanja*** u kojem možete urediti **AVG Internet Security 2011** konfiguraciju. Uglavnom se preporučuje da zadržite podrazumevana podešavanja ove aplikacije koje je definisao proizvođač softvera.

- ***Podešavanja zaštitnog zida*** - otvaranje samostalnog dijaloga za napredno konfigurisanje komponente ***Zaštitni zid.***

6.1.5. Pomoć

- ***Sadržaj*** - otvaranje AVG datoteka pomoći

- ***Pronađite pomoć na mreži*** - otvaranje AVG Web lokacije (http://www.avg.com/) na stranici centra za korisničku podršku

- ***Vaš AVG Web*** - otvaranje AVG Web lokacije (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*).

- ***Registrujte odmah*** - povezivanje sa stranicom za registraciju na AVG Web lokaciji (http://www.avg.com/). Unesite registracione podatke; besplatnu tehničku podršku mogu dobiti samo korisnici koji registruju svoj AVG proizvod.

Napomena*: Ako koristite probnu verziju programa* **AVG Internet Security 2011***, poslednje dve stavke su* ***Kupite odmah*** *i* ***Aktivacija*** *i omogućavaju vam da odmah kupite punu verziju programa. Ako je* **AVG Internet Security 2011** *instaliran sa prodajnim brojem, prikazuju se stavke* ***Registracija*** *i* ***Aktivacija****. Više informacija potražite u odeljku Licenca u ovoj dokumentaciji.*

- ***O programu AVG*** - otvaranje dijaloga ***Informacije*** koji sadrži pet 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***.

6.2. Informacije o bezbednosnom statusu

Odeljak ***Informacije o bezbednosnom statusu*** nalazi se u gornjem delu glavnog prozora programa AVG. U ovom odeljku uvek možete pronaći informacije o trenutnom bezbednosnom statusu programa **AVG Internet Security 2011**. Pogledajte opise ikona iz ovog odeljka i njihovo značenje:

 - Zelena ikona ukazuje na to da AVG potpuno funkcionalan. Računar je u potpunosti zaštićen i ažuriran, a sve instalirane komponente ispravno rade.

 - Narandžasta 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, a verovatno ste odlučili da isključite neku komponentu. I dalje ste zaštrićeni pomoću programa AVG. Međutim, obratite pažnju na podešavanja problematične komponente! Njeno ime će biti prikazano u odeljku ***Informacije o bezbednosnom statusu***.

Ova ikona se takođe pojavljuje i ako ste iz nekog razloga odlučili da zanemarite status greške komponente (*opcija „Zanemari stanje komponente" je dostupna u kontekstualnom meniju koji se otvara tako što ćete kliknuti desnim tasterom miša iznad odgovarajuće ikone komponente u pregledu komponente u glavnom prozoru programa AVG*). Možda ćete morati da koristite ovu opciju u određenoj situaciji, ali preporučujemo da isključite opciju „***Zanemari stanje komponente***" što pre.

 - Crvena ikona ukazuje na to da je status programa AVG kritičan! Neke komponente ne rade ispravno pa AVG ne može da zaštiti vaš računar. Odmah pokušajte da rešite prijavljeni problem. Ako ne možete sami da rešite problem, obratite se AVG timu za tehničku podršku.

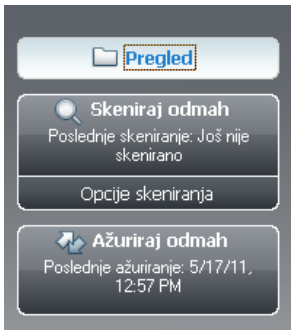
U slučaju da AVG nije podešen na optimalan rad, novo dugme nazvano Popravi (ili Popravi sve ukoliko problem uključuje više od jedne komponente) se pojavljuje pored informacije o bezbednosnom statusu. Pritisnite dugme da pokrenete automatski proces provere i konfiguracije programa. Ovo je lak način da podesite AVG na optimalan rad 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 možete dobiti u bilo kojem trenutku i pomoću ikone u sistemskoj traci poslova.*

6.3. Brze veze

Brze veze *(u odeljku sa leve strane u AVG korisničkom interfejsu)* omogućavaju trenutni pristup najvažnijim i najčešće korišćenim funkcijama programa AVG:



- ***Pregled*** - ovu vezu koristite da biste sa bilo kojeg otvorenog AVG interfejsa prešli na podrazumevani, sa pregledom svih instaliranih komponenti - pogledajte poglavlje ***Pregled komponenti*** >>

- ***Skeniraj sada*** - podrazumevano, dugme pruža informacije o(*tipu skeniranja, datumu poslednjeg pokretanja*) o poslednjem pokrenutom skeniranju. Možete da izvršite komandu ***Skeniraj odmah*** da biste ponovo pokrenuli isto skeniranje ili da kliknete na vezu ***Opcije skeniranja*** da biste otvorili AVG interfejs za skeniranje u kojem možete da pokrenete skeniranja, planirate skeniranja ili uređujete parametre skeniranja – pogledajte poglavlje ***AVG skeniranje***>>

- ***Ažuriraj sada*** - veza pruža datum poslednjeg pokretanja procesa ažuriranja. Pritisnite dugme da otvorite interfejs za ažuriranje i pokrenete AVG proces ažuriranja momentalno - videti poglavlje ***AVG ažuriranja***>>

Te veze su uvek dostupne iz korisničkog interfejsa. Kada upotrebite brzu vezu za pokretanje određenog procesa, otvoriće se novi dijalog u korisničkom interfejsu, ali će brze veze i dalje biti dostupne. Osim toga, aktivni proces prikazan je grafički..

6.4. Pregled komponenti

Odeljak ***Pregled komponenata*** nalazi se u centralnom delu AVG korisničkog interfejsa. Ovaj odeljak ima dva dela:

- Pregled svih instaliranih komponenti koji se sastoji od panela sa ikonom komponente i informacije o tome da li je ta komponenta aktivna ili ne

- Opis izabrane komponente

U okviru programa **AVG Internet Security 2011** , odeljak ***Pregled komponenti*** sadrži informacije o sledećim komponentama:

- ***Antivirusni program*** obezbeđuje zaštitu vašeg računara od virusa koji pokušavaju da prodru u njega - detalji >>

- ***Antispajver*** obezbeđuje da vaš računar bude zaštićen od spajvera i advera - detalji >>
- ***Odbrana od neželjene pošte*** proverava sve dolazne e-poruke i označava neželjenu e-poštu kao NEŽELJENU - detalji >>
- ***Zaštitni zid*** kontroliše način na koji računar razmenjuje podatke sa drugim računarima na Internetu ili lokalnoj mreži - detalji >>
- ***Skener linkova*** proverava rezultate pretrage koji se prikazuju u pregledaču Interneta - detalji >>
- ***Skener e-pošte*** proverava dolaznu i odlaznu poštu u potrazi za virusima - detalji >>
- ***Stalni štit*** radi u pozadini i skenira datoteke prilikom njihovog kopiranja, otvaranja ili čuvanja - detalji >>
- ***Family Safety*** pomaže vam da nadgledate aktivnosti dece na mreži i štiti ih od neprikladnog sadržaja Web lokacija - detalji >>
- ***LiveKive*** omogućava automatsko pravljenje rezervnih kopija vaših podataka na mreži - detalji >>
- ***Upravljanje ažuriranjem*** upravlja ažuriranjem programa AVG - detalji >>
- Υ οδελφκυ ***Licenca*** se prikazuje broj licence, tip licence i datum njenog isteka - detalji >>
- ***Online Shield*** skenira sve podatke koje preuzima pregledač Weba - detalji >>
- ***Anti-Rootkit*** detektuje programe i tehnologije čiji je cilj da kamufliraju zlonamerni softver - detalji >>
- ***Sistemski alati*** nudi detaljan pregled AVG okruženja i informacije o operativnom sistemu - detalji >>
- ***PC Analyzer*** analizator pruža informacije o statusu vašeg računara - detalji >>
- ***Zaštita identiteta*** - komponenta protiv zlonamernog softvera fokusirana na sprečavanje kradljivaca identiteta da ukradu vaše lične digitalne dragocenosti - detalji >>
- ***Bezbednosna traka sa alatkama*** omogućava vam da koristite željene AVG funkcije direktno iz Internet pregledača - detalji >>
- ***Daljinska administracija*** prikazuje se samo u okviru verzija iz serije AVG Business Edition, u slučaju da ste tokom procesa instalacijeoznačili da želite da instalirate ovu komponentu

Kliknite na ikonu određene komponente da biste je označili u pregledu komponenti. Opis osnovnih funkcija komponente istovremeno će se pojaviti u donjem delu korisničkog interfejsa. Dvaput kliknite na ikonu da biste otvorili interfejs izabrane komponente sa listom osnovnih statističkih podataka.

Kliknite desnim tasterom miša iznad ikone komponente da biste otvorili kontekstualni meni. Osim otvaranja grafičkog interfejsa komponente možete izabrati i opciju ***Zanemari stanje komponente***. Izaberite ovu opciju da biste naveli da ste svesni stanja greške komponente, ali da iz nekog razloga želite da se AVG ponaša na ovakav način i ne želite da vas obaveštava putem sive ikone na sistemskoj paleti.

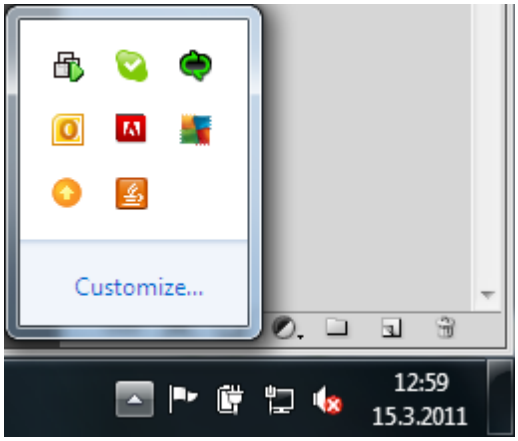
6.5. Statistika

Odeljak ***Statistika*** nalazi se u levom donjem uglu ***AVG korisničkog interfejsa***. On sadrži informacije o radu programa:

- ***Baza podataka o virusima*** - informiše vas o tome koja je verzija baze podataka o virusima trenutno instalirana
- ***AVG verzija*** - informiše vas o tome koja je verzija programa AVG instalirana *(broj ima oblik 10.0.xx, gde 10.0 označava broj linije proizvoda, a xx predstavlja broj verzije)*
- ***Licenca ističe*** - datum isteka vaše AVG licence

6.6. Ikona sistemske palete

Ikona sistemske palete (*na Windows traci zadataka*) pokazuje trenutni status programa **AVG Internet Security 2011**. Stalno je vidljiva u sistemskoj paleti, bez obzira na to da li je glavni prozor programa AVG otvoren ili zatvoren:



Ukoliko je u boji ***ikona sistemske palete*** ukazuje na to da su sve AVG komponente aktivne i potpuno funkcionalne. Takođe, AVG ikona na sistemskoj paleti može se prikazivati u boji i kada je AVG u stanju greške, ali ste potpuno svesni situacije i namerno ste odlučili da ***zanemarite stanje komponente***. Ikona sa znakom uzvika ukazuje na problem (*neaktivna komponenta, greška, itd.*). Dvaput kliknite na ***ikonu u sistemskoj paleti*** da biste otvorili glavni prozor i uredili neku komponentu.

Ikona sistemske palete vas obaveštava i o trenutnim aktivnostima programa AVG i mogućim promenama statusa programa (*npr. automatsko pokretanje planiranog skeniranja ili ažuriranja, promena profila zaštitnog zida, promena statusa komponente, greška, ...*) putem iskačućeg prozora koji se otvara iznad AVG ikone u sistemoj paleti:

Ikona u sistemskoj paleti može se koristiti i kao brza veza za pristup glavnom prozoru programa AVG u bilo kojem trenutku - dvaput kliknite na ikonu. Ako desnim tasterom miša kliknete na***ikonu u sistemskoj paleti*** otvoriće se kratak kontekstualni meni koji sadrži sledeće opcije:

- ***Otvori AVG korisnički interfejs*** - kliknite da biste otvorili AVG korisnički interfejs
- ***Skeniranja*** – kliknite da biste otvorili kontekstualni meni programa
- ***Zašitni zid*** - kliknite da otvorite kontekstualni meni opcija podešavanjaZaštitnog zida gde možete urediti glavne parametre:Status zaštitnog zida (*Zaštitni zid omogućen/Zaštitni zid onemogućen/Vanredni režim*), prebacivanje režima za igranjei profile Zaštitnog zida
- ***Pokreni PC Analyzer*** – kliknite da biste pokrenuli komponentu PC Analyzer
- ***Skeniranja u toku*** - ova stavka se prikazuje samo u slučaju da je skeniranje trenutno u toku na vašem 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*.
- ***Ažuriraj odmah*** - odmah se pokreće ažuriranje
- ***Pomoć*** - otvara datoteku za pomoć na njenoj početnoj stranici

6.7. AVG gadžet

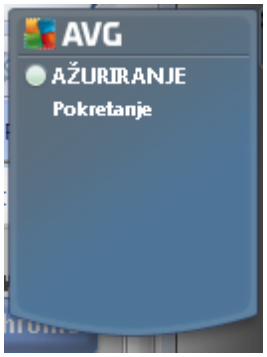
AVG gadžet se prikazuje na Windows radnoj površini (*Windows pomoćna traka*). Ova aplikacija je podržana samo kod operativnih sistema Windows Vista i Windows 7. ***AVG gadžet*** nudi trenutni pristup najvažnijim **AVG Internet Security 2011** funkcijama, npr. skeniranju iažuriranju:

AVG gadžetomogućava sledeće opcije brzog pristupa:

- ***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 gedžeta uz pomoć opcije ***Prikaži detalje*** (rezultati odgovarajućeg skeniranja biće navedeni u okviru stavke ***Skeniranje pomoću gedžeta iz bočne trake***).

- ***Ažuriraj sada*** - kliknite na vezu***Ažuriraj sada*** da pokrenete AVG ažuriranje direktno unutar gadgeta:



- ***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
- ***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
- ***PC Analyzer*** - otvara korisnički interfejs u komponenti ***PC Analyzer***
- ***Polje za pretragu*** - unesite ključnu reč i odmah ćete dobiti rezultate pretrage u novom prozoru podrazumevanog Web pregledača

7. Komponente programa AVG

7.1. Antivirusni program

7.1.1. Antivirusni program Principi

Mašina za skeniranje u okviru antivirusnog programa skenira sve datoteke i njihove aktivnosti (otvaranje/zatvaranje datoteka itd.) kako bi se proverilo da li sadrže poznate viruse. Detektovani virusi biće blokirani tako da ne mogu da preduzmu nikakvu akciju, a zatim će biti izbrisani ili smešteni u karantin. 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.

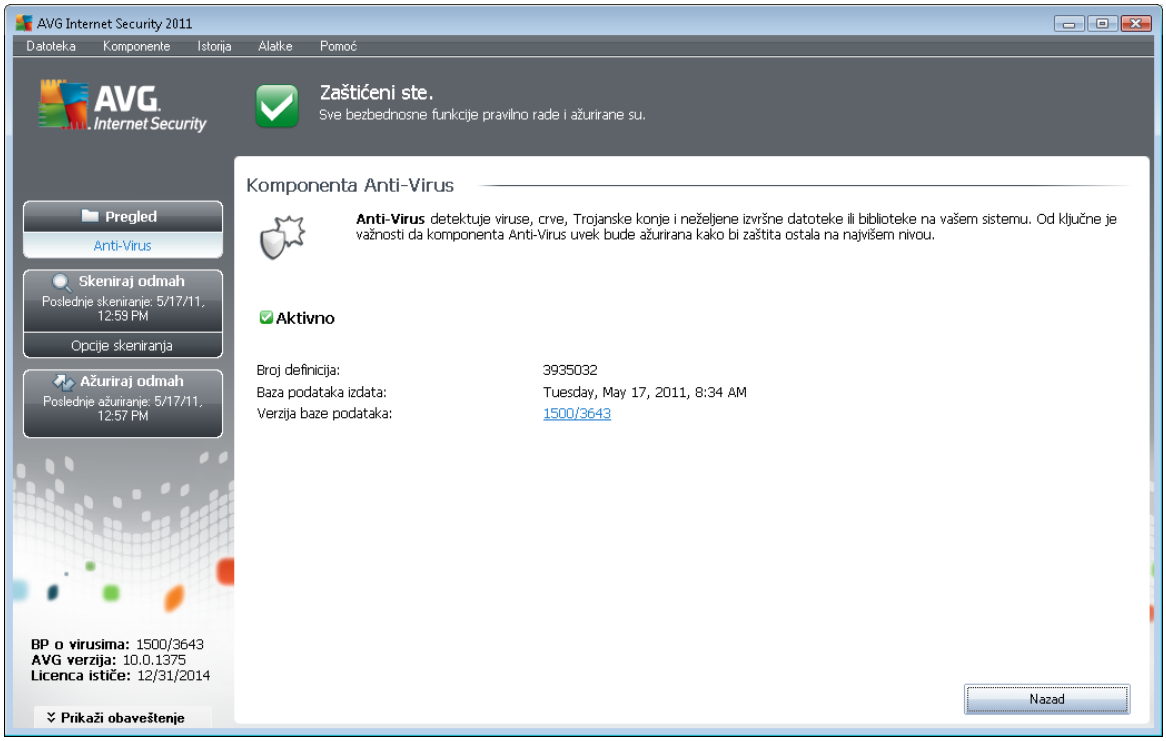
Važna funkcija aktivirusne zaštite jeste to da se nijedan poznat virus ne može pokrenuti na računaru!

Pošto samo jedna tehnologija može biti nedovoljna za otkrivanje ili identifikaciju virusa, ***Antivirusni program*** kombinuje nekoliko tehnologija da bi obezbedio zaštitu računara:

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

AVG takođe može da analizira i otkrije izvršne aplikacije ili DLL biblioteke koje mogu da budu potencijalno neželjene u okviru sistema. Te pretnje nazivamo potencijalno neželjenim programima (razne vrste špijunskog softvera, advera itd.) Osim toga, AVG skenira sistemski registrator u potrazi za sumnjivim stavkama, privremenim Internet datotekama i kolačićima za praćenje i dozvoljava da sve potencijalno štetne stavke tretirate na isti način kao i bilo koju drugu zarazu.

7.1.2. Interfejs antivirusnog programa



Interfejs komponente ***Antivirusnog programa*** pruža opšte informacije o njenim funkcijama, informacije o trenutnom statusu komponente (*Komponenta Antivirus je aktivna.*), kao i kratak pregled statistike komponente ***Antivirusnog programa*** :

- ***Broj definicija*** - pruža brojno stanje virusa definisanih u ažuriranoj verziji baze podataka virusa
- ***Izdanje baze podataka*** - označava datum i vreme poslednjeg ažuriranja baze podataka virusa
- ***Verzija baze podataka*** - definiše broj verzije trenutno instalirane baze podataka virusa; taj broj se uvećava nakon svakog ažuriranja baze podataka virusa

U interfejsu ove komponente dostupno je samo jedno dugme (***Nazad***) - kliknite na ovo dugme da biste se vratili u podrazumevani AVG korisnički interfejs (*pregled komponenti*).

7.2. Antispajver

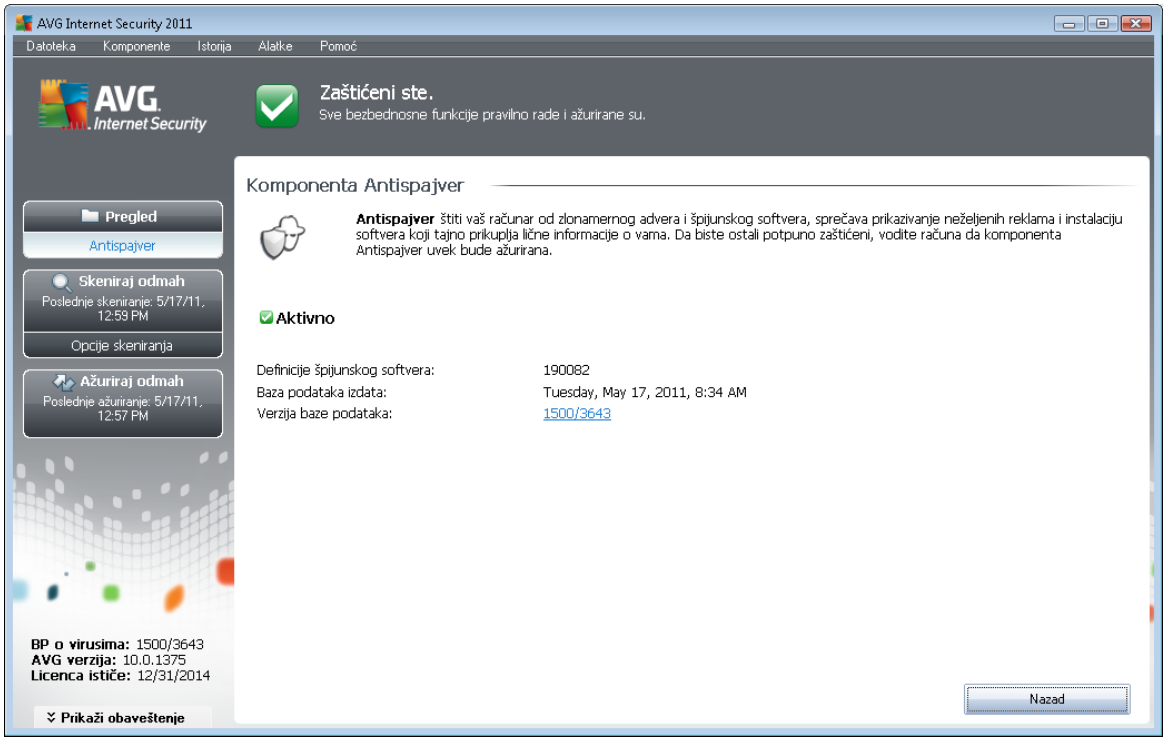
7.2.1. Princip rada antispajver komponente

Špijunski softver se obično definiše kao tip malvera, tj. softver koji prikuplja informacije sa računara korisnika bez njegovog znanja ili odobrenja. Neke špijunske 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.

Postoji i potencijalni rizik da je malver prenet na računar pre instalacije programa AVG ili da niste ažurirali program **AVG Internet Security 2011** najnovijim ispravkama za bazu podataka i program. Zato vam AVG omogućava da u potpunosti skenirate računar u potrazi za malverom/špijunskim softverom koristeći funkciju skeniranja. Ona takođe otkriva i malver koji je u stanju spavanja i neaktivan je, tj. malver koji je preuzet, ali još nije aktiviran.

7.2.2. Interfejs komponente Antispajver



Interfejs komponente ***Antispajver*** omogućava kratak pregled funkcionalnosti komponente, informaciju o njenom trenutnom statusu i neke ***Antispajver*** statističke podatke:

- ***Definicije špijunskog softvera*** - broj označava količinu uzoraka špijunskog softvera u najnovijoj verziji baze podataka špijunskog softvera
- ***Izdanje baze podataka*** - označava datum i vreme ažuriranja baze podataka špijunskog softvera
- ***Verzija baze podataka*** - definiše broj najnovije verzije baze podataka špijunskog softvera; taj broj se uvećava nakon svakog ažuriranja baze podataka virusa

U interfejsu ove komponente dostupno je samo jedno dugme (***Nazad***) - kliknite na ovo dugme da biste se vratili u podrazumevani AVG korisnički interfejs (*pregled komponenti*).

7.3. Anti-Spam

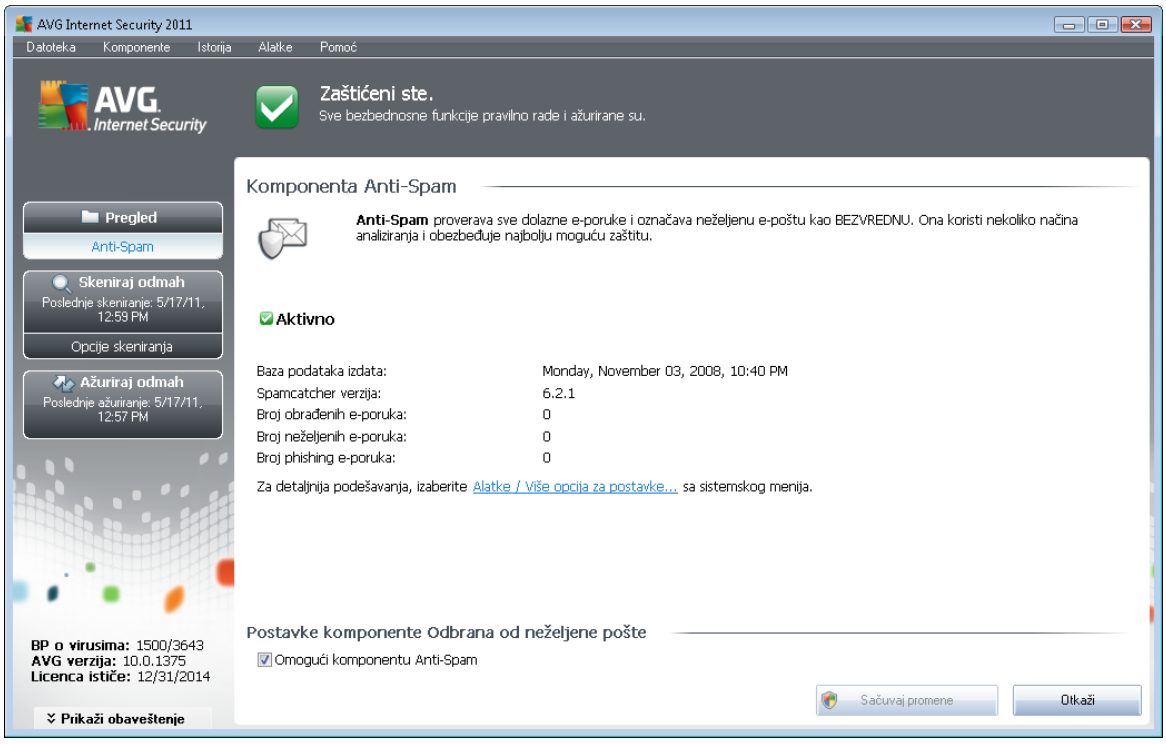
Bezvredna pošta se odnosi na neželjenu e-poštu, uglavnom reklame proizvoda ili usluga koje se masovno šalju na ogroman broj e-adresa istovremeno, puneći poštanske sandučiće primalaca. Bezvredna se ne odnosi na legitimnu neželjenu e-poštu za koju su primaoci dali svoje odobrenje. Bezvredna pošta nije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

7.3.1. Principi Anti-Spam odbrane

Komponenta „AVG odbrana od neželjene pošte“ proverava sve dolazne e-poruke i označava neželjene e-poruke kao bezvredne. Komponenta ***AVG odbrana od neželjene pošte*** može da izmeni temu e-poruke (*koja je identifikovana kao neželjena*) dodavanjem posebne tekstualne niske. Na taj način možete lako filtrirati e-poruke u vašem klijentu e-pošte.

Komponenta „AVG odbrana od neželjene pošte“ koristi nekoliko metoda za analizu kako bi obradila svaku e-poruku i nudi maksimalnu zaštitu od neželjenih e-poruka. ***Komponenta „AVG odbrana od neželjene 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“ neželjene pošte*) i da ručno dodate e-adrese na Belu listu (*nikad ne označavaj kao neželjeno*) i crnu listu (*uvek označi kao neželjeno*).

7.3.2. Anti-Spam Interfejs



U dijalogu komponente ***Odbrana od neželjene pošte*** naći ćete kratak tekst koji opisuje funkcionalnost ove komponente, informaciju o njenom trenutnom statusu, i sledeće statističke podatke:

- ***Baza podataka izdata*** - navodi datum i vreme ažuriranja i objavljivanja baze podataka neželjene pošte
- ***Spamcatcher verzija*** - definiše broj poslednje verzije mašine za odbranu od neželjene pošte
- ***Broj obrađenih poruka e-pošte*** - označava koliko je poruka e-pošte skenirano od poslednjeg pokretanja sistema odbrane od neželjene pošte
- ***Broj poruka neželjene pošte*** - označava koliko je od svih skeniranih poruka obeleženo kao neželjena pošta
- ***Broj phishing poruka*** - označava koliko je od svih skeniranih poruka obeleženo kao pokušaji namamljivanja

Dijalog***Odbrana od neželjene pošte*** dalje pruža vezu ka opcijama ***Alati/Napredna podešavanja***. Koristite vezu da se preusmerite na okruženje za napredno konfigurisanje svih**AVG Internet Security 2011**komponenti.

Imajte u vidu sledeće: *Proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja bi trebalo da menjaju samo iskusni korisnici.*

U interfejsu ove komponente dostupno je samo jedno dugme (***Nazad***) - kliknite na ovo dugme da biste se vratili u podrazumevani AVG korisnički interfejs (*pregled komponenti*).

7.4. 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 unutrašnju mrežu od napada koji dolaze spolja (obično sa Interneta) i kontrolišu komunikaciju na svakom mrežnom portu. Komunikacija se procenjuje u skladu sa definisanim pravilima, a zatim se dozvoljava ili zabranjuje. Ako zaštitni zid prepozna pokušaj napada, on „blokira“ pokušaj i ne dopušta da uljez 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 vaše 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 unutrašnjih korisnika drugih računara u mreži.

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.

7.4.1. Principi funkcionisanja zaštitnog zida

U okviru sistema AVG, komponenta ***Zaštitni zid*** kontroliše celokupan saobraćaj na svim mrežnim portovima na računaru. Na osnovu definisanih pravila ***Zaštitni zid*** procenjuje aplikacije koje su pokrenute na računaru i (i koje žele da se povežu sa Internetom/lokalnom mrežom) ili aplikacije koje spolja pristupaju računaru pokušavajući da se povežu sa njim. ***Zaštitni zid*** zatim dozvoljava ili zabranjuje komunikaciju na mrežnim portovima za svaku od tih aplikacija. Podrazumevano, ako je aplikacija nepoznata (tj. za nju nije definisano pravilo ***Zaštitnog zida***), ***Zaštitni zid*** će vas pitati da li želite da dozvolite ili blokirate taj pokušaj komunikacije.

Napomena: *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

7.4.2. 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, a 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 ne može se kopirati niti brisati, a njegove postavke se ne mogu menjati.
- ***Blokiraj sve***– sistemski profil komponente ***Zaštitni zid***, unapred podešen od strane proizvođača i uvek dostupan. Kada je ovaj profil aktiviran, svaki oblik komunikacije preko mreže je blokiran, pa je pristup računaru sa spoljnih mreža onemogućen, a ni računar ne može da komunicira sa spoljnim svetom. Ovaj sistemski profil ne može se kopirati niti brisati, a njegove postavke se ne mogu menjati.
- ***Prilagođeni profili***:

- ***Direktna veza sa Internetom***– pogodno za standardne stone kućne računare koji su direktno povezani sa Internetom ili notebook računare koji se povezuju sa Internetom izvan bezbedne mreže preduzeća. Izaberite ovu opciju ako se povezujete od kuće ili ako ste u okviru male mreže preduzeća bez centralne kontrole. Ovu opciju izaberite i ako putujete i pristupate Internetu sa notebook računara na nepoznatnim i potencijalno opasnim mestima (*internet kafei, hotelska soba itd.*). Kreiraće se restriktivnija pravila jer se pretpostavlja da ovi računari nemaju dodatnu zaštitu i zato zahtevaju maksimalnu zaštitu.

- ***Računar u domenu*** – prikladno za računare na lokalnoj mreži, npr. u školskoj ili korporativnoj mreži. Pretpostavlja se da mreža ima dodatne mere zaštite, pa bezbednosni nivo može biti niži nego na samostalnom računaru.

- ***Mala kućna ili kancelarijska mreža*** – prikladno za računare u maloj mreži, npr. kod kuće ili u malom preduzeću, gde je najčešće povezano samo nekoliko računara, bez „centralnog“ administratora.

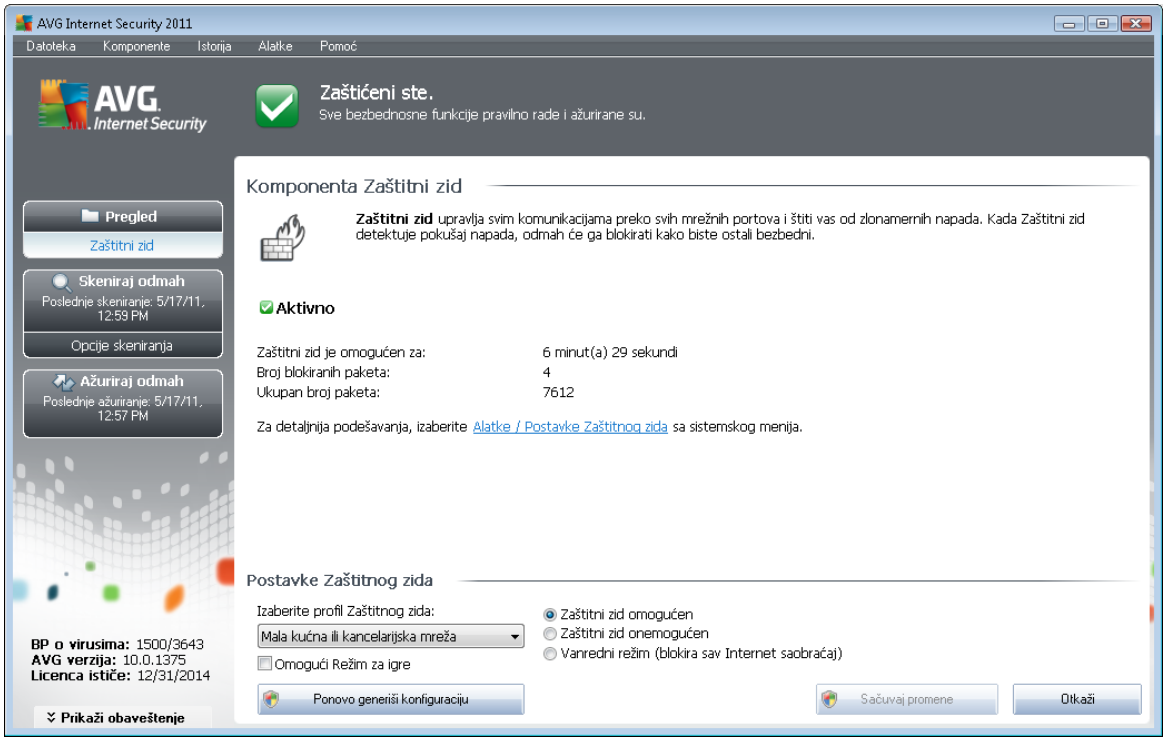
Zamena profila

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.

7.4.3. Interfejs zaštitnog zida



Interfejs komponente ***Zaštitni zid*** sadrži osnovne informacije o funkcionalnosti komponente, njenom statusu i kratak pregled statistike za ***Zaštitni zid*** :

- ***Zaštitni zid je omogućen u trajanju od*** - vremenski period od kako 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

Podešavanja zaštitnog zida

- ***Izbor profila zaštitnog zida*** - iz padajućeg menija izaberite jedan od definisanih profila - dva profila su uvek dostupna (*podrazumevani profili po imenu* ***Dozvoli sve*** *i* ***Blokiraj sve***), ostali profili su dodati ručno uređivanjem profila u dijalogu ***Profili*** u okviru stavke ***Postavke zaštitnog zida***.
- ***Omogući režim za igre*** – označite ovu opciju da biste bili sigurni da se tokom prikazivanja sadržaja preko 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.

- ***Status zaštitnog zida***:
    - o ***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***
    - o ***Zaštitni zid onemogućen*** – ova opcija potpuno isključuje ***Zaštitni zid***, pa je sav mrežni saobraćaj dozvoljen, ali se ne proverava!
    - o ***Vanredni 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: *Proizvođač softvera je podesio sve AVG komponente tako da se postignu 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
- ***Otkaži***- kliknite na ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenata*)

7.5. Skener linkova

7.5.1. Principi skeniranja linkova

Skener linkova 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 imena do malih firmi, i retko se zadržavaju na tim lokacijama duže od 24 sata. ***Skener linkova*** vas štiti analiziranjem web stranica iza svih veza na nekoj web stranici koju gledate i utvrđivanjem da su bezbedne u trenutku koji je najbitniji - kada kliknete na tu vezu.

Tehnologija ***Skenera linkova*** se sastoji iz dve funkcije, ***Štita za pretraživanje*** i ***Štita za pregledanje Interneta***:

- ***Štit za pretraživanje*** sadrži listu web lokacija (*URL adresa*) za koje se zna da su opasne. Kada pretražujete koristeći Google, Yahoo! Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg ili SlashDotsvi, svi rezultati pretrage se proveravaju prema ovoj listi i prikazuje se ikona sa ocenom (*za*

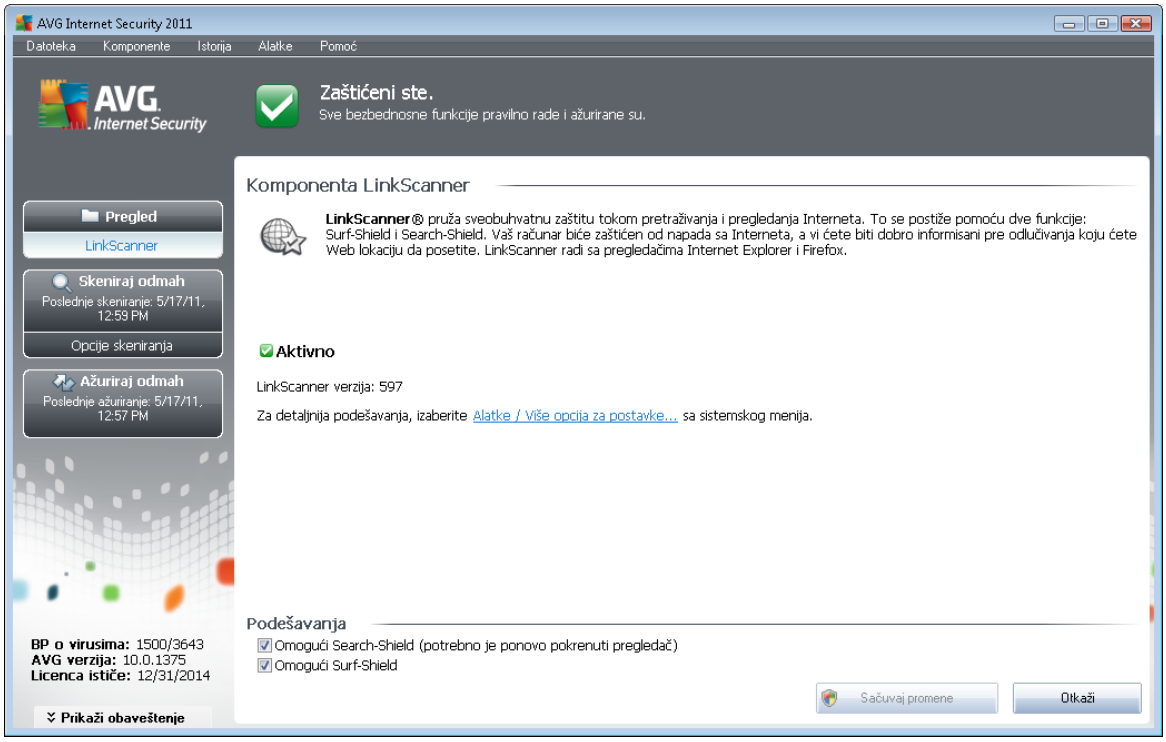
rezultate Yahoo pretrage se prikazuju samo ikone sa ocenom „opasna Web lokacija“).

- ***Štit za pregledanje Interneta***skenira sadržaj web lokacija koje posećujete, bez obzira na njihovu adresu. Čak i ako ***Štit za pretraživanje*** ne otkrije pojedine Web lokacije (*npr. ako se kreira nova zlonamerna web lokacija ili ako prethodno bezbedna web lokacija sada sadrži malver*), njih će otkriti i blokirati ***Štit za pregledanje Interneta*** kada pokušate da ih posetite.

Napomena: *Skener linkova nije predviđen za serverske platforme!*

7.5.2. Interfejs komponente Link Scanner

Interfejs komponente ***Skener linkova*** pruža kratak opis funkcionalnosti komponente i informaciju o njenom trenutnom statusu. Osim toga, možete naći informacije o najnovijem broju verziie baze podataka komponente ***Skener linkova*** (*Verzija komponente Skener linkova).*



Podešavanja komponente „Skener linkova“

U donjem delu dijaloga možete urediti nekoliko opcija:

- ***Omogućite*** ***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*).

7.5.3. Štit 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, and SlashDot*) biće procenjeni kako bi se proverilo da li sadrže opasne ili sumnjive linkove. Nakon što proveri linkove i označi one opasne, ***AVG skener linkova*** vas upozorava pre nego što kliknete na opasan ili sumnjiv link, 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 link upućuje je bezbedna (*ova ikona se neće prikazivati za bezbedne rezultate Yahoo! Rezultati JP pretrage*).

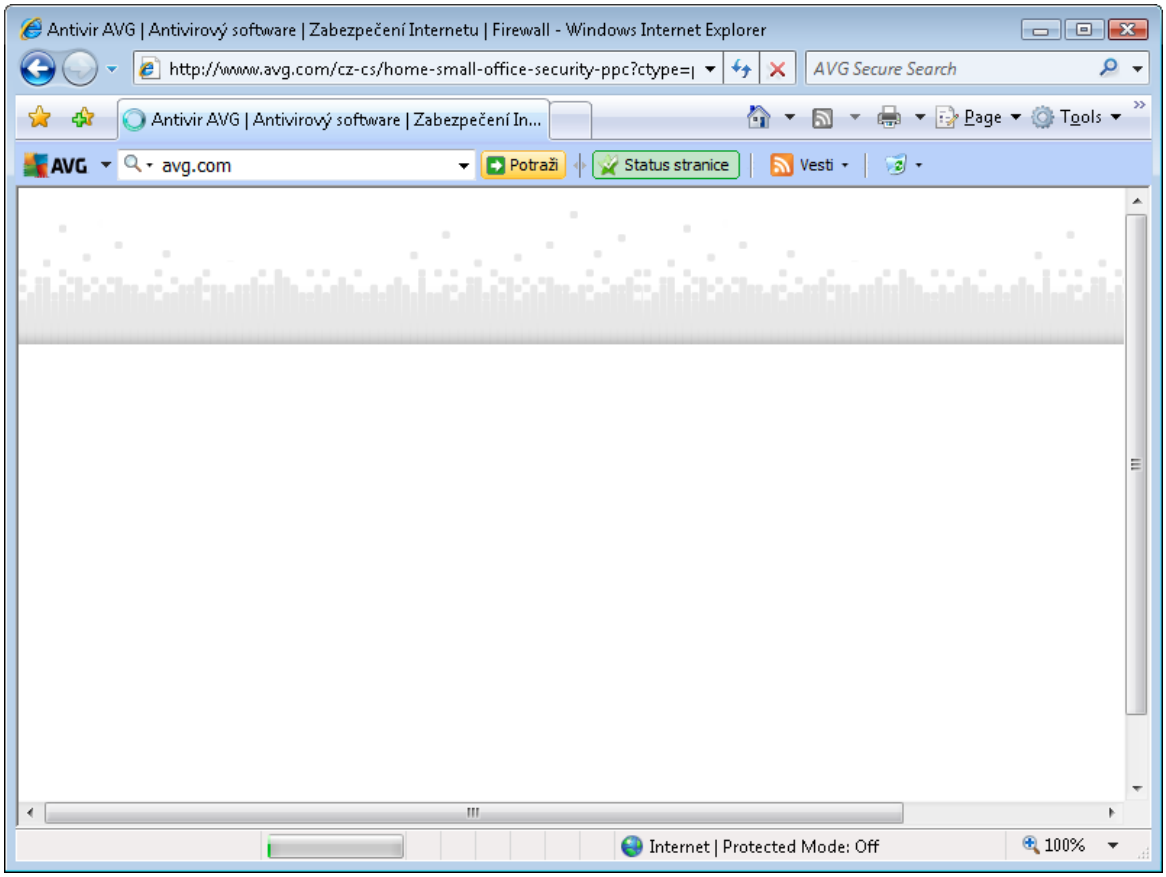
 Stranica na koju link upućuje ne sadrži pretnje, ali je donekle sumnjiva (*nesigurnog porekla ili motiva, zbog čega se ne preporučuje za kupovinu na mreži itd.*).

 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.

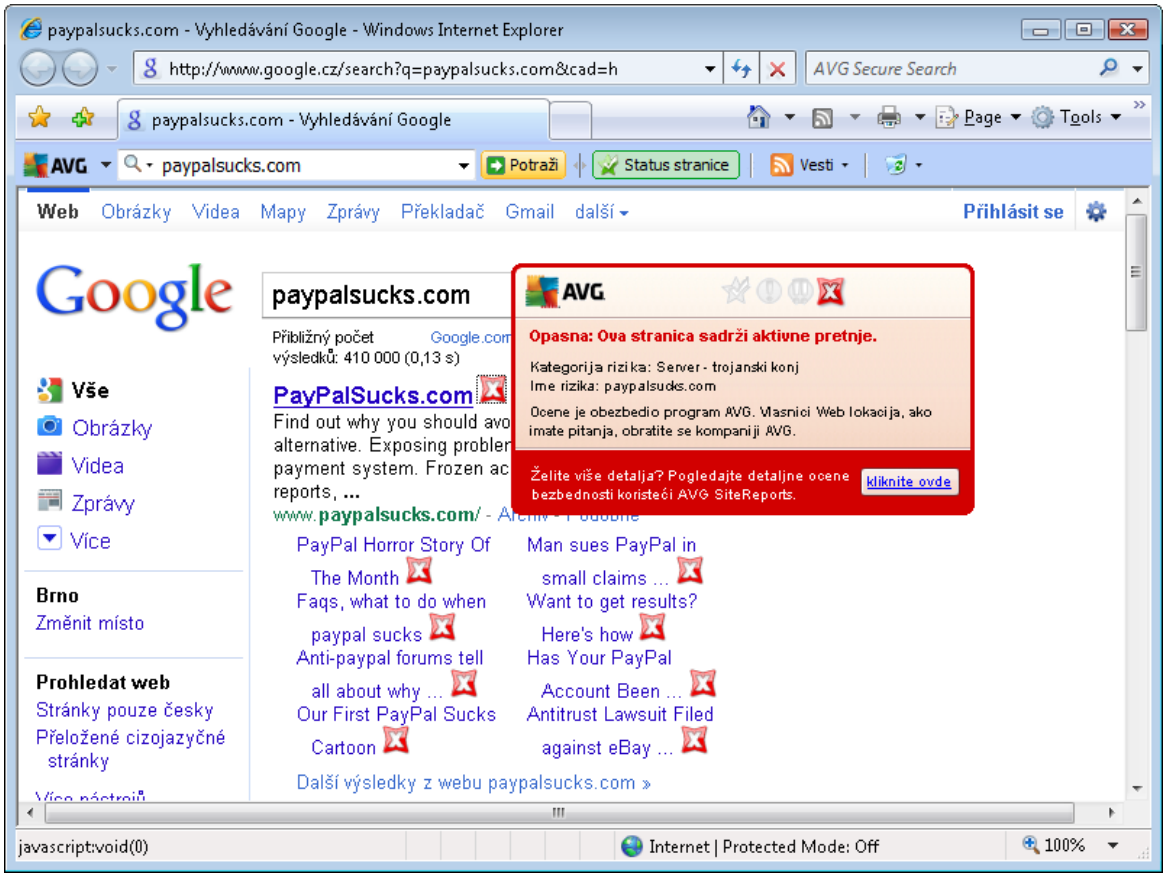
Ako postavite pokazivač iznad pojedinačnih ikona ocene, prikazaće se više informacija o tom linku. U informacije spadaju dodatne informacije o pretnji (*ako ih ima*):



7.5.4. Štit za pregledanje Interneta

Ovaj snažan vid zaštite blokiraće 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 ***AVG skener linkova*** 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, ***AVG Link Scanner*** će prikazati ekran upozorenja u Web pregledaču nalik sledećem:



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

7.6. Stalni štit

7.6.1. Principi rada komponente Stalni štit

Komponenta ***Stalni štit*** obezbeđuje neprekidnu zaštitu računara. Ona skenira svaku datoteku koju otvarate, čuvate ili kopirate i štiti sistemske oblasti računara. Kada ***Stalni štit*** otkrije virus u datoteci kojoj se pristupa, on zaustavlja operaciju koja se u tom trenutku izvršava i ne dozvoljava da se virus aktivira. U normalnim okolnostima, ovaj proces se obavlja neprimetno jer se odvija „u pozadini“ i bićete obavešteni samo kada se otkriju pretnje; ***Stalni štit*** istovremeno sprečava aktviranje pretnje i uklanja je. ***Stalni štit*** se učitava u memoriju računara tokom pokretanja sistema.

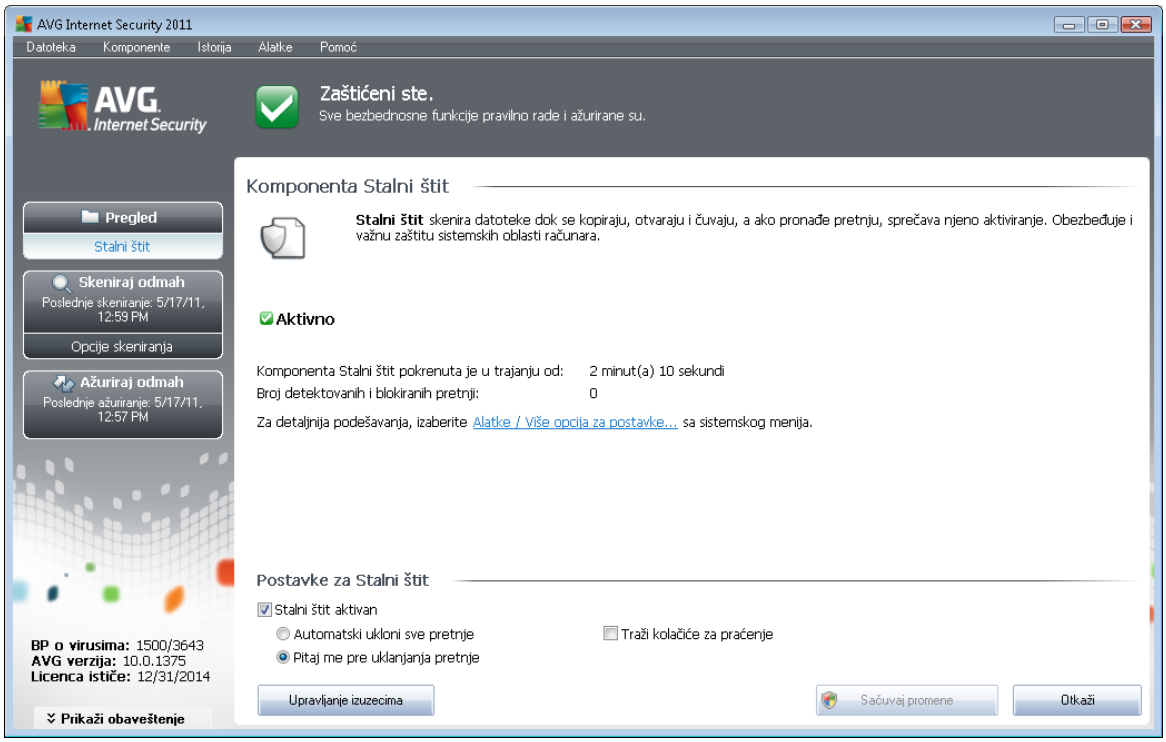
Mogućnosti koje nudi Stalni štit:

- Skeniranje određenih tipova mogućih pretnji
- Skeniranje prenosivih medijuma (*flash disk, itd.*)
- Skeniranje datoteka sa određenim oznakama tipa ili bez oznake tipa

- Dozvoli izuzetke iz skeniranja - određene datoteke ili fascikle koje se nikad neće skenirati

Upozorenje: stalni štit se učitava u memoriju računara tokom pokretanja sistema i izuzetno je važno da uvek bude uključen!

7.6.2. Interfejs komponente Stalni štit



Pored pregleda funkcionalnosti***Stalnog štita*** i informacija o statusu komponente, interfejs ***Stalnog štita*** nudi i neke statističke podatke:

- ***Stalni štit je aktivan*** - vremenski period od kako je ova komponenta poslednji put pokrenuta
- ***Detektovane i blokirane pretnje*** - broj detektovanih infekcija čije pokretanje/otvaranje je sprečeno (*ova vrednost se po potrebi može poništiti; npr. u statističke svrhe - Poništi vrednost*)

Postavke za Stalni štit

U donjem delu dijaloga nalazi se odeljak ***Stalni štit - postavke*** u kojem možete urediti osnovne postavke komponente (*detaljnije konfigurisanje, kao i kod ostalih komponenata, dostupno je ako otvorite stavku Alatke/Napredna podešavanja iz sistemskog menija*).

Opcija ***Stalni štit je aktivan*** omogućava vam da jednostavno uključite/isključite stalnu zaštitu. Ova funkcija je podrazumevano uključena. Ako je stalna zaštita uključena, možete odlučiti kako će se postupati sa eventualnim detektovanim zarazama (način uklanjanja):

- automatski (***Automatski ukloni sve pretnje***)
- ili tek nakon dozvole korisnika (***Pitaj me pre uklanjanja pretnje***)

Ovaj izbor ne utiče na nivo bezbednosti, već samo zavisi od vaših želja.

U oba slučaja, možete da izaberete da li želite da uključite opciju ***Traži kolačiće za praćenje***. U određenim slučajevima, možete uključiti ovu opciju da biste postigli najviši nivo bezbednosti, ali je ona podrazumevano isključena. (*kolačići = 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*).

Napomena: *proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. 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* ***Alatke / Napredna podešavanja****, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu AVG napredna podešavanja.*

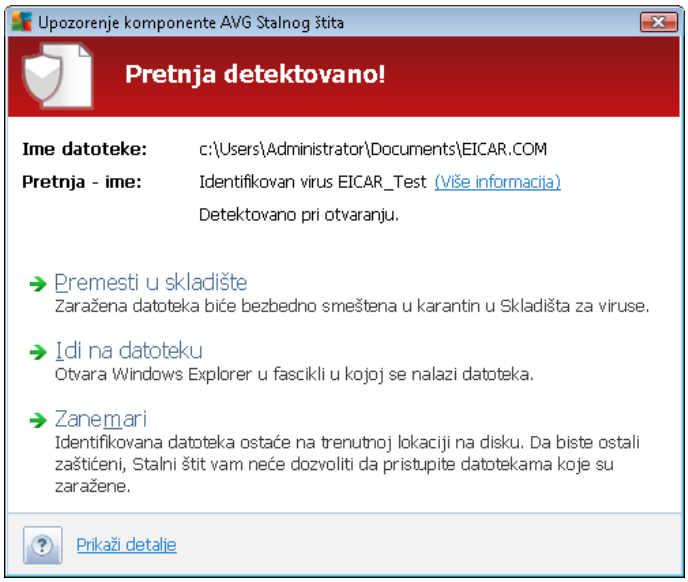
Kontrolna dugmad

U interfejsu komponente ***Stalni štit*** dostupna su sledeća kontrolna dugmad:

- ***Upravljanje izuzecima*** - otvara dijalog ***Stalni štit - izuzete stavke*** u kojem možete definisati koje će fascikle i datoteke biti izuzete iz skeniranja
- ***Sačuvaj promene*** - kliknite na ovo dugme da biste sačuvali i primenili promene koje ste napravili u ovom dijalogu
- ***Otkaži***- kliknite na ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenata*)

7.6.3. Detekcija od strane Stalnog štita

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*).

Dalje, morate da odlučite koju akciju treba preduzeti - sledeće opcije su dostupne:

Imajte u vidu da, zavisno od posebnih uslova (koja vrsta datoteke je zaražena i gde je locirana), sve opcije nisu uvek dostupne!

- ***Ukloni pretnju kao iskusan korisnik*** – označite ovo polje ako pretpostavljate da vam neće biti dozvoljeno da uklonite pretnju kao običan korisnik. Iskusni korisnici imaju šira prava pristupa, pa ćete, ako se pretnja nalazi u određenim sistemskim fasciklama, možda morati da upotrebite ovo polje za potvrdu da biste mogli da je uklonite.

- ***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 (*t.j. premestite u* ***Skladište virusa***)

- ***Premesti u Skladište*** - virus će biti premešten u AVG ***Skladište za viruse***

- ***Idi do datoteke*** - ova opcija vas preusmerava do tačne lokacije sumnjivog objekta (*otvara novi prozor programa Windows Explorer*)

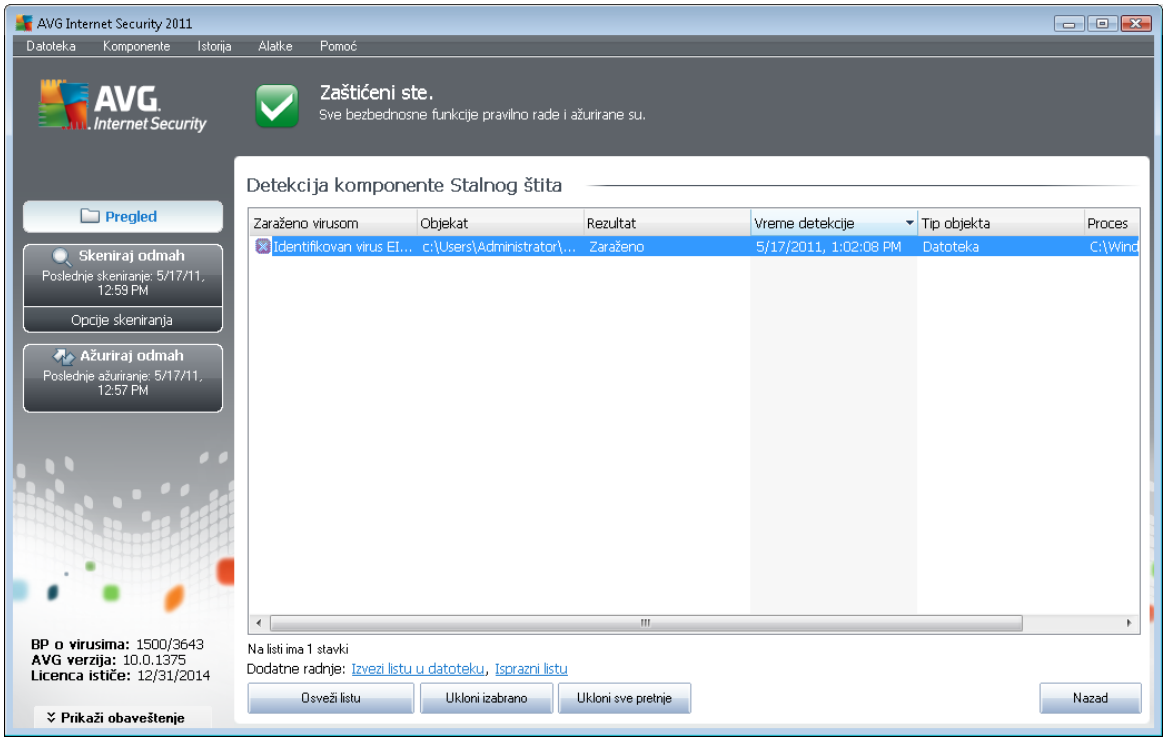
- ***Zanemari*** - savetujemo vam da NE koristite ovu opciju ako za to nemate dobar razlog!

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.

Celokupan pregled pretnji koje je detektovao***Stalni štit*** 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 štit***, 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*** vratiće vas u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenti*).

7.7. 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. Možete da podesite odgovarajući nivo zaštite za svako dete i da zasebno nadgledate svako dete putem jedinstvenih podataka za prijavljivanje.

Ova komponenta je aktivna samo ako je proizvod ***AVG Family Safety*** instaliran na vašem računaru. Ako proizvod ***AVG Family Safety*** nije instaliran, kliknite na odgovarajuću ikonu u okviru **AVG Internet Security 2011** korisničkog interfejsa i bićete preusmereni na Web lokaciju proizvoda gde možete da pronađete sve potrebne detalje.

7.8. AVG LiveKive

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.

Ova komponenta je aktivna samo ako je proizvod ***AVG LiveKive*** instaliran na vašem računaru. Ako proizvod ***AVG LiveKive*** nije instaliran, kliknite na odgovarajuću ikonu u okviru **AVG Internet Security 2011** korisničkog interfejsa i bićete preusmereni na Web lokaciju proizvoda gde možete da pronađete sve potrebne detalje.

7.9. Skener 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.

7.9.1. Principi skeniranja 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 i The Bat*). Prvenstveno je namenjen korišćenju sa aplikacijama e-pošte kao što su Outlook Express, Mozilla, Incredimail, itd.

Tokom instalacije programa AVG 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*).

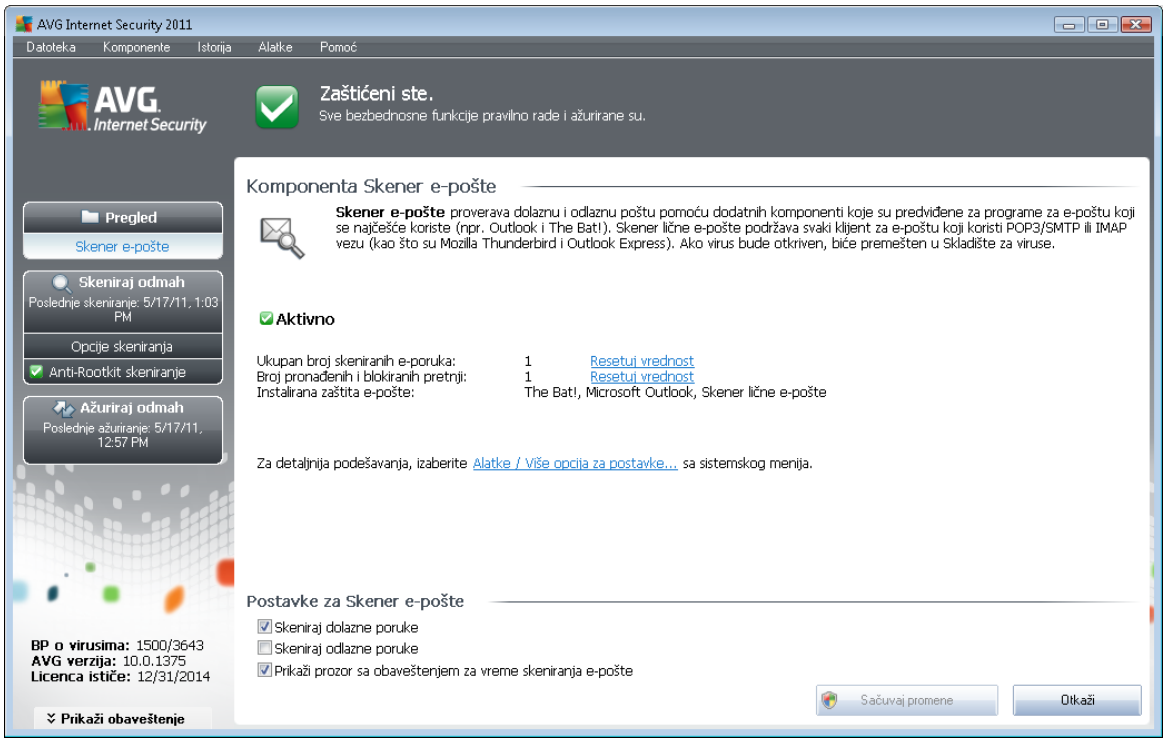
Skener e-pošte funkcioniše kao interfejs između klijenta e-pošte i servera e-pošte na Internetu.

- ***Dolazna pošta:*** kada primate 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 prilozima nalaze virusi, a zatim je šalje na SMTP server (*skeniranje odlazne pošte je podrazumevano onemogućeno i može se ručno podesiti*).

Napomena: *AVG skener e-pošte nije predviđen za serverske platforme!*

7.9.2. Interfejs komponente Skener e-pošte



U dijalogu komponente ***Skener e-pošte*** možete naći kratak tekst koji opisuje funkcionalnost ove komponente, informaciju o njenom trenutnom statusu i sledeće statističke podatke:

- ***Ukupan broj skeniranih e-poruka*** - broj skeniranih e-poruka od poslednjeg pokretanja komponente ***Skener e-pošte*** (*ova vrednost se po potrebi može poništiti; npr. u statističke svrhe - Poništi vrednost*)

- ***Broj pronađenih i blokiranih pretnji*** - broj detektovanih slučajeva zaraze u e-porukama od poslednjeg pokretanja komponente ***Skener e-pošte***

- ***Instalirana zaštita e-pošte*** - informacije o određenoj dodatnoj komponenti za zaštitu e-pošte koja se odnosi na vaš podrazumevani instalirani klijent za e-poštu.

Postavke za Skener e-pošte

U donjem delu dijaloga nalazi se odeljak po imenu ***Podešavanja skenera e-pošte*** u kojem možete urediti neke od osnovnih funkcija ove komponente:

- ***Skeniraj dolazne poruke*** - izaberite ovu opciju ako želite da se sve e-poruke koje stižu na vašnalog skeniraju kako bi se proverilo da li sadrže viruse. Ova opcija je podrazumevano uključena i ne preporučuje se da je menjate!
- ***Skeniraj odlazne poruke*** - izaberite ovu opciju ako želite da se sve e-poruke koje se šalju sa vašeg naloga skeniraju kako bi se proverilo da li sadrže viruse. Ova opcija je podrazumevano isključena.
- ***Prikaži prozor obaveštenja u toku skeniranja e-pošte*** - označite ovu stavku da potvrdite da želite da budete obaveštavani putem dijaloga za obaveštavanje koji se prikazuje iznad AVG ikone na sistemskoj traci tokom skeniranja e-pošte pomoću ***Skener e-pošte*** komponente. Ova opcija je podrazumevano uključena i ne preporučuje se da je menjate!

Napredna konfiguracija komponente ***Skener e-pošte*** dostupna je ako otvorite stavku sistemskog menija ***Alatke/Napredna podešavanja***; međutim, napredno konfigurisanje trebalo bi da obavljaju samo iskusni korisnici!

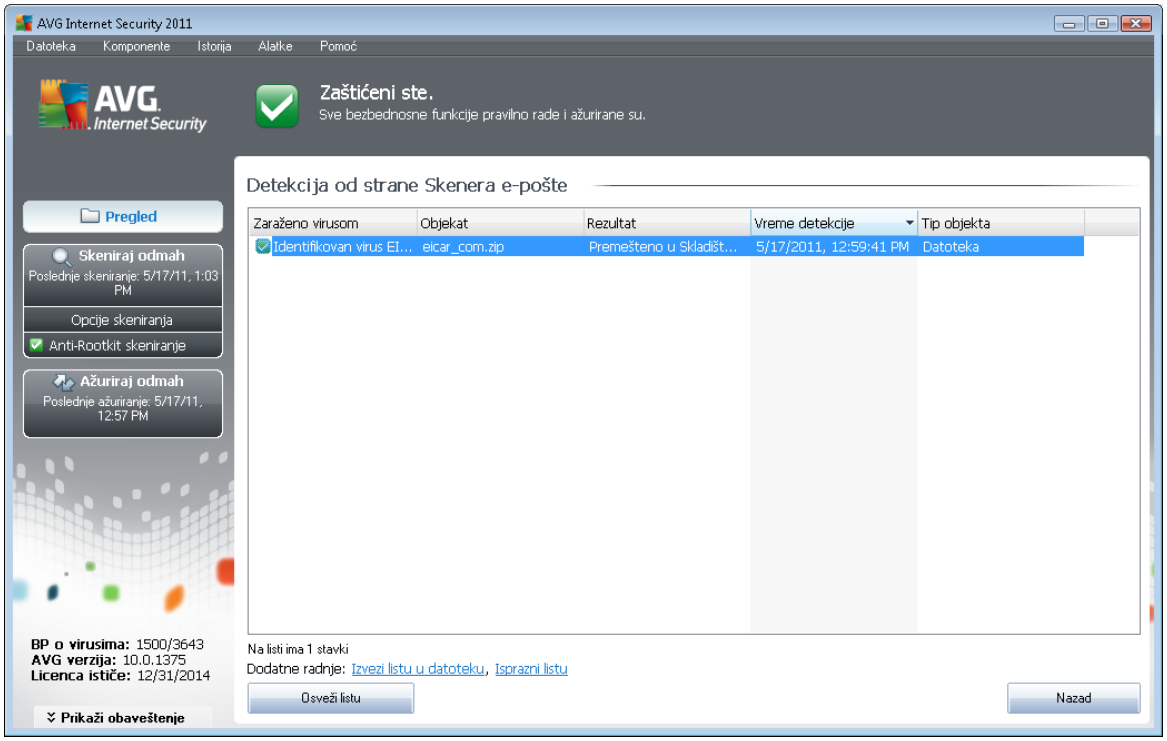
Imajte u vidu sledeće: *Proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku* ***Alatke / Napredna podešavanja****, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu AVG napredna podešavanja.*

Kontrolna dugmad

U interfejsu komponente ***Skener 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
- ***Otkaži***- kliknite na ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenata*)

7.9.3. Detekcija od strane skenera e-pošte



U dijalogu ***Detekcija skenerom e-pošte*** (*kojem možete pristupiti pomoću opcije iz sistemskog menija Istorija / Detekcija skenerom e-pošte*) moći ćete da vidite listu svih nalaza koje je detektovala komponenta ***Skener 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*** - ažuriranje liste otkrivenih pretnji
- ***Nazad*** - prebacuje vas nazad na prethodno prikazani dijalog

7.10. Upravljanje ažuriranjem

7.10.1. Principi upravljanja ažuriranjem

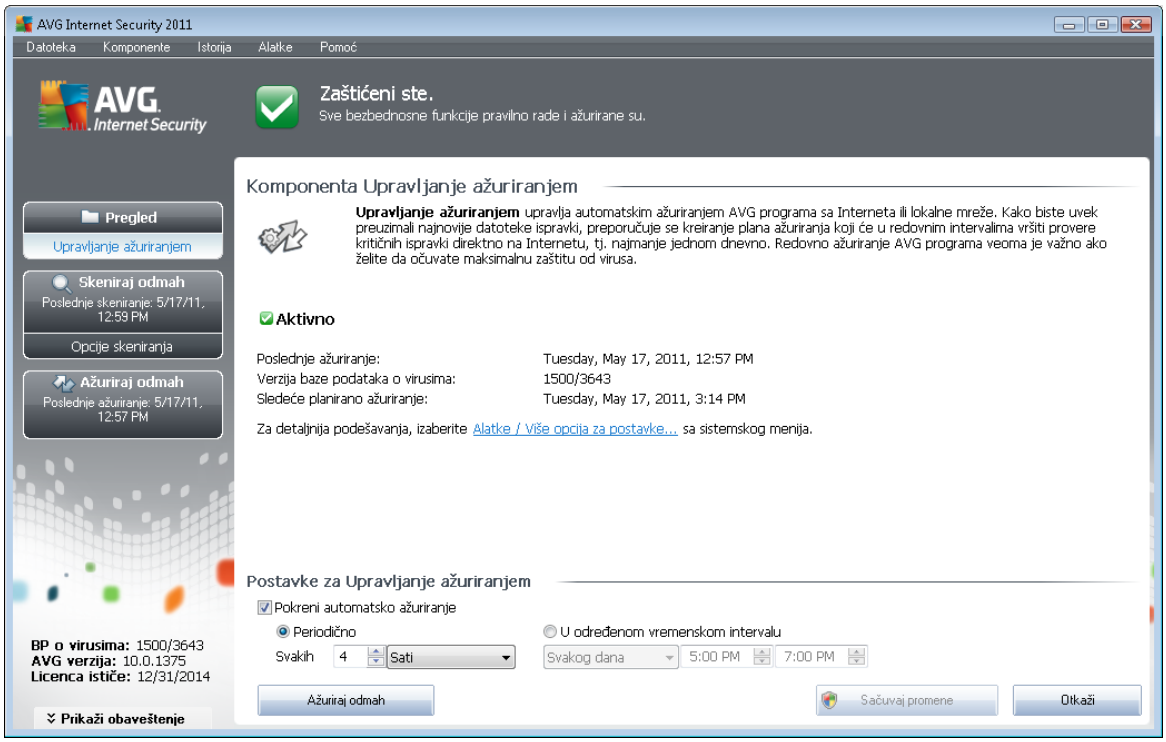
Nijedan bezbednosni softver ne može garantovati pouzdanu zaštitu od raznih vrsta pretnji ako se redovno ne ažurira! Kreatori virusa stalno traže nove propuste u softveru i operativnim sistemima koje mogu da iskoriste. Svakodnevno se pojavljuju novi virusi, nov malver, novi napadi sa mreže. Zato proizvođači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

Od ključnog je značaja da redovno ažurirate program AVG!

Komponenta ***Upravljanje ažuriranjem*** pomaže vam da upravljate redovnim ažuriranjem. U okviru ove komponente, možete zakazati automatsko preuzimanje datoteka za ažuriranje sa Interneta ili lokalne mreže. Ažuriranje osnovnih definicija virusa trebalo bi da se obavlja svakodnevno, ako je moguće. Manje hitno ažuriranje programa može se obavljati jednom nedeljno.

Napomena: *Obratite pažnju na poglavlje Ažuriranje programa AVG za više informacija o vrstama i nivoima ažuriranja!*

7.10.2. Interfejs komponente Upravljanje ažuriranjem



Interfejs ***Upravljanje ažuriranjem***prikazuje informaciju o funkcionalnosti komponente, njenom trenutnom statusu i pruža važne statističke podatke:

- ***Poslednje ažuriranje*** – navodi datum i vreme poslednjeg ažuriranja baze podataka
- ***Verzija baze podataka*** - definiše broj verzije trenutno instalirane baze podataka virusa; taj broj se uvećava nakon svakog ažuriranja baze podataka virusa
- ***Sledeće planirano ažuriranje*** – navodi datum i vreme sledećeg planiranog ažuriranja baze podataka

Postavke za Upravljanje ažuriranjem

U donjem delu dijaloga pronaći ćete odeljak***Postavke upravljanja ažuriranjem*** gde možete praviti promene pravila za pokretanje ažuriranja. Možete definisati da li želite da se datoteke za ažuriranje automatski preuzimaju (***Automatski započni ažuriranje***) ili samo na zahtev. Opcija ***Automatski započni ažuriranje*** podrazumevano je uključena i preporučuje se da to ne menjate! Redovno preuzimanje najnovijih datoteka za ažuriranje ključno je za ispravan rad bilo kojeg bezbednosnog softvera!

Takođe možete definisati vreme pokretanja ažuriranja:

- ***Periodično*** - definišite vremenski interval
- ***U određenom vremenskom intervalu*** - definišite tačno vreme u toku svakog dana kada ažuriranje treba da se pokrene

Podrazumevano je da se ažuriranje obavlja svaka četiri sata. Preporučuje se da ne menjate ovo podešavanje ukoliko nemate ozbiljan razlog za to!

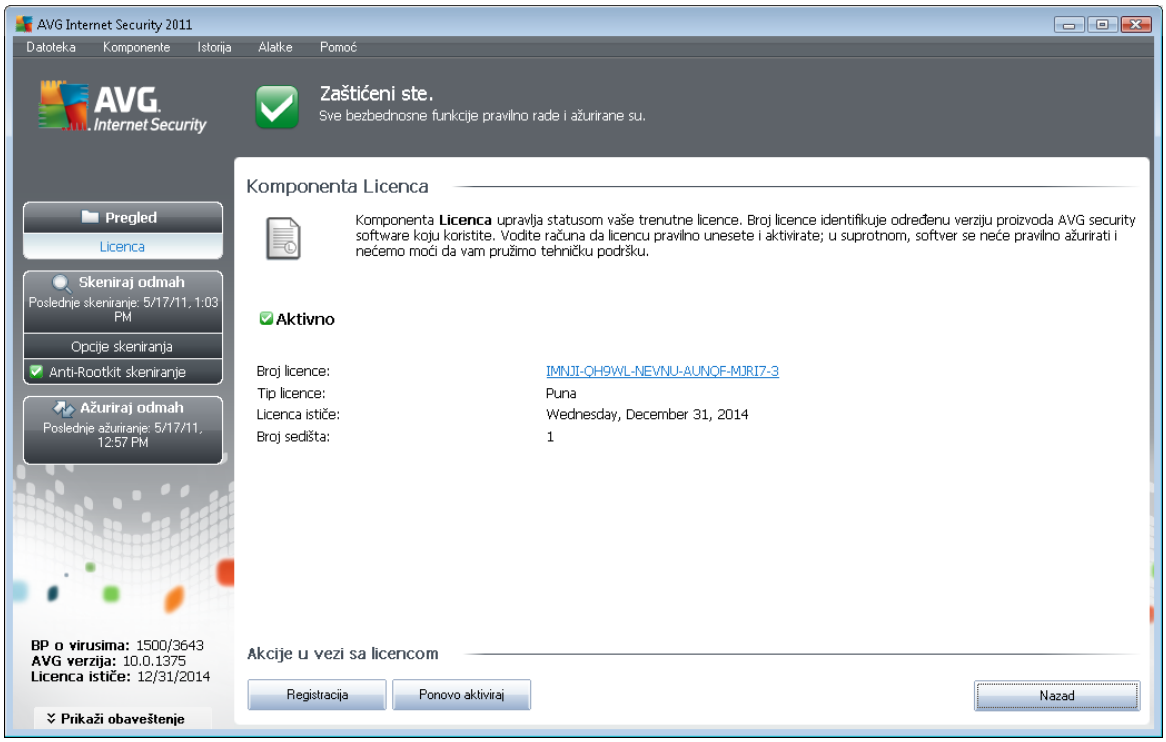
Napomena: *proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku* ***Alatke / Napredna podešavanja****, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu AVG napredna podešavanja.*

Kontrolna dugmad

U interfejsu komponente ***Upravljanje ažuriranjem*** dostupna su sledeća kontrolna dugmad:

- ***Ažuriraj odmah*** - pokreće trenutno ažuriranje na zahtev
- ***Sačuvaj promene*** - kliknite na ovo dugme da biste sačuvali i primenili promene koje ste napravili u ovom dijalogu
- ***Otkaži***- kliknite na ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenata*)

7.11. Licenca



U interfejsu komponente ***Licenca*** naći ćete kratak tekst koji opisuje funkcionalnost komponente, informaciju o njenom trenutnom statusu i sledeće informacije:

- ***Broj licence*** - pruža skraćenu formu broja vaše licence (*iz bezbednosnih razloga nedostaje zadnjih četiri simbola*). Pri unošenju vašeg broja licence, morate biti potpuno precizni i uneti je kao što je prikazano. Zbog toga vam preporučujemo da pri svakom unošenju broja licence koristite metod „kopiraj i nalepi“.

- ***Tip licence*** - određuje tip instaliranog proizvoda.

- ***Licenca ističe*** - ovaj datum određuje period važenja vaše licence. Ako želite da nastavite da koristite **AVG Internet Security 2011** nakon tog datuma, morate obnoviti licencu. Obnavljanje licence možete obaviti na mreži na AVG web lokaciji.

- ***Broj sedišta*** - broj radnih stanica na kojima imate pravo da instalirate **AVG Internet Security 2011**.

Kontrolna dugmad

- ***Registracija*** - povezivanje sa stranicom za registraciju na AVG Web lokaciji (http://www.avg.com/). Unesite registracione podatke; besplatnu tehničku podršku mogu dobiti samo korisnici koji registruju svoj AVG proizvod.

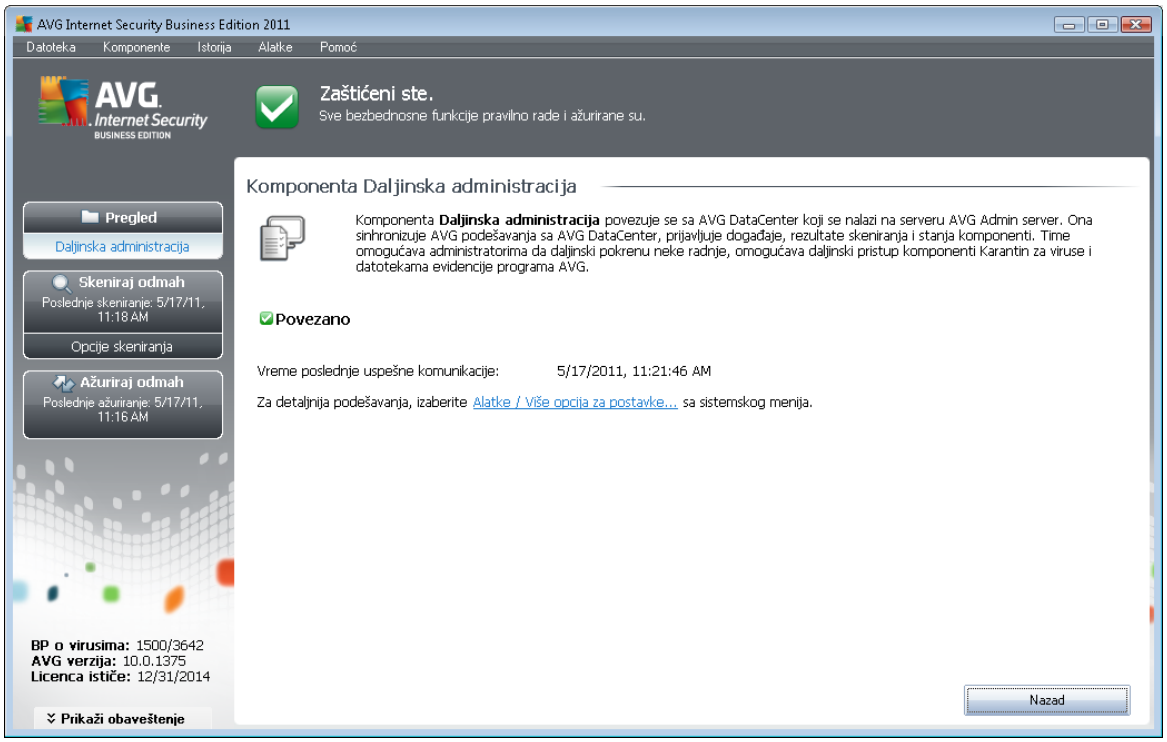
- ***Ponovo aktiviraj*** - otvaranje dijaloga ***Aktivacija AVG programa*** sa podacima koje ste uneli u dijalogu ***Prilagođavanje programa AVG*** u toku procesa instalacije. U ovom

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*).

Napomena: *Ako koristite probnu verziju programa* **AVG Internet Security 2011**, *na dugmadima se prikazuje tekst* ***Kupite odmah*** *i* ***Aktivacija***, *i ona vam omogućavaju da odmah kupite punu verziju programa. Ako je* **AVG Internet Security 2011** *instaliran sa prodajnim brojem, na dugmadima se prikazuje tekst* ***Registracija*** *i* ***Aktivacija***.

- ***Nazad***- pritisnite ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenti*).

7.12. Daljinska administracija



Komponenta ***Daljinska administracija*** prikazuje se u korisničkom interfejsu **AVG Internet Security 2011** samo ako ste instalirali Business Edition Vašeg proizvoda (*vidite komponentu* ***Licenca***). U dijalogu ***Daljiska administracija*** možete naći informacije o tome da li je komponenta aktivna i povezana sa serverom. Sva podešavanja komponente ***Daljinska administracija*** moraju se izvršiti u okviru***Napredna podešavanja / Daljinska administracija***.

Za detaljan opis opcija komponente i funkcija u okviru AVG sistema za daljinsku administraciju pročitajte dokumentaciju koja je posvećena isključivo toj temi. Ova dokumentacija se može preuzeti na AVG web lokaciji (www.avg.com), u odeljku ***Centar za podršku / Preuzimanje / Dokumentacija*** .

Kontrolna dugmad

- ***Nazad*** - pritisnite ovo dugme da biste se vratili u podrazumevani AVG korisnički interfejs (*pregled komponenti*).

7.13. Online Shield

7.13.1. Princip rada komponente Online Shield

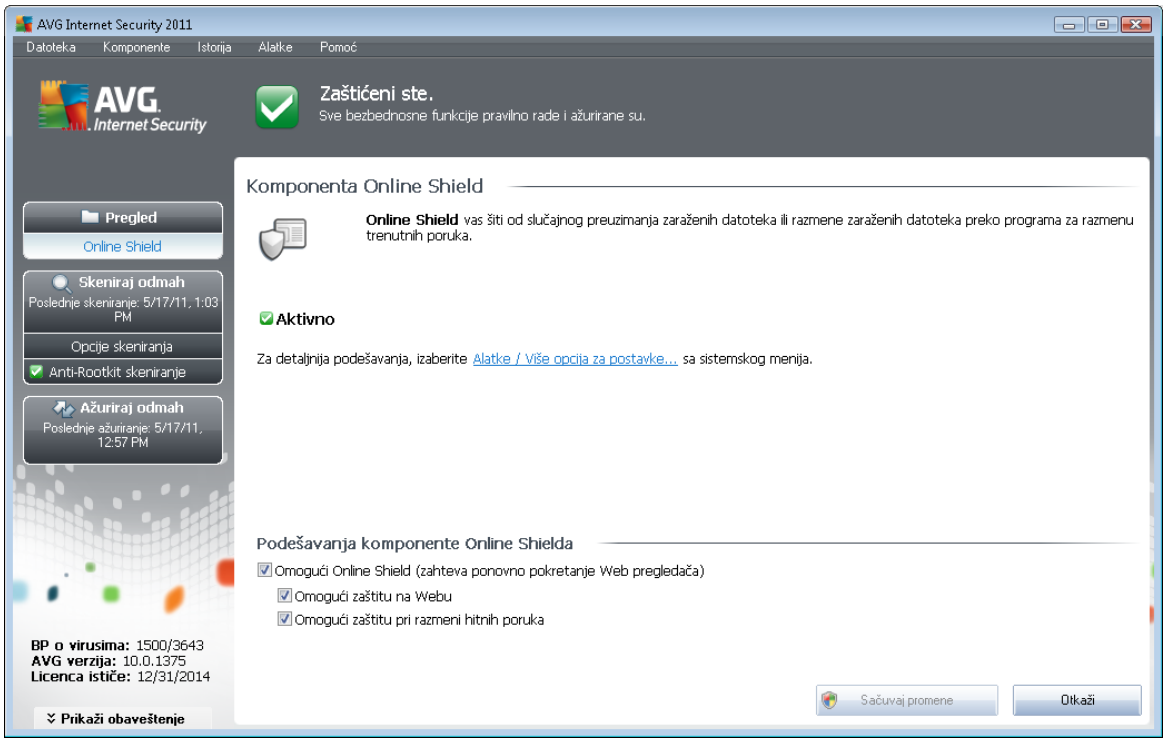
Online Shield predstavlja vrstu stalne zaštite u realnom vremenu; on skenira sadržaj web stranica koje posećujete (*i potencijalne datoteke koje se na njima nalaze*) čak pre nego što se prikažu u vašem web pregledaču ili preuzmu na vaš računar.

Online Shield detektuje ako stranica koju želite da posetite sadrži opasan javascript i sprečava prikazivanje stranice. Takođe, on prepoznaje malver koji se nalazi na stranici i odmah prekida njegovo preuzimanje kako ne bi dospeo na vaš računar.

Napomena: *AVG Online Shield nije namenjen za serverske platforme!*

7.13.2. Interfejs komponente Online Shield

Interfejs komponente ***Online Shield*** opisuje ponašanje ove vrste zaštite. Dalje možete naći informaciju o trenutnom statusu komponente. U donjem delu ekrana nalaze se osnovne opcije za uređivanje funkcija ove komponente:



Podešavanja komponente Online Shield

Kao prvo, na raspolaganju vam je opcija da istog trenutka uključite/isključite komponentu ***Online Shield*** tako što ćete označiti stavku ***Omogući Online Shield***. Ova opcija je podrazumevano omogućena, pa je i komponenta ***Online Shield*** . Osim ako nemate dobar razlog da menjate ove postavke, preporučujemo da ova komponenta ostane aktivna. Ako je stavka označena i ***Online Shield***je aktivan, još dve opcije konfigurisanja se aktiviraju:

- ***Omogući zaštitu na webu*** - ovom opcijom se potvrđuje da ***Online Shield*** treba da obavlja skeniranje sadržaja web stranica.
- ***Omogući zaštitu hitnih poruka*** - označite ovu stavku ako želite da ***Online Shield***potvrdi da je komunikacija hitnim porukama (*npr. ICQ, MSN Messenger, ...*) bezbedna od virusa.

Napomena: *proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. 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* ***Alatke / Napredna podešavanja****, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu AVG napredna podešavanja.*

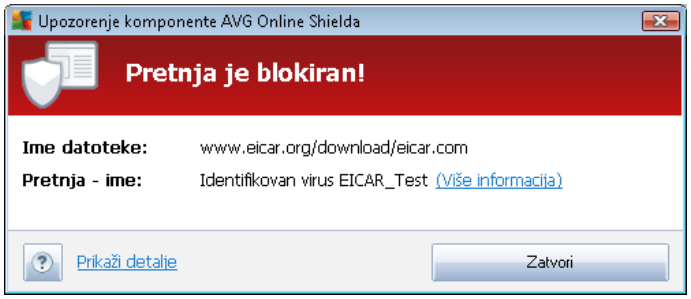
Kontrolna dugmad

U interfejsu komponente ***Online Shield*** dostupna su sledeća kontrolna dugmad:

- ***Sačuvaj promene*** - kliknite na ovo dugme da biste sačuvali i primenili promene koje ste napravili u ovom dijalogu
- ***Otkaži***- kliknite na ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenti*)

7.13.3. Detekcija komponente Online Shield

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:



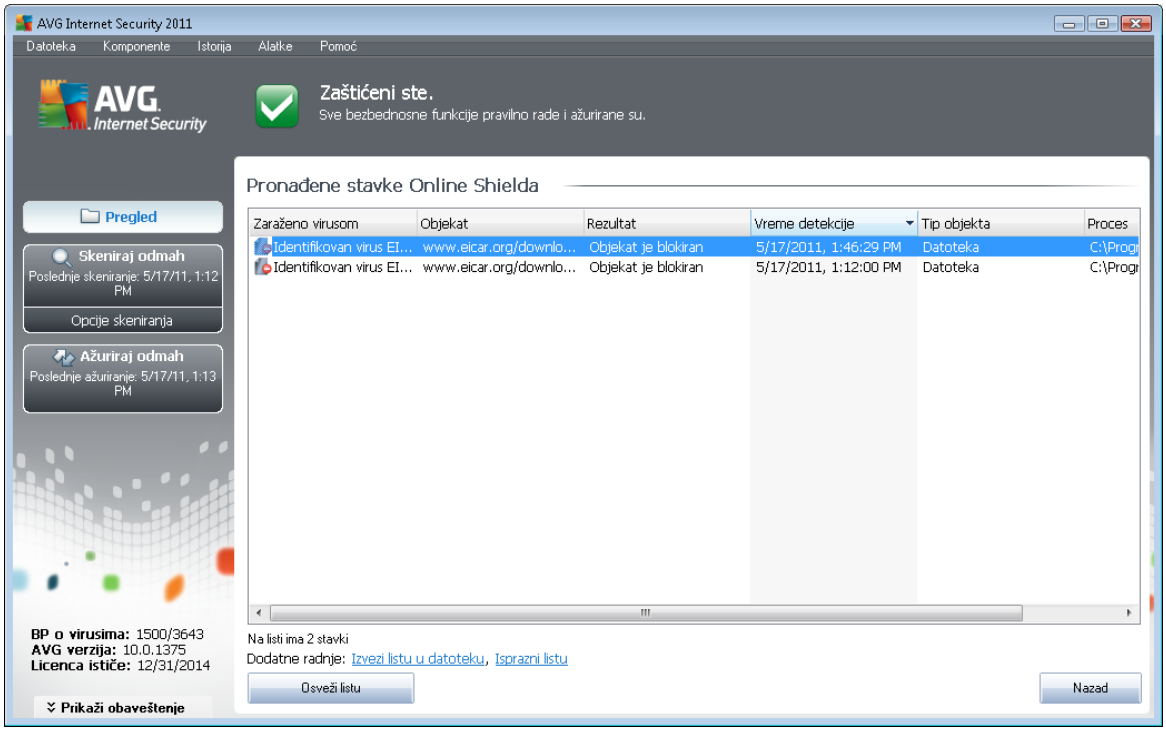
U okviru ovog dijaloga upozorenja naći ćete podatke o datoteci koja je detektovana i obeležena kao zaražena (*Naziv datoteke*), naziv prepoznate infekcije (*Naziv pretnje*), i vezu ka ***Enciklopediji virusa*** gde možete naći detaljne informacije o detektovanoj infekciji(*ukoliko je poznata*). Ovaj 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***). Dugme ***Osveži listu*** će ažurirati listu pretnji koje je pronašao ***Online Shield***. Dugme ***Nazad*** vratiće vas u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenti*).

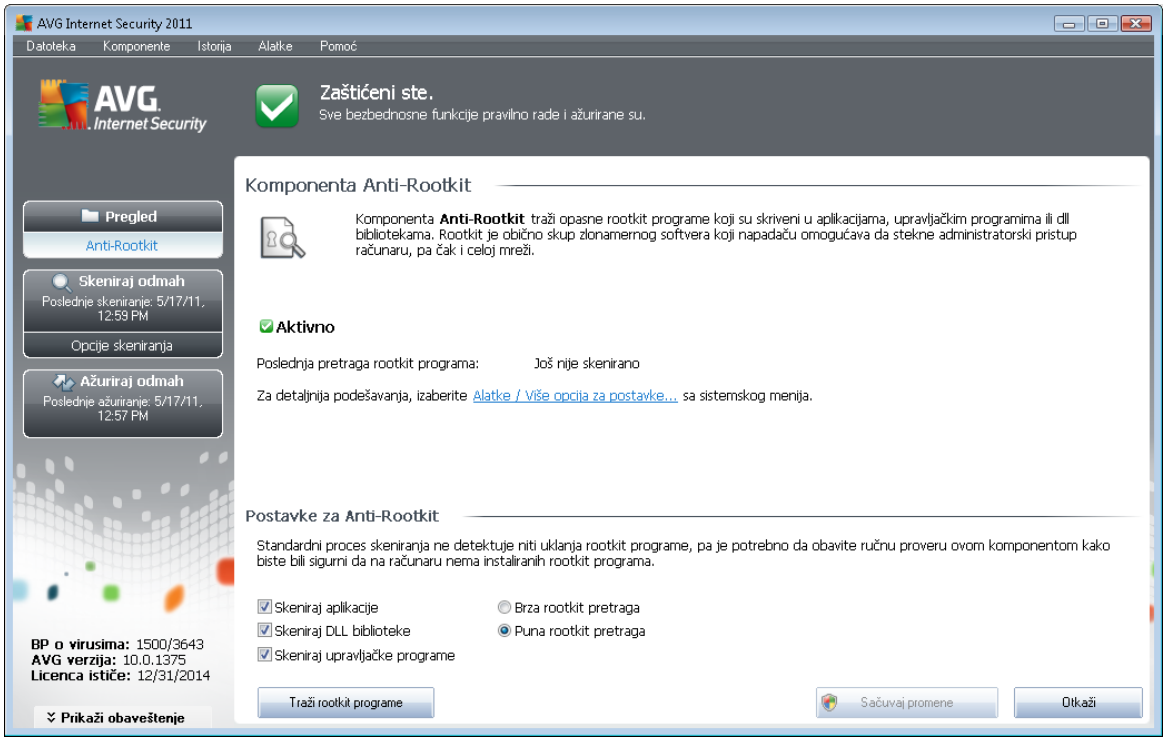
7.14. Anti-Rootkit

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.

7.14.1. Principi odbrane od rootkit programa

AVG Anti-Rootkit je specijalizovana alatka koja otkriva i efikasno uklanja opasne rootkit programe, tj. programe i tehnologije koji mogu da prikriju prisustvo zlonamernog softvera na vašem računaru. ***AVG 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 ***AVG 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.

7.14.2. Interfejs komponente Anti-Rootkit



Interfejs komponente ***Anti-Rootkit***pruža kratak opis funkcionalnosti komponente, informiše o trenutnom statusu komponente i takođe pruža informaciju kada je poslednji put pokrenut test ***Anti-Rootkit*** (***Poslednja rootkit pretraga***). Dijalog***Anti-Rootkit***dalje pruža vezu ka opcijama***Alati/ Napredna podešavanja***. Koristite vezu da se preusmerite ka okruženju za napredno konfigurisanje

Anti-Rootkitkomponente.

Imajte u vidu sledeće: *Proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja bi trebalo da menjaju samo iskusni korisnici.*

Anti-Rootkit podešavanja

U donjem delu dijaloga pronaći ćete odeljak ***Anti-Rootkit podešavanja*** u kojem možete podesiti osnovne funkcije rootkit skeniranja. Prvo potvrdite izbor u odgovarajućim poljima za potvrdu da biste odredili objekte koje bi trebalo skenirati:

- ***Skeniraj aplikacije***
- ***Skeniraj DLL biblioteke***
- ***Skeniraj upravljačke programe***

Zatim možete izabrati 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*)

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 komponenata*)
- ***Otkaži*** - pritisnite ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenata*) bez čuvanja unetih izmena

7.15. Sistemske alatke

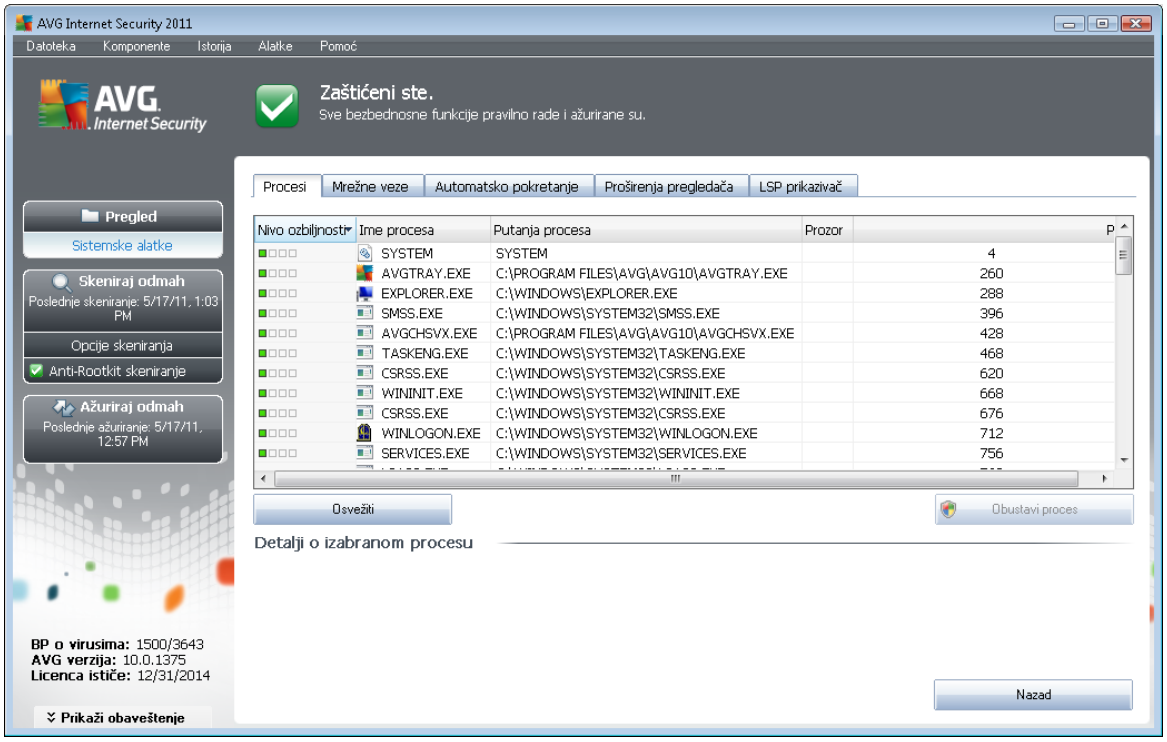
Sistemske alatake – odnosi se na alatke koje pružaju detaljan pregled **AVG Internet Security 2011** okruženja i operativnog sistema. Komponenta nudi pregled:

- 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!

7.15.1. Procesi



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

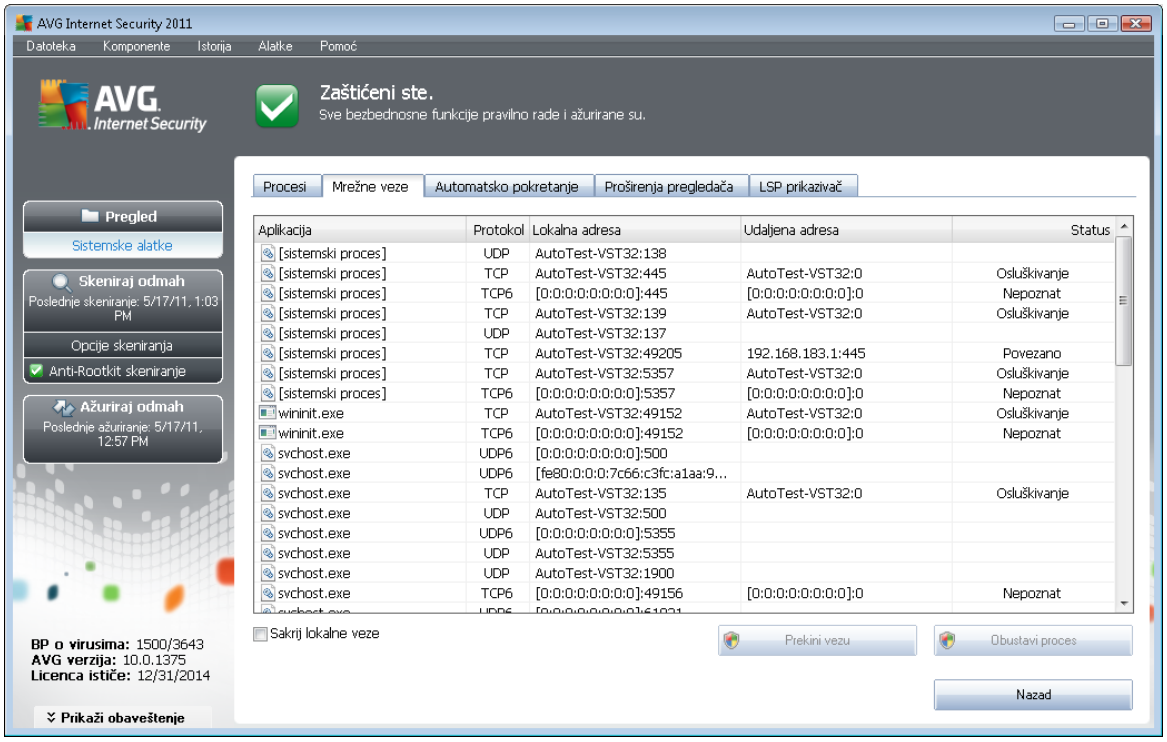
- ***Nivo ozbiljnosti*** – grafički prikaz ozbiljnosti odgovarajućeg procesa na skali od četiri nivoa počevši od manje ozbiljne pretnje (■□□□) pa do veoma ozbiljne (■■■■)
- ***Ime procesa*** - ime aktivnog procesa.
- ***Putanja procesa*** - fizička putanja do pokrenutog procesa
- ***Prozor*** - označava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

Kontrolna dugmad

U intefejsu ***Sistemske alatke*** 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 AVG korisnički interfejs (*pregled komponenti*)

7.15.2. 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

Dostupna su sledeća kontrolna dugmad:

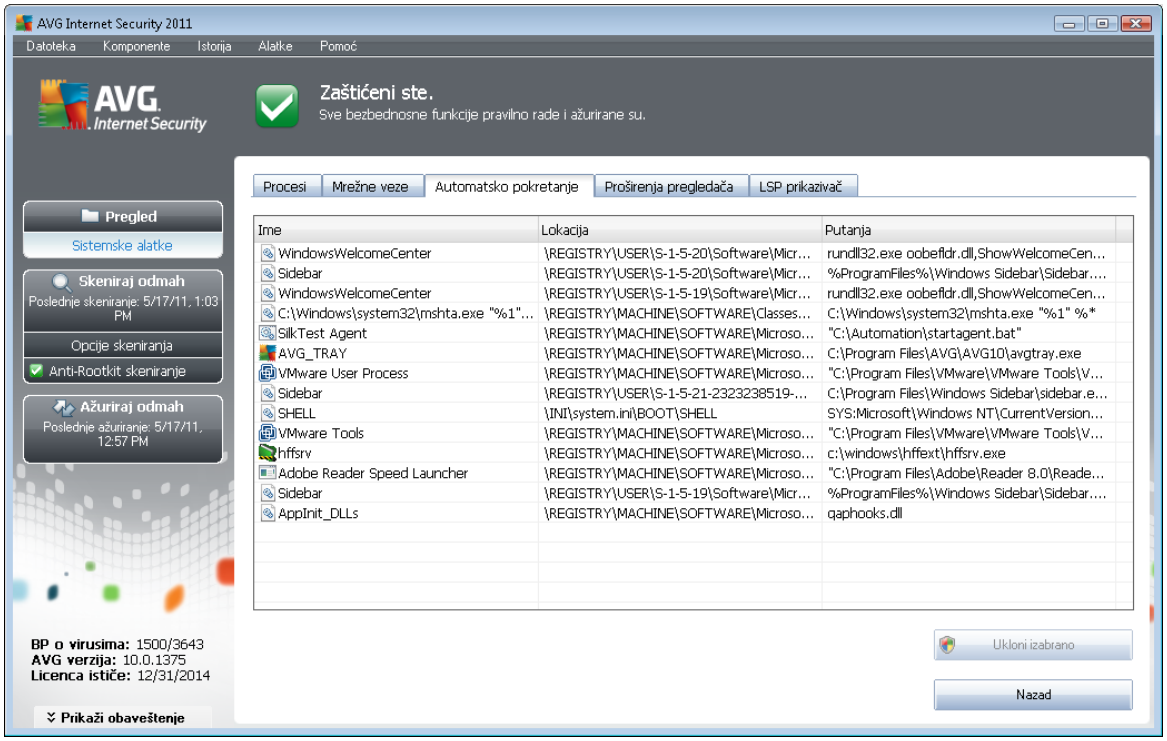
- ***Prekini vezu*** - prekidanje jedne ili više mreža koje ste izabrali na listi

- ***Prekini proces*** - zatvaranje jedne ili više aplikacija koje koriste vezu izabranu na listi

- ***Nazad*** - vraćanje na podrazumevani ***AVG korisnički interfejs*** (pregled komponenata).

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!

7.15.3. Automatsko pokretanje



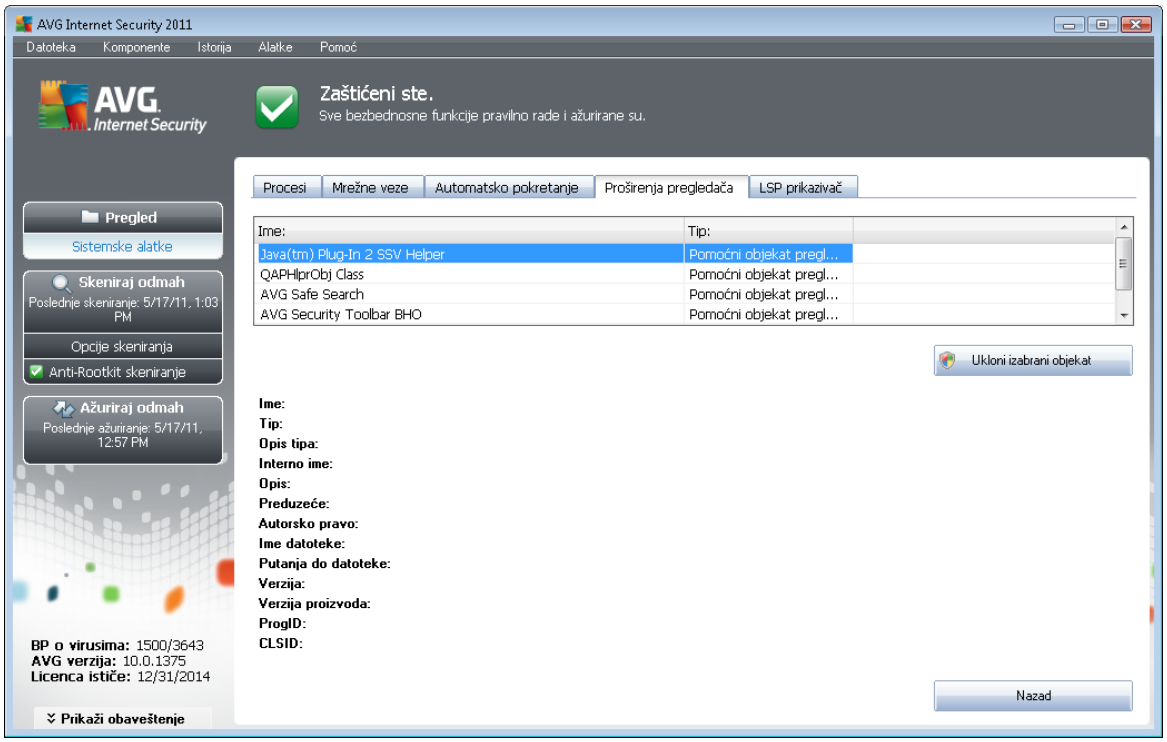
U dijalogu ***Automatsko pokretanje*** data je lista svih aplikacija koje se pokreću zajedno sa

operativnim sistemom Windows. Vrlo često se dešava da se nekoliko malver aplikacija doda u stavku pokretanja u registratoru.

Jednu ili više stavki možete da izbrišete tako što ćete ih izabrati i kliknuti na dugme ***Izbriši izabrane stavke.*** Dugme ***Nazad*** vratiće vas u podrazumevani AVG korisnički interfejs (*pregled komponenti*).

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

7.15.4. Proširenja pregledača



Dijalog ***Proširenja pregledača*** sadrži listu dodatnih komponenata (*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.

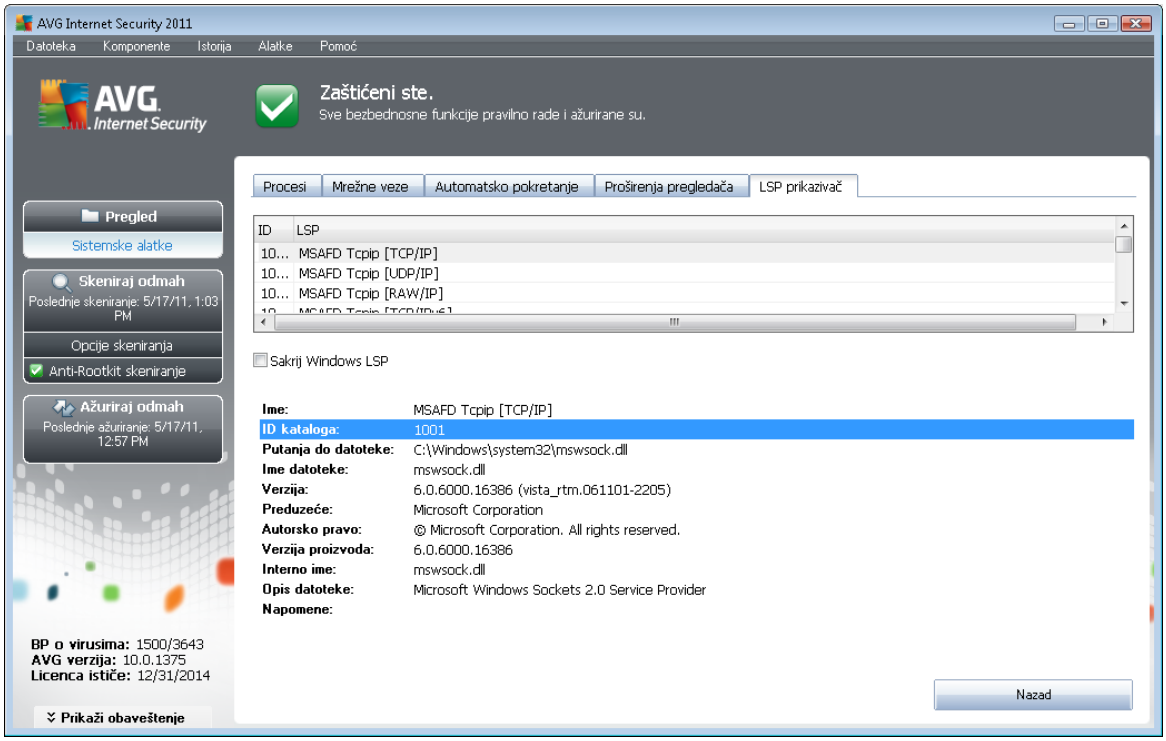
Kontrolna dugmad

Na kartici ***Proširenja pregledača*** nalaze se 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 ***AVG korisnički interfejs*** (pregled komponenti)

7.15.5. LSP prikazivač



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

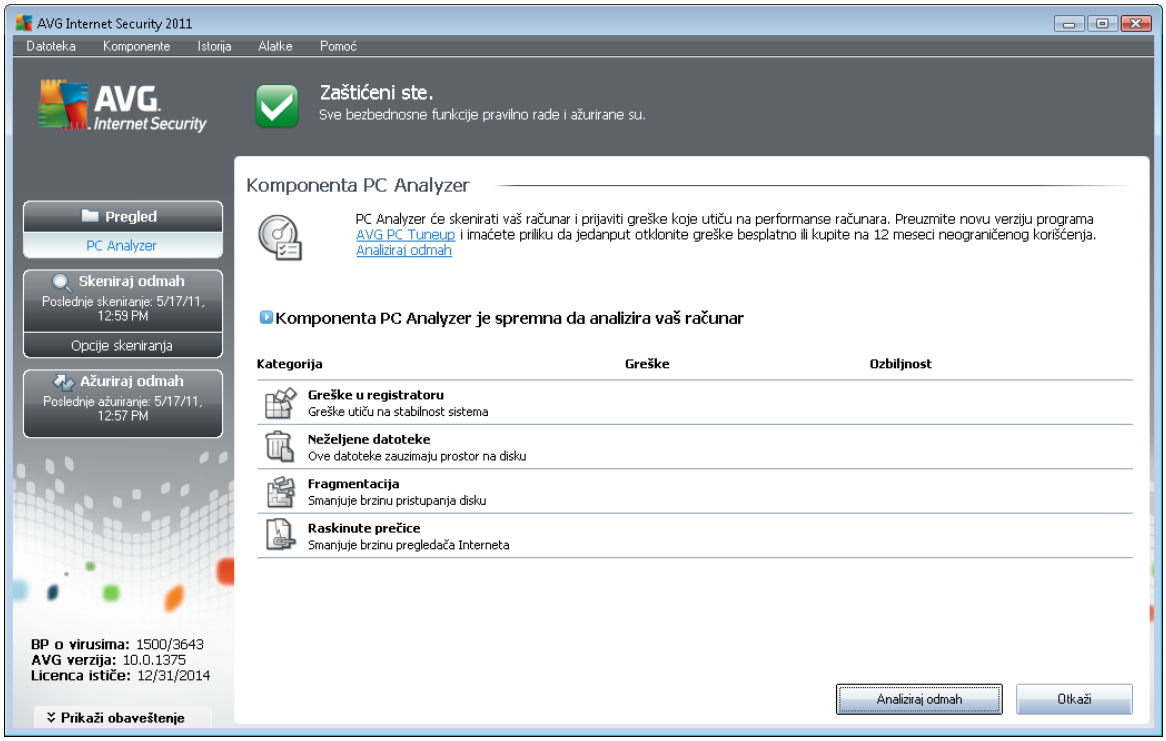
Dobavljač slojevitih usluga (LSP) je sistemski upravljački program povezan sa uslugama umrežavanja operativnog sistema Windows. On ima pristup svim podacima koji se unose na računar, kao i onima koji se šalju sa računara, uključujući i mogućnost izmene ovih podataka. Neki LSP-ovi su neophodni da bi se 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.

Da biste na listu uključili Windows LSP, opozovite izbor u polju za potvrdu ***Sakrij Windows LSP.***
Dugme ***Nazad*** vratiće vas u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenti*).

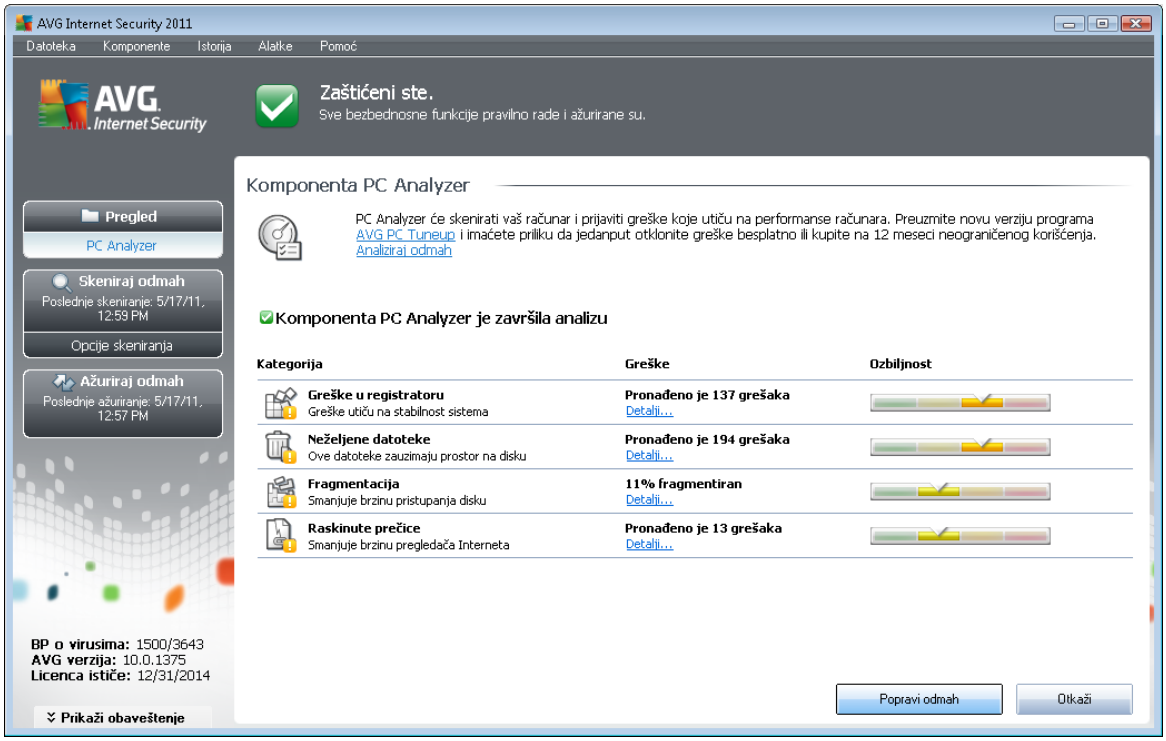
7.16. PC Analyzer

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 popravljanje 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 odmah*** (*prikazuje se pre nego što analiza počne*) - pritisnite ovo dugme da odmah pokrenete analizu vašeg računara
- ***Popravi sada*** (*prikazano kada se analiza završi*)- pritisnite dugme da odete na AVG web lokaciju (http://www.avg.com/) na stranicu koja pruža detaljne i ažurirane informacije u vezi sa komponentom ***PC Analyzer***
- ***Otkaži*** - pritisnite ovo dugme da zaustavite pokrenutu analizu ili da se vratite na podrazumevani AVG korisnički interfejs (*pregled komponenti*) kada se analiza završi

7.17. Zaštita identiteta

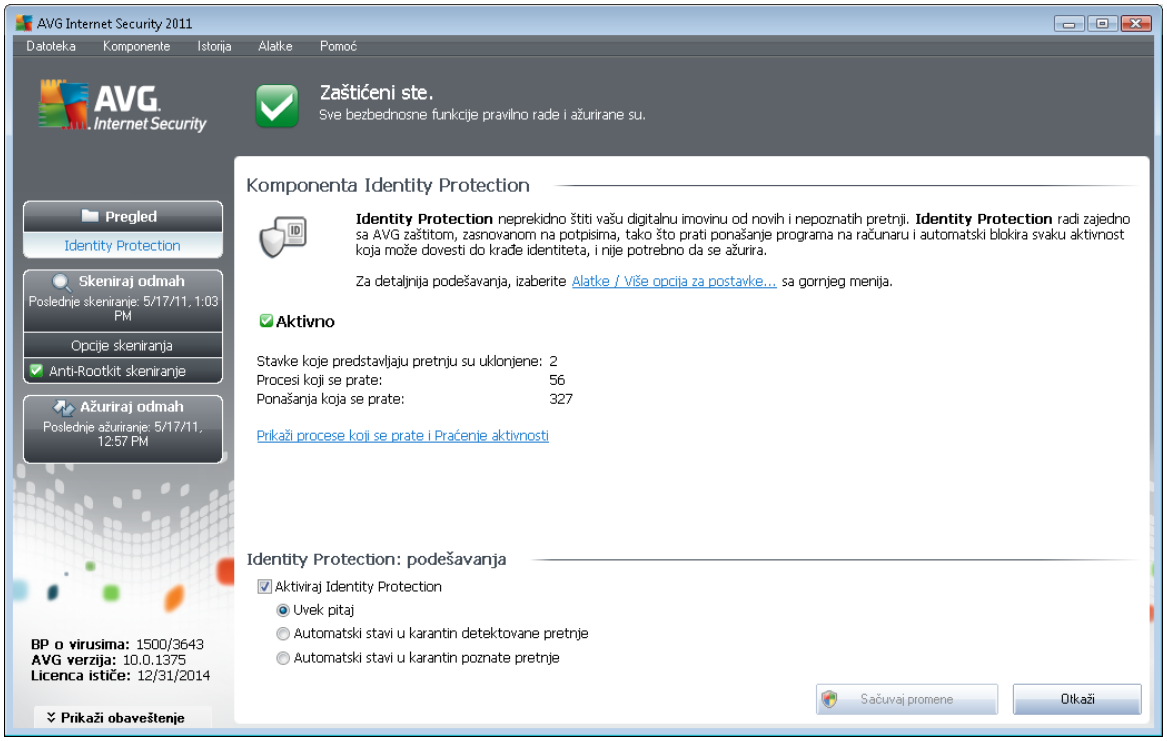
AVG zaštita identiteta je proizvod za odbranu od malvera čija je namena da spreči kradljivce identiteta da ukradu vaše lozinke, podatke o bankovnom računu, brojeve kreditnih kartica i druge vredne digitalne podatke pomoću različitih vrsta zlonamernog softvera (*malvera*) usmerenog na vaš računar. Ova komponenta vodi računa o tome da svi programi na vašem računaru rade pravilno. ***AVG zaštita identiteta*** konstantno uočava i blokira sumnjivo ponašanje i štiti vaš računar od svih vrsta novog malvera.

7.17.1. Principi zaštite identiteta

AVG zaštita identiteta je komponenta odbrane od malvera koja vas štiti od različitih vrsta malvera (*špijunskog softvera, botova, krađe identiteta, ...*) upotrebom tehnologija za analizu ponašanja i pruža zaštitu od nepoznatih i novih virusa. Budući da malver programi postaju sve složeniji i dolaze u obliku običnih programa koje mogu vaš računar staviti u službu napadača koji želi da ukrade vaš identitet, ***AVG zaštita identiteta*** vas štiti od ovakve nove vrste malvera koji se izvršava kao običan program. Ova komponenta nudi dodatnu zaštitu pored one koju pruža ***AVG Anti-Virus***koji vas štiti od poznatih virusa i virusa u obliku datoteke upotrebom mehanizma potpisa i skeniranjem.

Preporučujemo da instalirate i komponentu AVG Anti-Virus i komponentu „AVG zaštita identiteta“ kako biste imali kompletnu zaštitu vašeg računara.

7.17.2. Interfejs zaštite identiteta



Interfejs komponente ***Zaštita identiteta***pruža kratak opis osnovne funkcionalnosti komponente, njen status i neke statističke podatke:

- ***Uklonjeni malver programi*** - 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 ***Sistemski alati*** gde možete naći detaljan pregled svih nadgledanih procesa.

Podešavanja zaštite identiteta

U donjem delu dijaloga nalazi se odeljak ***Postavke zaštite identiteta*** u kojem možete urediti neke od osnovnih funkcija ove komponente:

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

U nekim slučajevima, komponenta ***Zaštita identiteta*** može prijaviti da su neke validne datoteke sumnjive ili opasne. Budući da komponenta ***Zaštita identiteta*** 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 ***Zaštita identiteta*** 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

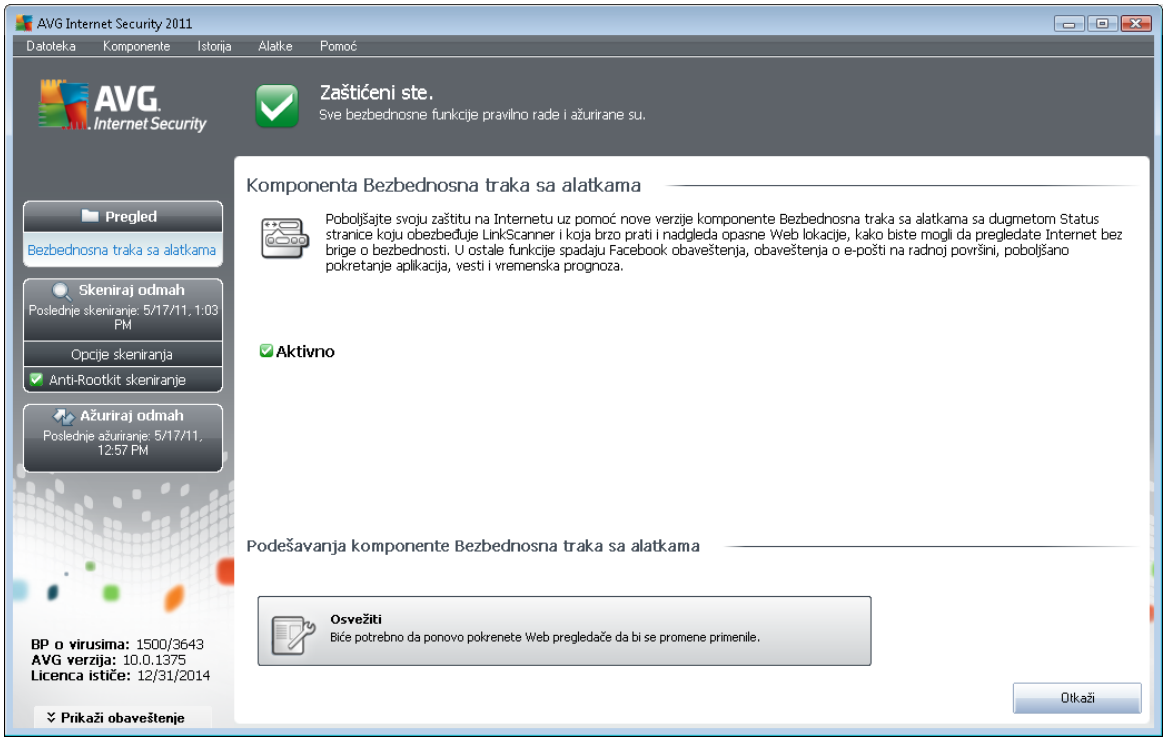
Kontrolna dugmad

U interfejsu komponente ***Zaštita identiteta*** dostupna su sledeća kontrolna dugmad:

- ***Sačuvaj promene*** - kliknite na ovo dugme da biste sačuvali i primenili promene koje ste napravili u ovom dijalogu
- ***Otkaži***- kliknite na ovo dugme da biste se vratili u podrazumevani ***AVG korisnički interfejs*** (*pregled komponenata*)

7.18. Bezbednosna traka sa alatkama

Bezbednosna traka sa alatkama je opcionalna traka sa alatkama za Web pregledač koja pruža poboljšanu AVG zaštitu i lak pristup raznim funkcijama u toku pregledanja Interneta. ***Bezbednosnu traku sa alatkama*** trenutno podržavaju Web pregledači Internet Explorer (*6.0 ili novija verzija)* i Mozilla Firefox *(3.0 ili novija verzija*):



Svim podešavanjima komponente ***Bezbednosna traka sa alatkama*** možete pristupiti direktno iz ***Bezbednosne trake sa alatkama*** u Web pregledaču.

8. AVG bezbednosna traka sa alatkama

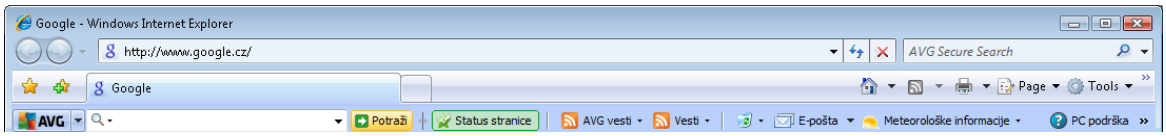
AVG bezbednosna traka sa alatkama je nova alatka koja radi u kombinaciji sa komponentom ***LinkScanner*** . ***AVG bezbednosna traka sa alatkama***se može koristiti za kontrolu funkcija ***LinkScanner*** i podešavanje njihovog ponašanja.

Ako izaberete da instalirate traku sa alatkama tokom instalacije **AVG Internet Security 2011**, ona će automatski biti dodata u vaš Web pregledač (*Internet Explorer 6.0 ili novija verzija i Mozilla Firefox 3.0 ili novija verzija*). Ostali Web pregledači trenutno nisu podržani.

Napomena: *ako koristite neki alternativni pregledač Interneta (npr. Avant Browser) može doći do neočekivanog ponašanja.*

8.1. Interfejs AVG bezbednosne trake sa alatkama

AVG bezbednosna traka sa alatkama je osmišljena da radi sa programima ***MS Internet Explorer*** (*verzija 6.0 ili novija*) i ***Mozilla Firefox*** (*verzija 3.0 ili novija*). Kada ste odlučiti da instalirate ***AVG bezbednosnu traku sa alatkama*** (*tokom procesa instalacije programa AVG od vas se tražilo da odlučite da li želite ili ne želite da instalirate komponentu*), komponenta će se nalaziti u vašem web pregledaču odmah ispod trake za adresu:



AVG bezbednosna traka sa alatkama sastoji se od sledećih elemenata:

8.1.1. AVG dugme sa logotipom

Ovo dugme omogućava pristup glavnim stavkama trake sa alatkama. Kliknite na dugme sa logotipom da biste bili preusmereni na AVG web lokaciju. Ako kliknete na pokazivač pored AVG ikone, otvoriće se sledeće:

- ***Informacije o traci sa alatkama*** - link ka matičnoj stranici ***AVG bezbednosne trake sa alatkama koja sadrži detaljne informacije o zaštiti koju pruža traka sa alatkama***
- ***Pokreni AVG*** - otvara **AVG Internet Security 2011** ***korisnički interfejs***
- ***AVG info*** - otvara kontekstualni meni sa sledećim vezama ka važnim sigurnosnim informacijama o sledećem**AVG Internet Security 2011**:
    - *O pretnjama* - otvara AVG web lokaciju na strani koja pruža najvažnije podatke o najvećim pretnjama, preporuke za uklanjanje virusa, informacije o ažuriranju AVG, pristup bazama podataka virusa i druge bitne informacije
    - *AVG vesti* – otvaranje Web stranice na kojoj se nalaze najnovija saopštenja za štampu u vezi sa programom AVG
    - *Trenutni nivo pretnje* – otvaranje Web stranice laboratorije virusa sa grafičkim

prikazom trenutnog nivoa pretnje na Webu

- *AVG laboratorija za pretnje* - otvara AVG izveštajeweb lokaciju gde možete potražiti određene pretnje po nazivu i dobiti detaljne informacije o svakoj

- ***Opcije*** - otvaranje dijaloga za konfigurisanje u kojem možete da prilagodite postavke ***AVG bezbednosne trake sa alatkama*** kako bi ona odgovarala vašim potrebama - pogledajte sledeće poglavlje ***Opcije AVG bezbednosne trake sa alatkama***

- ***Izbriši istoriju***- omogućava vam da u okviru ***AVG bezbednosne trake sa alatikama*** izbrišete celokupnu istoriju ili da zasebno izbrišete istoriju pretrage, istoriju pregledača, istoriju preuzimanja datoteka i da izbrišete kolačiće.

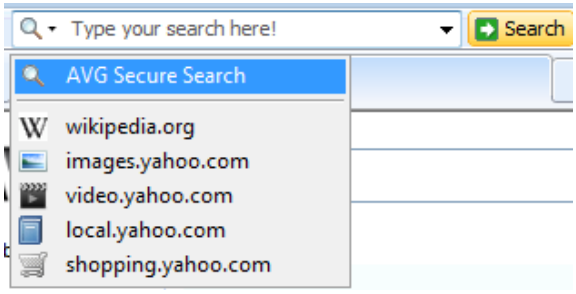
- ***Ažuriranje*** - proveravanje da li postoje novi sadržaji za ažuriranje ***AVG bezbednosne trake sa alatkama***

- ***Pomoć*** - omogućava opcije otvaranja datoteke za pomoć, kontaktiranja AVG tehničke podrške , slanja povratnih informacija u vezi vašeg proizvoda ili prikazivanja detaljnih informacija o verziji trake sa alatima

8.1.2. Polje za pretragu koju pokreće AVG Secure Search (powered by Google)

AVG Secure Search (powered by Google) polje za pretragu je jednostavan i bezbedan način za pretraživanje Weba pomoću pretraživača AVG Secure Search (powered by Google). Unesite reč ili frazu u polje za pretragu, kliknite na dugme ***Pretraži*** ili pritisnite taster ***Enter*** da biste započeli pretragu direktno na AVG Secure Search (powered by Google) serveru, bez obzira na to koja stranica se trenutno prikazuje. U polju za pretragu prikazuje se i vaša istorija pretraživanja. Pretraživanja pomoću polja za pretragu analizira komponenta ***Štit za pretraživanje***.

Umesto toga, u u okviru polja za pretragu možete se prebaciti na Wikipedia ili neki određen servis za pretragu - videti sliku:



8.1.3. Status stranice

Direktno u traci sa alatkama, ovo dugme prikazuje procenu trenutno prikazae web stranice na osnovu kriterijuma komponente ***Štit za pregledanje Interneta*** **:**

- - Stranica na koju veza upućuje je bezbedna

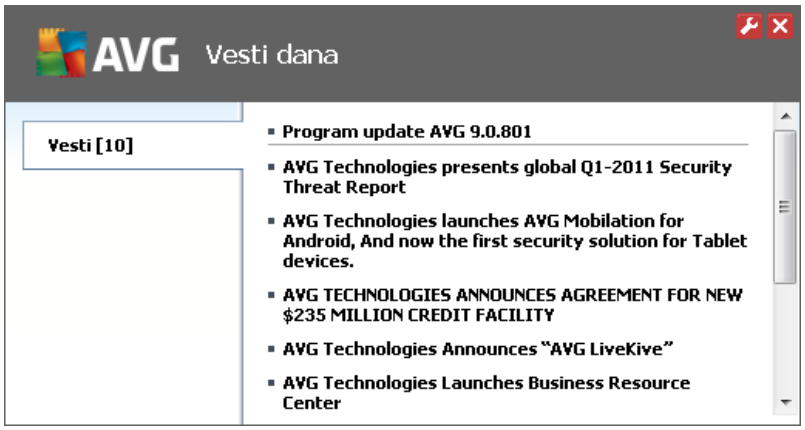
- - Stranica je donekle sumnjiva.

-  - Stranica sadrži veze ka stranicama koje su sigurno opasne.
-  - Stranica na koju veza upućuje sadrži aktivne pretnje! Radi vaše sopstvene bezbednosti, neće vam biti dozvoljeno da posetite ovu stranicu.
-  - Stranici se ne može pristupiti i zato se ne može skenirati.

Kliknite na ovo dugme da biste otvorili informativni prozor u kojem se nalaze detaljni podaci o određenoj Web stranici.

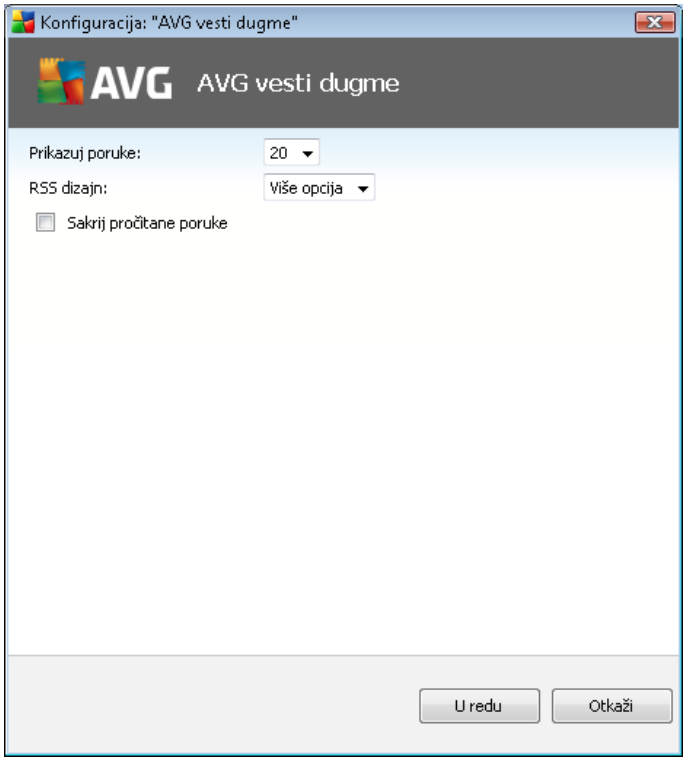
8.1.4. AVG vesti

Direktno iz ***AVG bezbednosne trake sa alatkama***, ovo dugme otvara pregled poslednjih ***udarnih vesti***vezanih za AVG, kako novinskih tako i izdatih od strane kompanije:



U desnom gornjem uglu možete videti dva crvena kontrolna dugmeta:

-  - dugme otvara uređivački dijalog gde možete odrediti parametre***dugmeta za AVG vesti*** prikazanog u okviru***AVG bezbednosne trake sa alatkama***:

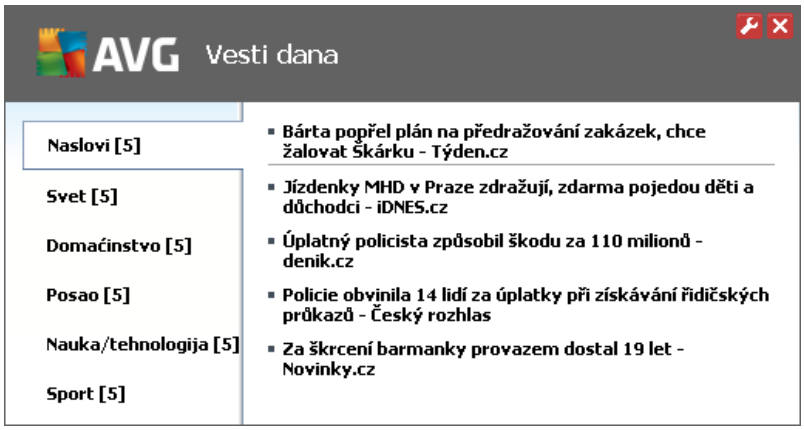


- **_Prikaži poruke_** - menja željeni broj poruka koje će biti prikazane u trenutku
- **_RSS izgled_**- birajte između Naprednog/Osnovnog režima trenutnog prikaza pregleda vesti(*podrazumevano je odabran napredni način - videti sliku iznad*)
- **_Sakrij pročitane poruke_** - označi ovu stavku radi potvrde da se svaka pročitana poruka više ne prikazuje, tako da nove poruke mogu da se dodaju

- - kliknite na ovo dugme da zatvorite trenutno otvoreni pregled vesti

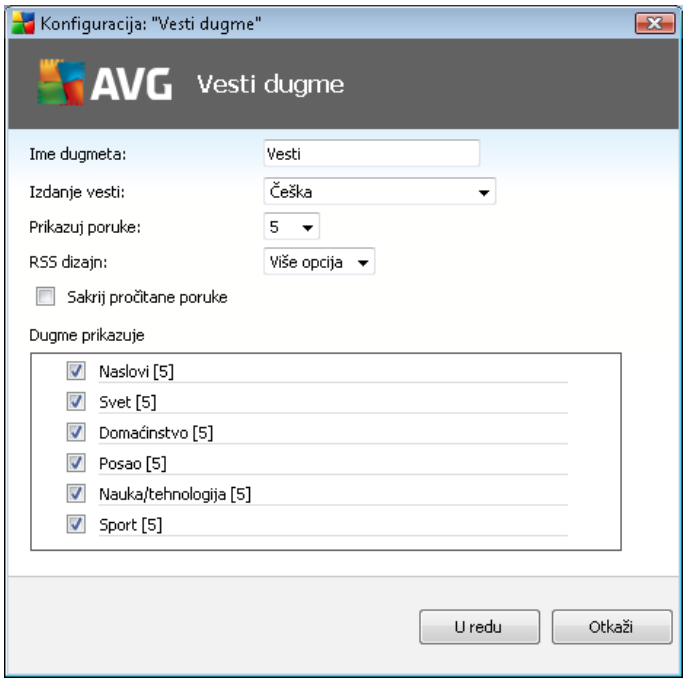
8.1.5. Vesti

Uobičajeno, direktno iz ***AVG bezbednosne trake sa alatima***, ovo dugme otvara pregled najnovijih vesti iz odabranih medija, podeljen u nekoliko odeljaka:



U desnom gornjem uglu možete videti dva crvena kontrolna dugmeta:

- - dugme otvara uređivački dijalog gde možete odrediti parametre***dugmeta za Vesti*** prikazanog u okviru***AVG bezbednosne trake sa alatkama***:



o ***Naziv dugmeta*** - imate opciju promene naziva dugmeta kako je prikazan u okviru ***AVG bezbednosne trake sa alatima***

o ***Izdanje vesti*** - odaberite zemlju sa liste kako biste imali prikazane vesti iz odabranog regiona
o ***Prikaži poruke*** - odredite željeni broj poruka koje će biti prikazane u trenutku
o ***RSS izgled*** - menjajte između Osnovne/Napredne opcije da izaberete izgled pregleda vesti (

napredni izgled je podrazumevano podešen, videti sliku iznad)

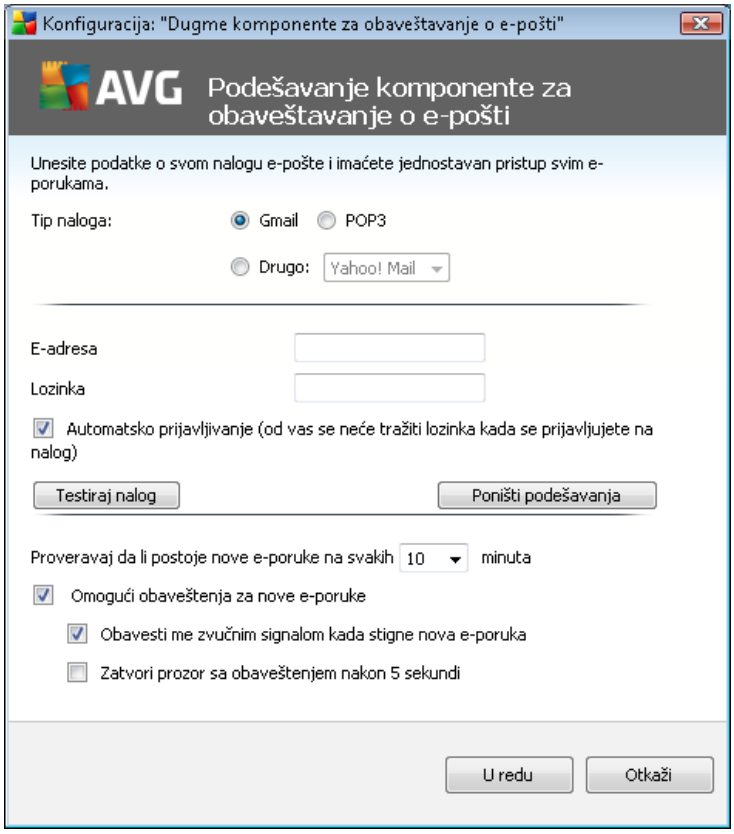
- ***Sakrij pročitane poruke*** - označite ovu stavku da potvrdite da pročitane poruke ne treba da budu i dalje prikazivane u pregledu vesti i da ih treba zameniti sa novim naslovom
- ***Dugme prikazivanja*** - u ovom polju možete dodeliti vrstu vesti koju treba da prikazuje ***AVG bezbednosna traka sa alatkama*** u pregledu vesti
  - - kliknite na ovo dugme da zatvorite trenutno otvoreni pregled vesti

8.1.6. Izbriši istoriju

Korišćenjem ovog dugmeta možete obrisati istoriju vašeg web pregledača baš kao putem opcije***AVG logotip -> Izbriši istoriju*** .

8.1.7. Komponenta za obaveštavanje o e-pošti

Dugme ***Komponenta za obaveštavanje o e-pošti***vam omogućava da aktivirate opciju kojom ćete biti obaveštavani o novim pristiglim porukama e-pošte direktno u interfejsu ***AVG bezbednosne trake sa alatkama*** . Dugme otvara sledeći uređivački dijalog u kome možete definisati parametre vašeg naloga za e-poštu i pravila za prikazivanje e-pošte. Molimo vas da sledite uputstva u dijalogu:



- ***Tip naloga*** - Označava tip protokola koji vaš nalog za e-poštu koristi. Možete birati između sledećih mogućnosti: *Gmail*, *POP3* ili odabrati naziv servera iz padajućeg menija u okviru stavke *Ostali* (*trenutno, možete koristiti ovu opciju ako je vaš nalog na Yahoo! JP ili Hotmail pošti*). Ukoliko niste sigurni koji tip servera za e-poštu vaš nalog koristi, pokušajte da dobijete tu informaciju od vašeg provajdera za e-poštu ili vašeg provajdera internet usluga.

- ***Prijavljivanje*** – u odeljku ispod unesite tačnu *adresu e-pošte* i odgovarajuću *lozinku*. Zadržite opciju*Auto prijavljivanje* označenom da ne biste morali da popunjavate podatke iznova.

- ***Testiraj nalog*** – koristite ovo dugme da biste testirali unete informacije.

- ***Poništi podešavanja*** – brzo uklanja gorenavedenu adresu e-pošte.

- ***Proveri ima li novih poruka svakih ... minuta*** - Definišite vremenski interval koji će se koristiti za proveru novih poruka e-pošte (*u opsegu od 5-120 minuta*) i označite da li i kako želite da budete obavešteni o pristizanju nove poruke.

- ***Omogući obaveštenja za nove e-poruke*** – opozovite izbor u ovom polju za potvrdu da biste onemogućili vizuelna obaveštenja o prispeću novih e-poruka.

    - ***Obavesti me zvučnim signalom kada stigne nova e-poruka*** – opozovite izbor u ovom polju za potvrdu da biste onemogućili zvučna obaveštenja o prispeću novih e-poruka.

    - ***Zatvori prozor sa obaveštenjem nakon 5 sekundi*** – označite izbor u ovom polju za potvrdu ako želite da se prozor sa vizuelnim obaveštenjem o prispeću novih e-poruka automatski zatvori nakon 5 sekundi.

8.1.8. Informacija o vremenu

Dugme ***Vreme*** prikazuje informaciju o trenutnoj temperaturi (*koja se ažurira se svakih 3-6 sati*) na destinaciji koju ste odabrali direktno iz interfejsa ***AVG bezbednosne trake sa alatima***. Kliknite na dugme da otvorite novi inormacioni panel sa detaljnim vremenskim pregledom:

Zatim nađite uređivačke opcije:

- ***Promeni lokaciju*** - kliknite na tekst***Promeni lokaciju*** da bi se prikazao novi dijalog nazvan ***Potraži svoju lokaciju***. Unesite naziv željene lokacije u tekstualno polje i potvrdite

klikom na ***Traži*** dugme. Zatim, u okviru liste svih lokacija istog naziva odaberite destinaciju koju ste tražili. Konačno, informacioni panel će se prikazati ponovo pružajući informacije o vremenu za odabranu lokaciju.

- ***Konverter Farenhajt / Celzijus*** - u gornjem desnom uglu informacionog panela možete birati između Farenhajtove i Celzijusove skale. Zavisno od vašeg izbora, informacija o temperaturi će nadalje biti prikazivana u odabranoj skali.

- ***Puna prognoza*** – ako ste zainteresovani za punu i detaljnu prognozu, koristite vezu ***Puna prognoza*** da biste došli do specijalizovane Web lokacije za vremensku prognozu.

8.1.9. Facebook

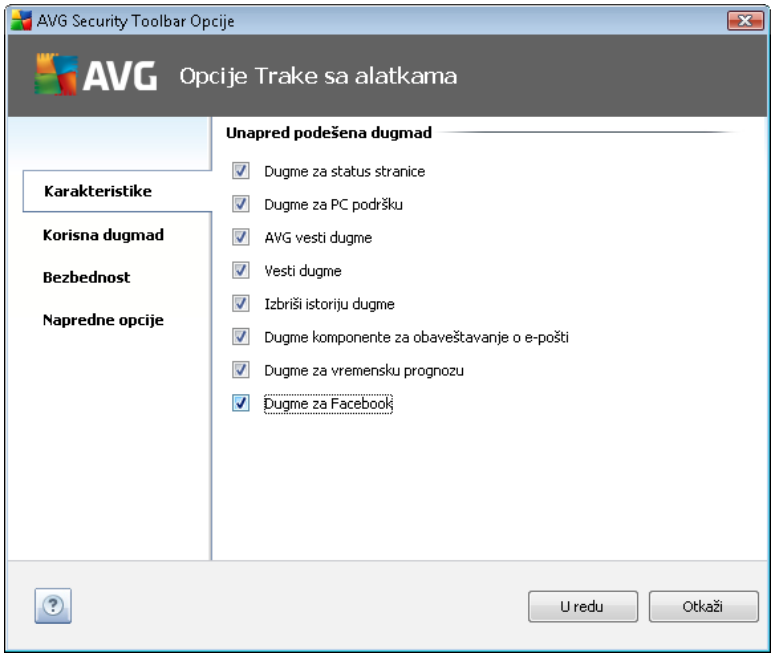
Dugme ***Facebook*** omogućava vam da se direktno povežete sa društvenom mrežom Facebook iz ***AVG bezbednosne trake sa alatkama*** . Kliknite na dugme i pojaviće se poziv za prijavljivanje; kliknite ponovo da otvorite ***dijalog za prijavljivanje na Facebook*** . Unesite vaše pristupne podatke i pritisnite dugme ***Poveži*** . Ukoliko još uvek nemate Facebooknalog, možete da otvorite jedan direktnim korišćenjem veze***Prijavi se za Facebook*** .

Nakon što ste obavili proces registracije za Facebook, bićete pozvani da omogućite aplikaciju ***AVG društveno proširenje***. Funkcionalnost ove aplikacije je suštinska za vezu traka sa alatkama - Facebook, stoga je preporučljivo da se dozvoli njen rad, pa se uverite da je omogućen. Zatim, Facebook veza će se aktivirati i dugme ***Facebook*** u okviru ***AVG bezbednosne trake sa alatkama*** će sada ponuditi standardne opcije Facebook menija.

8.2. Opcije AVG bezbednosne trake sa alatkama

Svim parametrima za podešavanje ***AVG bezbednosne trake sa alatkama*** možete da pristupite direktno iz okna ***AVG bezbednosne trake sa alatkama***. Interfejs za uređivanje se otvara putem menija *AVG / Opcije* na traci sa alatkama kao novi dijalog ***Opcije trake sa alatkama*** koji je podeljen na četiri dela:

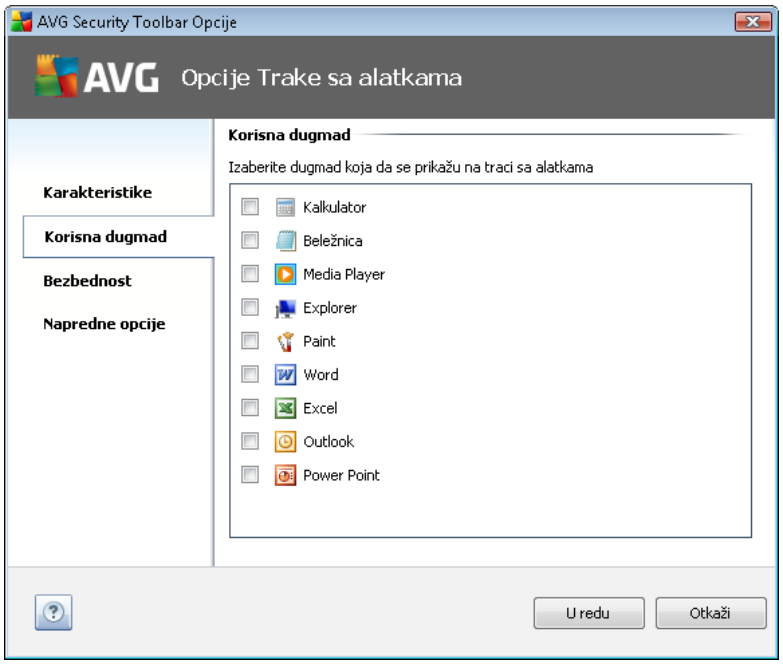
8.2.1. Kartica „Opšte"



Na ovoj kartici možete da odredite koja će se kontrolna dugmad trake sa alatkama prikazivati ili ne na ***AVG bezbednosnoj traci sa alatkama*** . Izaberite odgovarajuću opciju ako želite da prikažete neko dugme. U nastavku je naveden opis funkcije svakog dugmeta na traci sa alatkama:

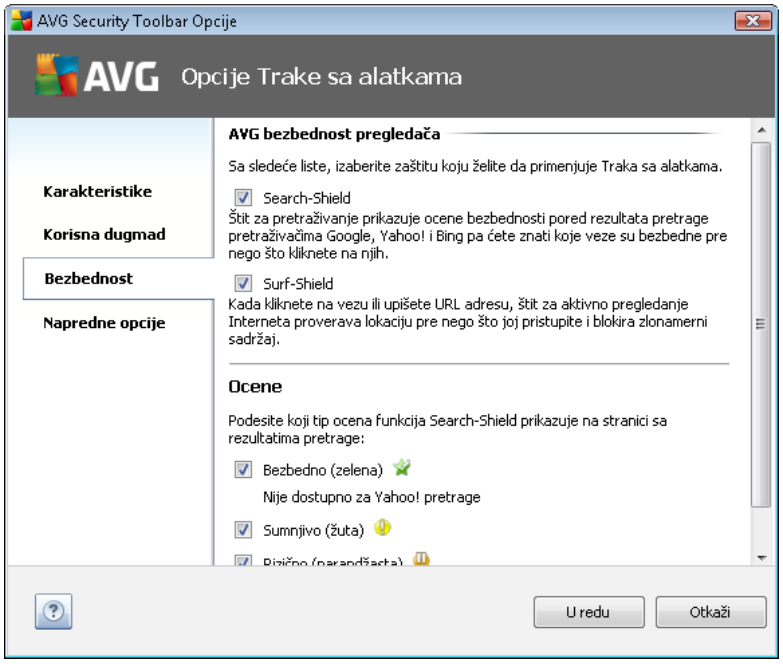
- ***Dugme za status stranice -*** dugme nudi mogućnost prikazivanja informacije o bezbednosnom statusu trenutno otvorene stranice u okviru ***AVG bezbednosne trake sa alatima***
- Δυγμε ***AVG vesti*** - ovo dugme otvara Web stranicu na kojoj se nalaze najnovija sopštenja za štampu u vezi sa programom AVG
- Δυγμε ***Vesti*** - kada kliknete na ovo dugme, prikazuje se strukturalni pregled aktuelnih vesti iz dnevne štampe
- ***Dugme „Izbriši istoriju"*** - ovo dugme vam omogućava da izbrišete celu istoriju, ili da izbrišete istoriju pretrage, istoriju pregledača, istoriju preuzimanjaili da izbrišete kolačiće direktno iz okna AVG bezbednosne trake sa alatkama
- ***Dugme za obaveštavanje o e-pošti***- dugme dozvoljava da budu prikazane vaše nove pristigle poruke e-pošte u okviru interfejsa ***AVG bezbednosne trake sa alatkama***
- ***Dugme vremenske prognoze*** - dugme nudi momentalnu informaciju o vremenskim uslovima u odabranom području
- ***Facebook dugme*** - dugme nudi direktnu vezu sa Facebook društvenu mrežu

8.2.2. Kartica „Korisna dugmad"



Kartica ***Korisna dugmad*** vam omogućava da sa liste izaberete aplikacije i da njihove ikone prikažete u interfejsu trake sa alatkama. Ikona služi kao brzi link i omogućava vam da odmah pokrenete odgovarajuću aplikaciju.

8.2.3. Kartica „Bezbednost"



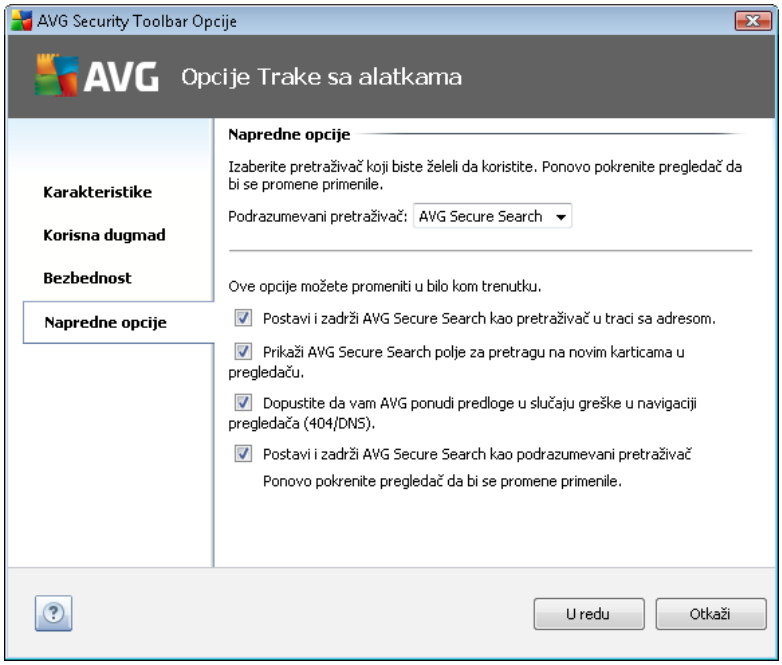
Kartica ***Bezbednost*** podeljena je na dva dela, ***AVG bezbednost pregledača*** i ***Ocene***, i omogućava

vam da potvrdite izbor u odgovarajućim poljima za potvrdu kako biste ***AVG bezbednosnoj traci sa alatkama*** dodelili željenu funkciju:

- ***AVG bezbednost pregledača*** - izaberite ovu opciju kako biste aktivirali ili isključili ***AVG štit za pretraživanje*** i/ili uslugu ***Štit za pregledanje Interneta***
- ***Ocene*** - izaberite željene grafičke simbole koje će za ocenjivanje rezultata pretrage koristiti komponenta ***štit za pretraživanje***
  - o stranica je bezbedna
  - o stranica je donekle sumnjiva
  - o stranica sadrži linkove ka stranicama koje su sigurno opasne
  - o stranica sadrži aktivne pretnje
  - o stranici se ne može pristupiti i zato se ne može skenirati

Označite odgovarajuću opciju kako biste potvrdili da želite da budete obaveštavani o ovom određenom nivou pretnje. Međutim, prikazivanje crvenog znaka na stranicama koje sadrže aktivne i opasne pretnje nije moguće isključiti. ***Preporučuje se da ne menjate podrazumevanu konfiguraciju koju je podesio prodavac programa osim ako nemate dobar razlog za to.***

8.2.4. Kartica „Napredne opcije"



Na kartici ***Napredne opcije*** najpre izaberite pretraživač koji želite da se podrazumevano koristi. Možete da izaberete *AVG Secure Search (powered by Google), Baidu, WebHledani*, *Yandex i Yahoo! JP*. Kada izaberete podrazumevani pretraživač, ponovo pokrenite Internet pregledač kako bi promena stupila na snagu.

Osim toga, možete aktivirati ili isključiti određene postavke***AVG bezbednosne trake sa alatkama*** *(navedeno poglavlje se odnosi na podrazumevane AVG Secure Search (powered by Google) postavke)*:

- ***Postavi i zadrži AVG Secure Search (powered by Google) kao pretraživač u traci za adresu*** – ako je označena, ova opcija vam omogućava da unesete ključnu reč direktno u traku za adresu u Web pregledaču, a usluga Google će se koristiti automatski za pronalaženje relevantnih Web lokacija.

- ***Neka AVG daje predloge u slučaju greške u navigaciji pregledača (404/DNS)*** - ako prilikom pretraživanja weba naiđete na stranicu koja ne postoji ili stranicu koja se ne može prikazati (greška 404), bićete automatski preusmereni na Web stranicu na kojoj ćete moći da izaberete alternativne stranice sa sličnom temom.

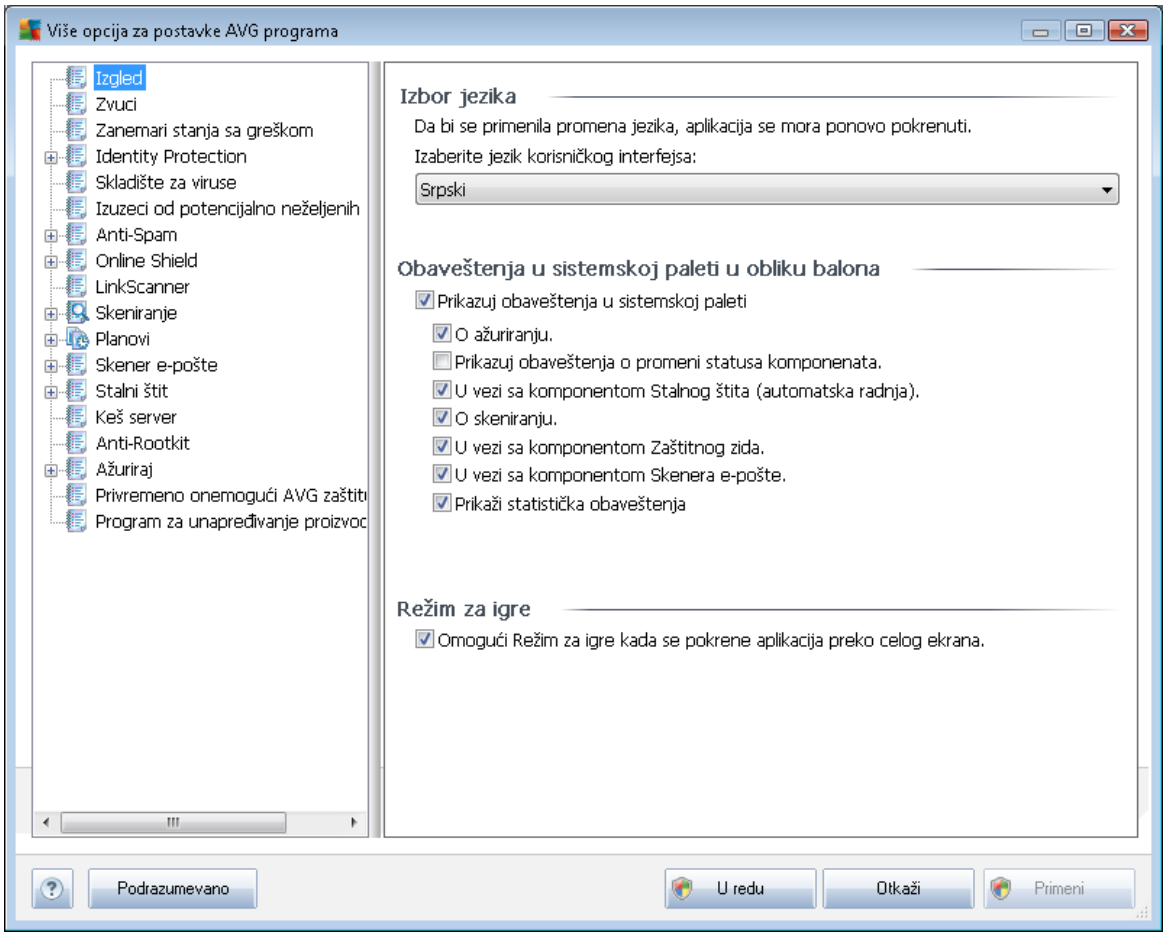
- ***Postavi i zadrži AVG Secure Search (powered by Google) kao podrazumevani pretraživač*** – Google je podrazumevani pretraživač za pretragu Weba u okviru ***AVG bezbednosne trake sa alatkama***, a aktiviranjem ove opcije takođe može postati podrazumevani pretraživač u vašem pregledaču.

9. AVG napredna podešavanja

Dijalog za napredna podešavanja programa **AVG Internet Security 2011** 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.

9.1. Izgled

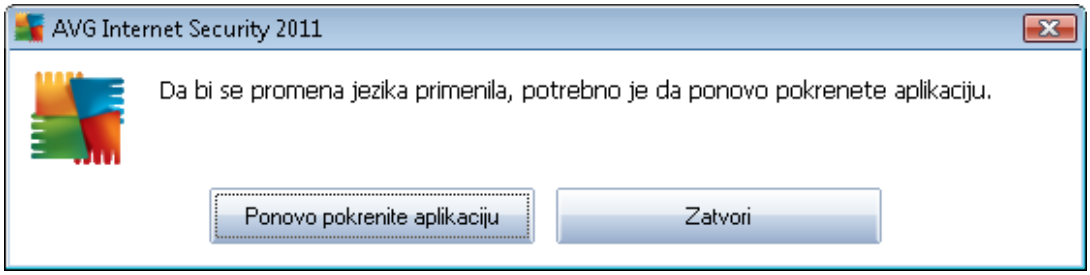
Prva stavka navigacionog stabla, ***Izgled***, odnosi se na opšta podešavanja AVG korisničkog interfejsa , kao i nekoliko osnovnih opcija ponašanja aplikacije:



Izbor jezika

U odeljku ***Izbor jezika***, možete izabrati željeni jezik sa padajućeg menija; izabrani jezik će se koristiti za čitavi AVG korisnički interfejs. Padajući meni nudi samo one jezike koje ste prethodno odabrali da budu instalirani tokom procesa instalacije (*videti poglavljeOpcija prilagođavanja*) plus engleski (*koji se instalira podrazumevano*). Međutim, da biste završili prebacivanje aplikacije na drugi jezik, potrebno je da ponovo pokrenete korisnički interfejs; pratite sledeće korake:

- Izaberite željeni jezik za aplikaciju i potvrdite izbor pritiskom na dugme ***Primeni*** (u donjem desnom uglu)
- Kliknite na dugme ***U redu*** da biste potvrdili
- Pojaviće se novi dijalog koji vas obaveštava da promena jezika AVG korisničkog interfejsa zahteva ponovno pokretanje aplikacije:



Obaveštenja u sistemskoj paleti u obliku balona

U ovom odeljku možete izabrati da se ne prikazuju obaveštenja u sistemskoj paleti u obliku balona koja vas informišu o statusu aplikacije. Obaveštenja u obliku balona se podrazumevano prikazuju i preporučuje se da ostavite ovu konfiguraciju! Obaveštenja u obliku balona obično vas informišu o promeni statusa neke AVG komponente, na šta je potrebno da obratite pažnju!

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 AVG komponentu), možete definisati i navesti željene opcije tako što ćete označiti/poništiti izbor sledećih opcija:

- ***Prikazuj obaveštenja u sistemskoj paleti*** - podrazumevano, ova stavka je izabrana (*uključena*), pa se obaveštenja prikazuju. Opozovite izbor ove stavke da biste potpuno isključili sva obaveštenja u obliku balona. Ako je ova stavka uključena, možete dodatno definisati koja će se obaveštenja prikazivati:
    - ***Prikazuj obaveštenja u sistemskoj paleti o ažuriranju programa*** - odlučite da li će se prikazivati informacije o pokretanju, toku i završetku ažuriranja programa AVG;
    - ***Prikazuj obaveštenja o promeni statusa komponenata*** - odlučite da li će se prikazivati informacije o aktivnosti/neaktivnosti komponenata ili potencijalnim problemima u okviru komponente. Prilikom prijavljivanja stanja greške komponente, ova opcija je jednaka informativnoj funkciji ikone sistemske palete (promeni boje) koja prijavljuje probleme u AVG komponentama;
    - ***Prikazuj obaveštenja vezana zaStalni štit u sistemskoj traci (automatska radnja)*** - izaberite da li da informacija u vezi procesa čuvanja, kopiranja i otvaranja datoteka bude prikazana ili ne (*ova konfiguracija samo pokazuje da li je opcija Stalnog štita Automatsko lečenje uključena*);
    - ***Prikazuj obaveštenja u sistemskoj paleti o skeniranju*** - odlučite da li će se prikazivati informacije o automatskom pokretanju planiranog skeniranja, njegovom

toku i rezultatima;

- ***Prikazuj obaveštenja u sistemskoj paleti u vezi sa zaštitnim zidom*** - odlučite da li će se obaveštenja u vezi sa statusom i procesima zaštitnog zida, npr. upozorenja o aktiviranju/deaktiviranju ove komponente, mogućem blokiranju saobraćaja itd. prikazivati ili ne;

- ***Prikazuj obaveštenja u sistemskoj paleti u vezi sa komponentom Skener e-pošte*** - odlučite da li će se prikazivati informacije o skeniranju sve dolazne i odlazne pošte.

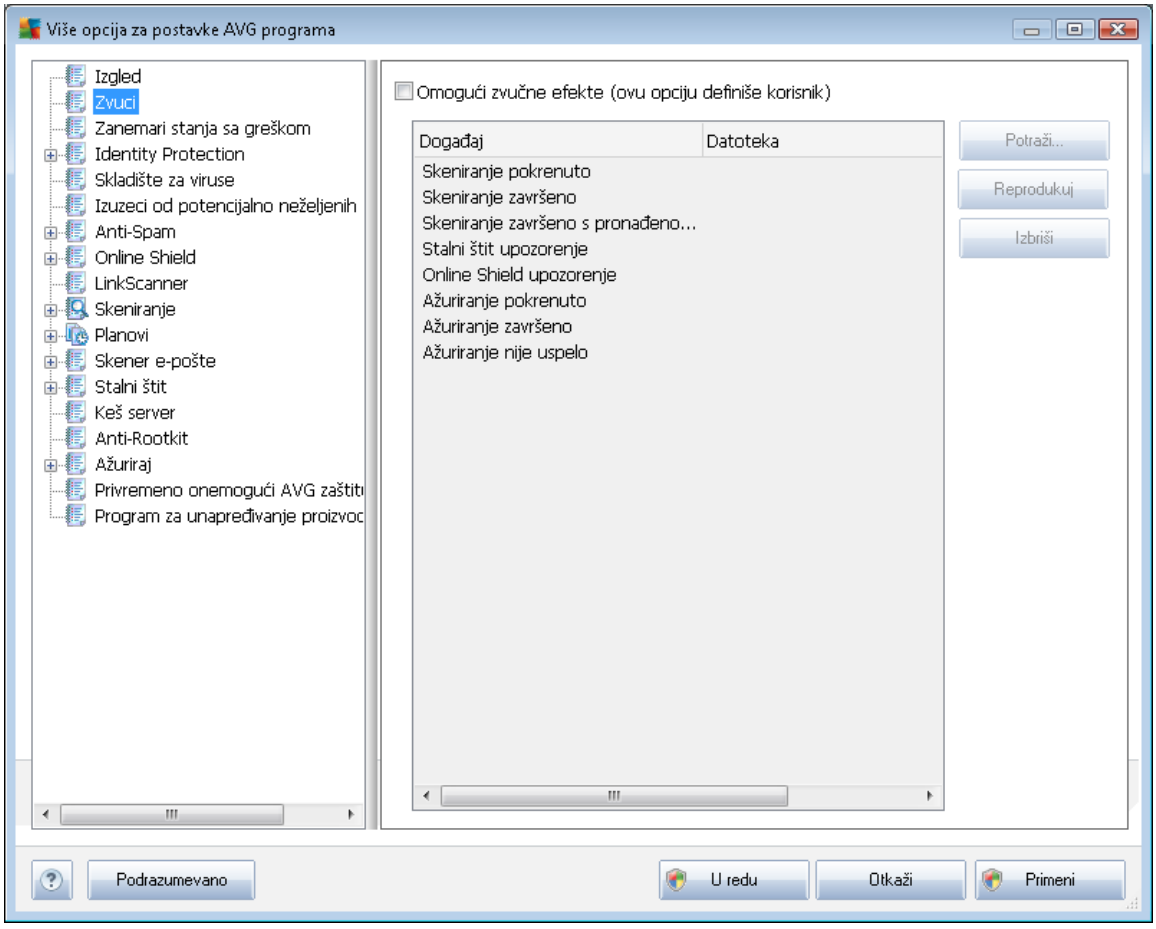
- ***Prikaži statistička obaveštenja*** – ne opozivajte izbor ove opcije ako želite da se na sistemskoj paleti redovno prikazuju statistička obaveštenja.

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 ***Omogući režim za igre kada se prikazuje sadržaj preko celog ekrana*** (*podrazumevana postavka*).

9.2. Zvuci

U dijalogu ***Zvukovi*** možete izabrati da li želite da budete obaveštavani o određenim AVG radnjama putem zvučnog obaveštenja. Ako želite, izaberite opciju ***Omogući zvučne efekte*** (*podrazumevano je isključena*) da biste aktivirali listu AVG radnji:

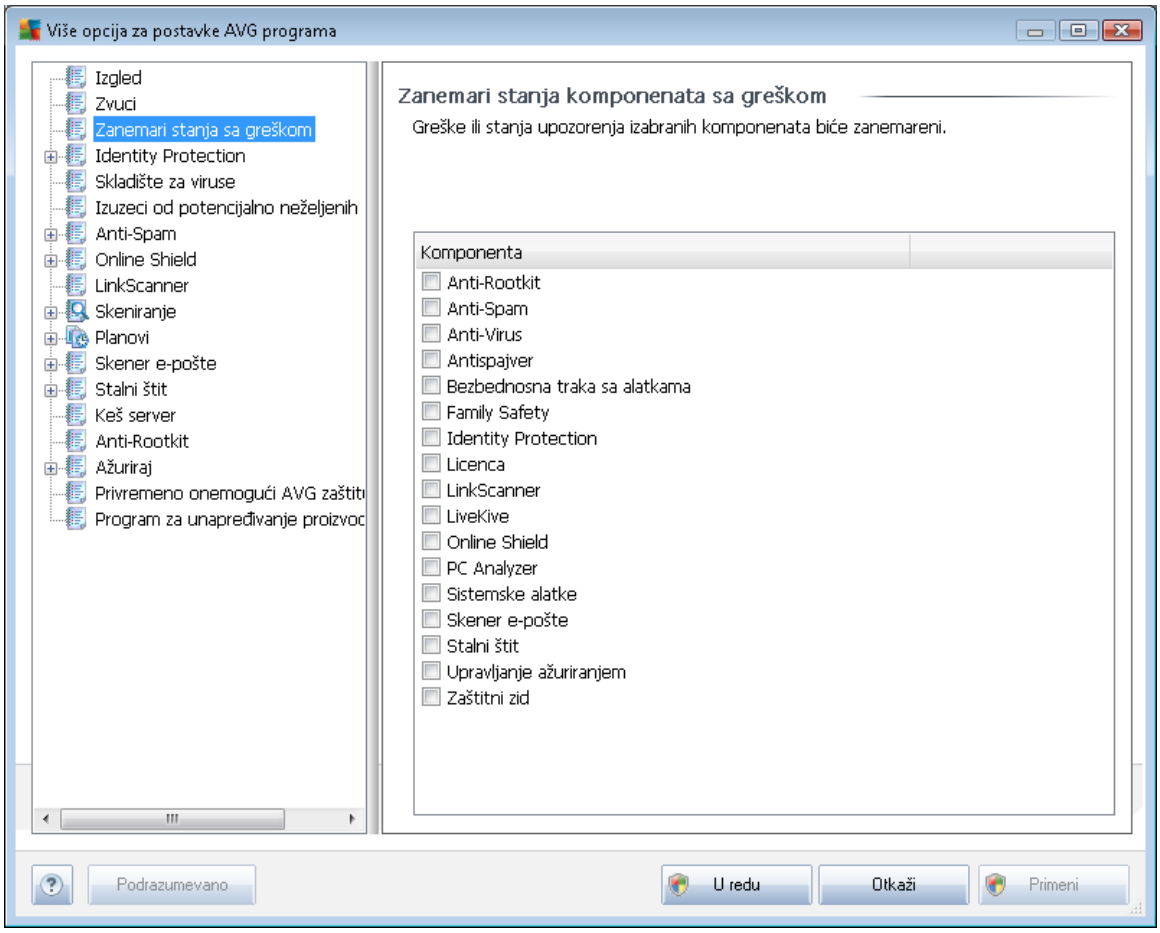


Potom sa liste izaberite odgovarajući događaj i pronađite (***Potraži***) na disku odgovarajući zvuk koji želite da dodelite ovom događaju. Da biste poslušali izabrani zvuk, označite događaj na listi događaja i kliknite na dugme ***Reprodukuj*** . Kliknite na dugme ***Izbriši*** da biste uklonili zvuk dodeljen određenom događaju.

Napomena: *podržani su samo zvukovi u *.wav formatu!*

9.3. Zanemarivanje stanja sa greškom

U dijalogu ***Zanemari stanje komponenti sa greškom*** možete izabrati one komponente za koje ne želite da dobijate obaveštenja:



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

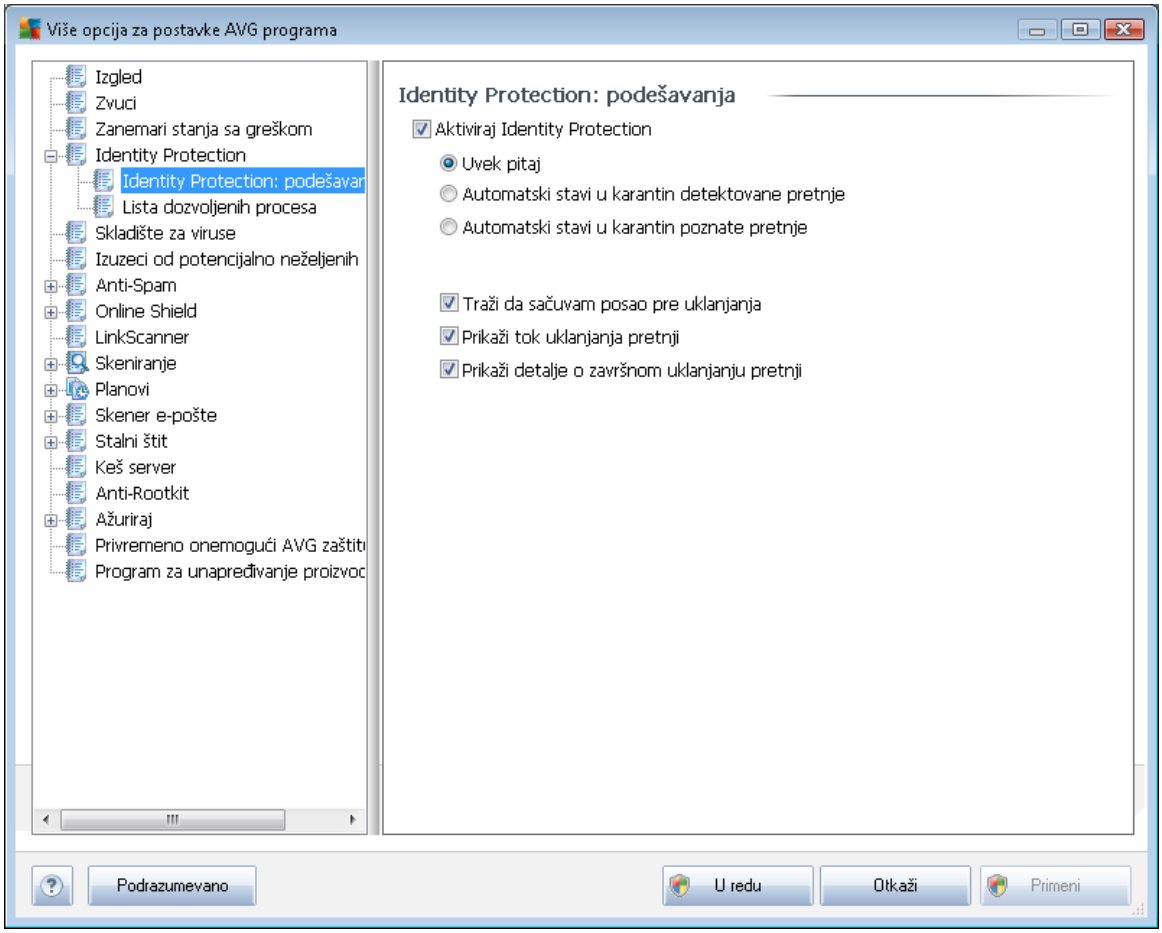
Možda će biti potrebno da u nekoj situaciji iz nekog razloga privremeno isključite komponentu (*to se ne preporučuje, trebalo bi da sve komponente stalno budu uključene i u podrazumevanoj konfiguraciji, ali postoji mogućnost da ih isključite*). U tom slučaju, ikona na sistemskoj paleti vas automatski 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 za ***zanemarivanje stanja komponente*** je takođe dostupna za određene komponente direktno iz pregleda komponente u glavnom prozoru programa AVG.

9.4. Identity Protection

9.4.1. Postavke zaštite identiteta

Dijalog ***Postavke zaštite identiteta***vam omogućava da uključite/isključite osnovne funkcije komponente ***Zaštita identiteta***:



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 ***Zaštita identiteta*** 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 ***AVG 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 potvdu ako želite da se sve aplikacije koje su detektovane kao potencijalni malver automatski smeštaju u ***AVG skladište za viruse***.

Osim toga, možete da izaberete i dodatne stavke kako biste opcionalno aktivirali još funkcija komponente ***Zaštita identiteta***:

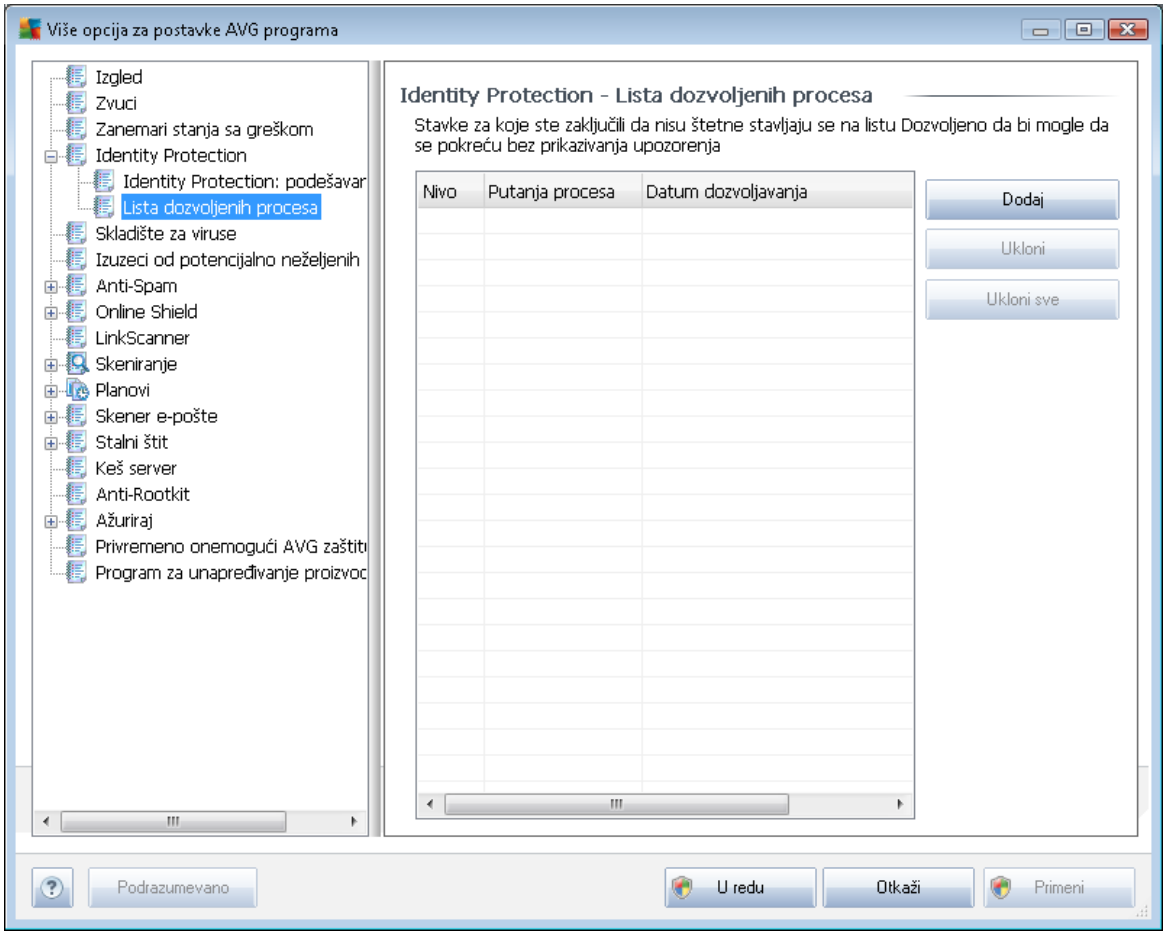
- ***Pitaj da sačuvaš svoj rad pre nego što se ukloni*** - (*podrazumevano je isključeno*) - ne opozivajte izbor u ovom polju za potvrdu ako želite da budete upozoreni pre nego što se aplikacija detektovana kao potencijalni malver stavi u karantin. Ukoliko radite samo sa aplikacijom, vaš projekat će 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 malvera*** - (*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 malvera*** - (*podrazumevano je uključeno*) - ako je ova stavka uključena, komponenta ***Zaštita identiteta*** će prikazivati detaljne informacije o svakom objektu stavljenom u karantin (*nivo ozbiljnosti, lokacija itd.*).

9.4.2. 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. Onda u tom slučaju označite sumnjivu aplikaciju (*otkrivenom kao bezbedna na osnovu njenog ponašanja*) i potvrdite da je treba zadržati na računaru, aplikacija će biti dodata na takozvanu listu ***Dozvoljena zaštita identiteta*** i više se neće prijavljivati kao potencijalno opasna:



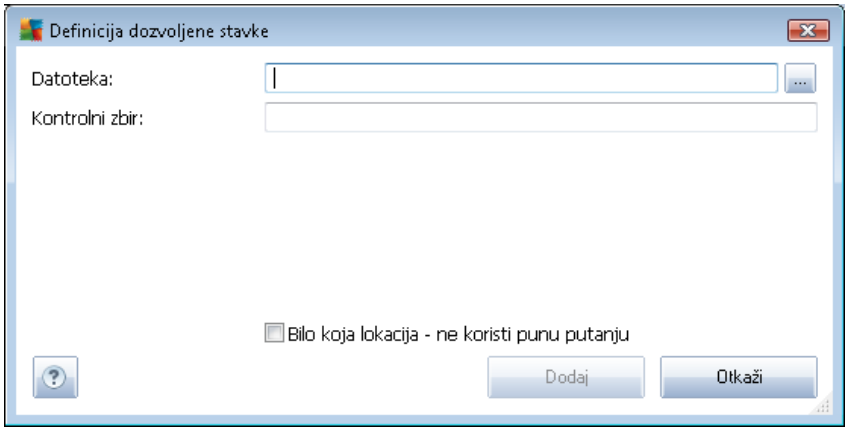
Lista ***Dozvoljena zaštita identiteta*** pruža sledeće informacije o svakoj aplikaciji:

- ***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 ***Zaštita identiteta - Lista dozvoljenih procesa***nalaze se sledeća kontrolna dugmad:

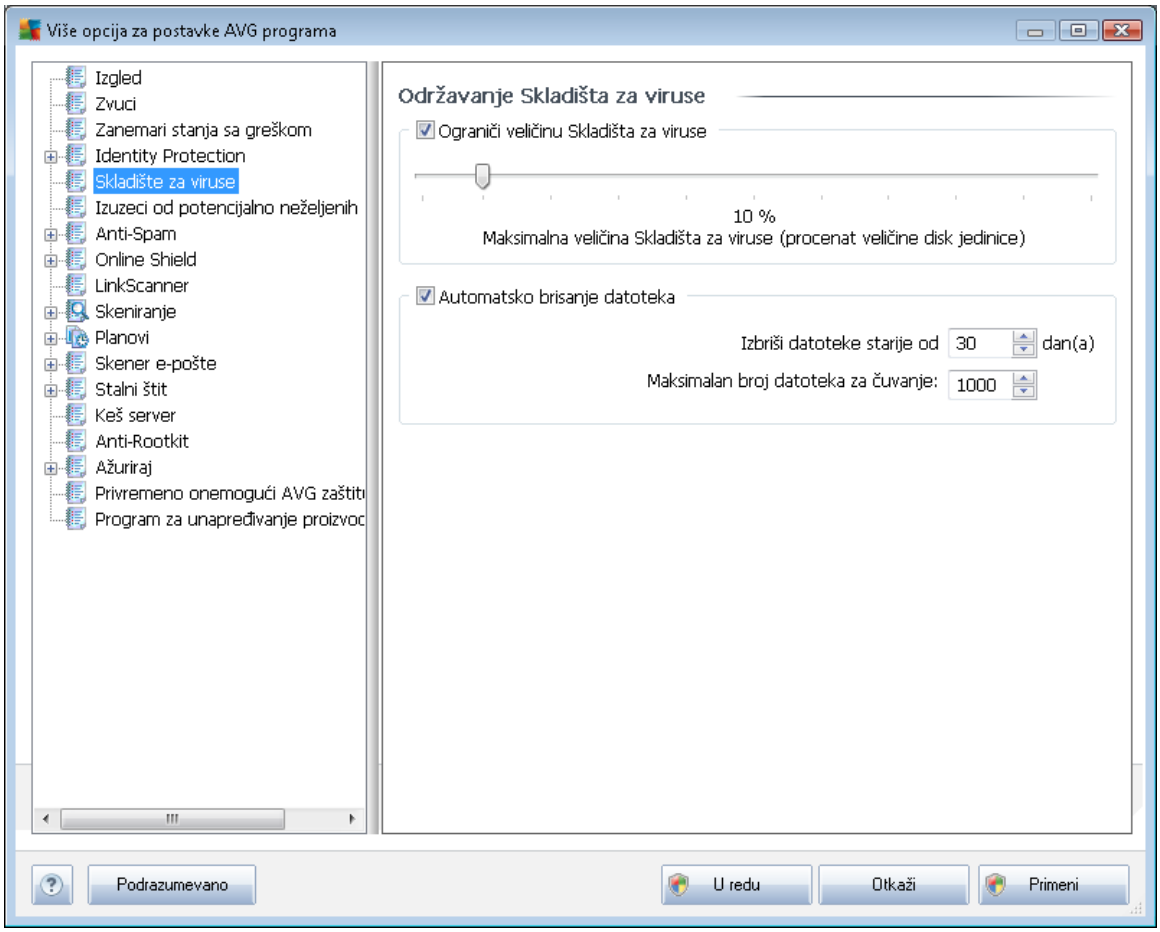
- ***Dodaj*** - kliknite na ovo dugme da biste dodali novu aplikaciju na listu dozvoljenih aplikacija. Pojaviće se sledeći dijalog:



- o ***Datoteka*** - upišite punu putanju do datoteke (*aplikacije*) koju želite da označite kao izuzetak
- o ***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.
- o 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

9.5. Skladište za viruse

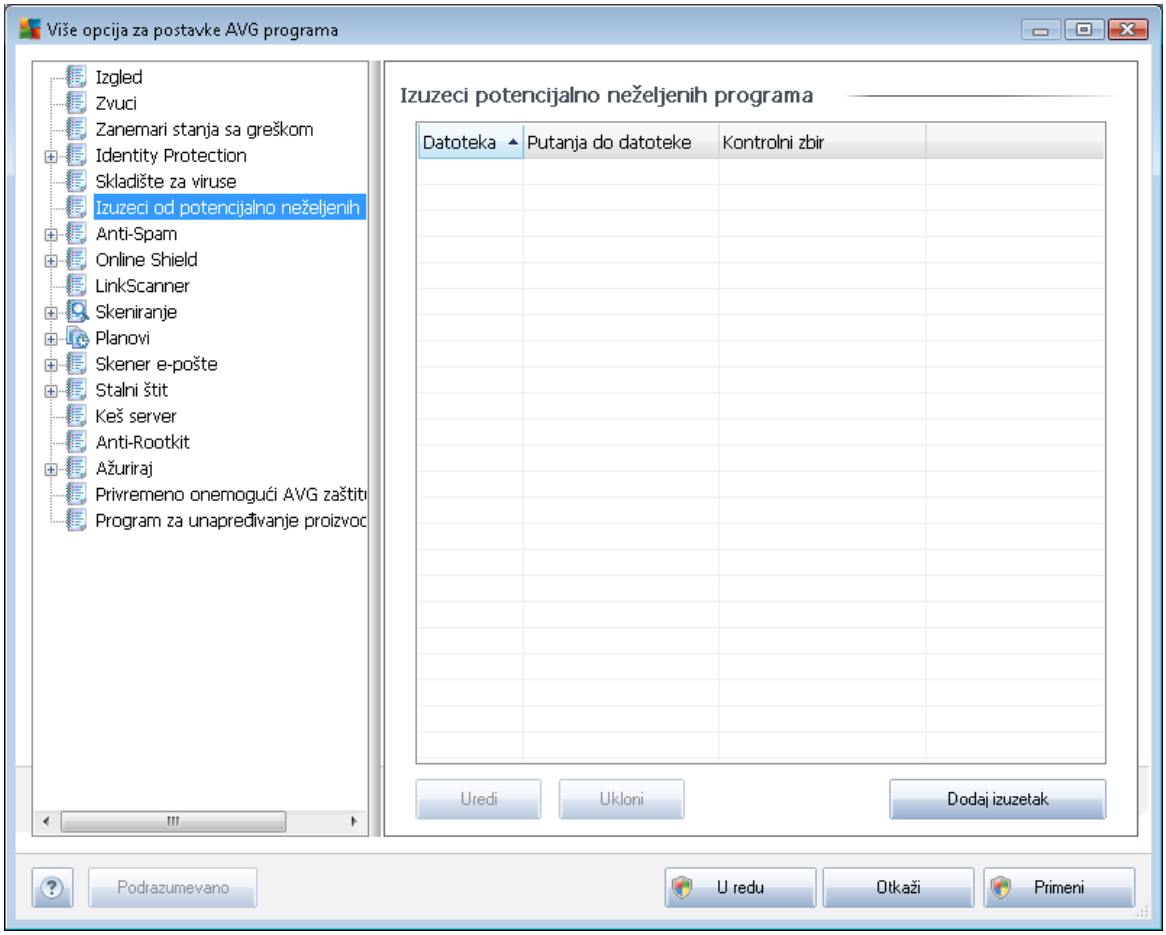


U dijalogu ***Održavanje Skladišta za viruse*** možete definisati nekoliko parametara u vezi sa administracijom objekata koji se čuvaju u ***Skladištu za viruse***:

- ***Ograniči veličinu skladišta za viruse*** - pomoću klizača podesite maksimalnu veličinu ***skladišta za viruse***. Veličina se definiše kao procenat veličine lokalnog diska.
- ***Automatsko brisanje datoteka*** - u ovom odeljku možete definisati maksimalni vremenski interval za čuvanje objekata u ***Skladištu za viruse*** (***Izbriši datoteke starije od ... dana***), kao i maksimalni broj datoteka za čuvanje u ***Skladištu za viruse***(***Maksimalni broj datoteka za čuvanje***)

9.6. Izuzeci od potencijalno neželjenih programa

AVG Internet Security 2011 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 želeti da zadrži određene neželjene programe na računaru (*programe koji su namerno instalirani*). Neki programi, naročito oni besplatni, sadrže adver. AVG može da otkrije taj adver i da o njemu izvesti kao o ***Potencijalno neželjenom programu***. Ako takav program želite da zadržite na računaru, možete da ga definišete kao Izuzetak potencijalno neželjenih programa:



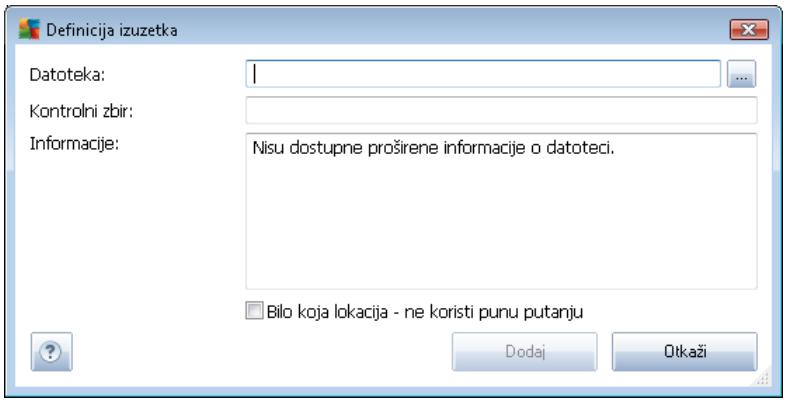
U dijalogu ***Izuzeci potencijalno neželjenih programa*** nalazi se lista već definisanih i važećih izuzetaka potencijalno neželjenih programa. Listu možete da uredite, kao i da izbrišete postojeće stavke ili da dodate nove izuzetke. Na listi se mogu naći sledeće informacije o svakom izuzetku:

- ***Datoteka*** - pruža 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

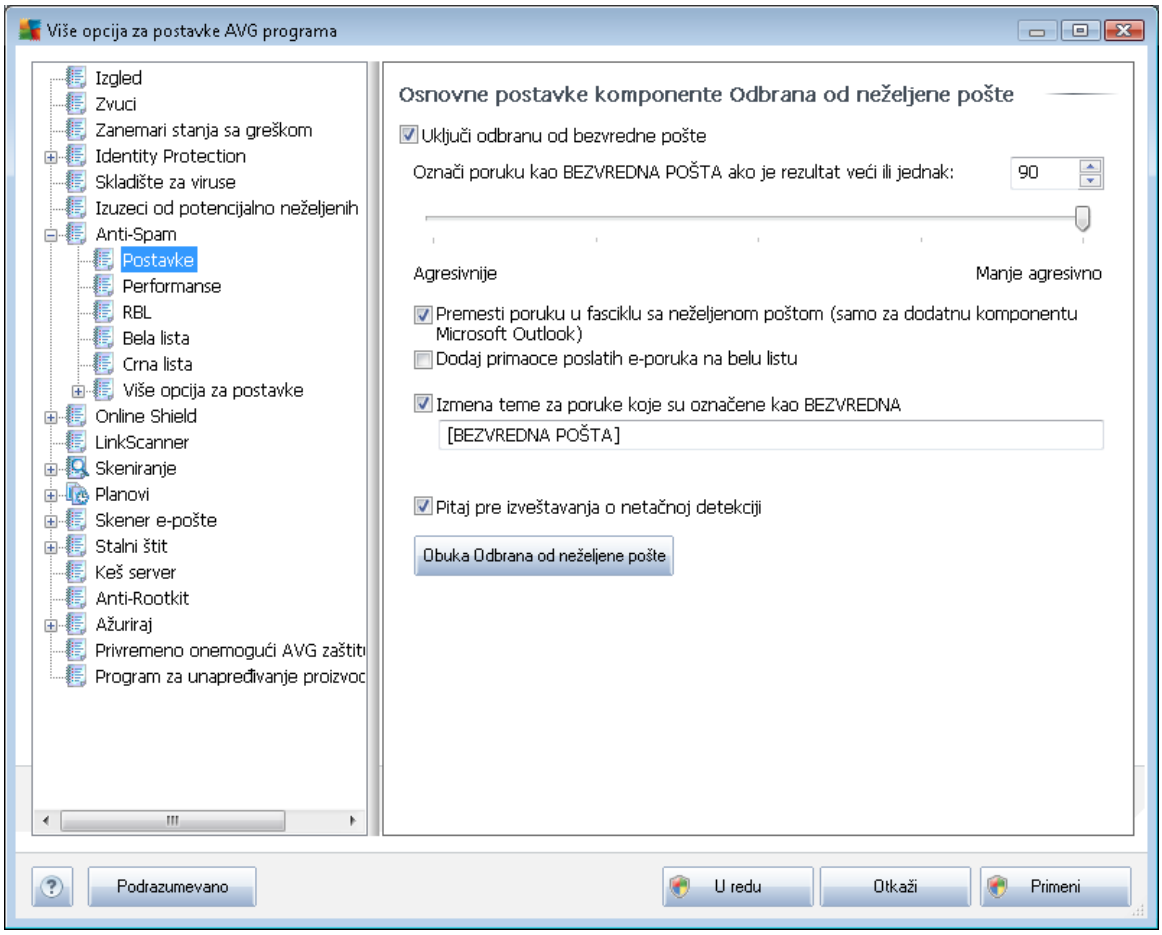
- ***Dodaj izuzetak*** – otvaranje dijaloga za uređivanje u kojem možete definisati parametre novog izuzetka koji će biti kreiran:



  - ***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*** - prikazivanje postojećih dodatnih informacija o izabranoj datoteci (*informacije o licenci/verziji itd.*)
  - ***Bilo koja lokacija - ne koristi punu putanju*** - ako želite da ovu datoteku definište kao izuzetak samo na određenoj lokaciji, ostavite ovo polje neoznačeno.Ukoliko je polje označeno, određena datoteka je definisana kao izuzetak bez obzira gde je locirana (*međutim, svakako morate da unesete punu putanju do te datoteke; datoteka će tada biti korišćena kao jedinstven primer za mogućnost da se dve datoteke istog imena pojavljuju u vašem sistemu*).

9.7. Odbrana od bezvredne pošte

9.7.1. Postavke



U dijalogu ***Osnovne postavke odbrane od neželjene pošte*** možete da potvrdite/opozovete izbor u polju za potvrdu ***Uključi zaštitu od neželjene pošte*** da biste dozvolili/zabranili skeniranje e-pošte u potrazi za neželjenom 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 neželjene 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 neželjene biće filtrirane. Postoji mogućnost da budu filtrirane i poruke koje nisu bezvredne (neželjene).

- ***Vrednost 50-59*** - veoma agresivna konfiguracija. Jednako je verovatno da će biti obuhvaćene i e-poruke koje nisu bezvredne, kao i prave neželjene poruke. Ovaj granični opseg se ne preporučuje za uobičajenu upotrebu.

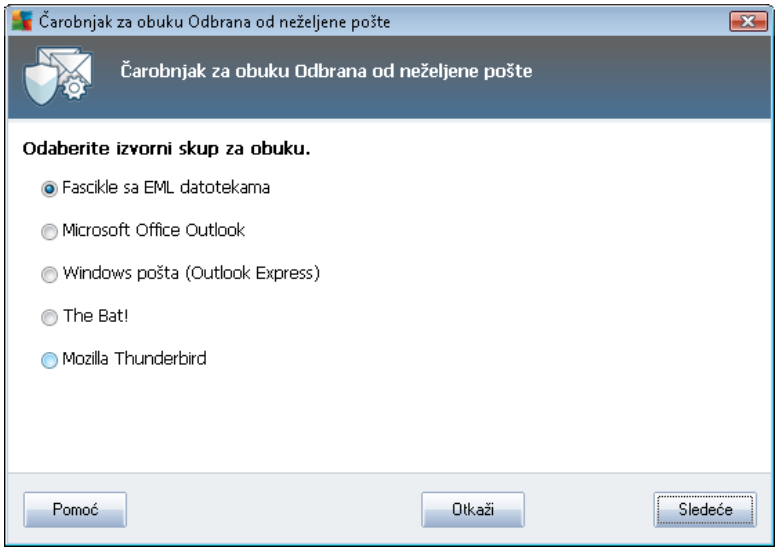
U dijalogu ***Osnovne postavke odbrane od neželjene pošte*** možete definisati i kako će se postupati sa otkrivenom neželjenom poštom:

- ***Premesti poruku u fasciklu sa neželjenom poštom*** - potvrdite izbor u ovom polju za potvrdu ako želite da se svaka otkrivena neželjena poruka automatski premešta u fasciklu sa neželjenom poštom u okviru vašeg klijenta e-pošte;
- ***Dodaj primaoce 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 koju 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 pogrešne detekcije*** - 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

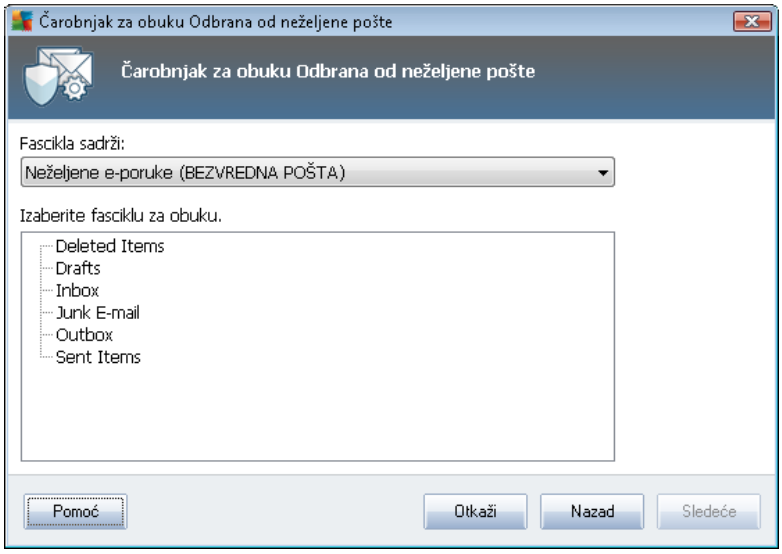
- ***Fascikla sa EML datotekama*** - ako koristite neki drugi program za e-poštu, najpre bi trebalo da sačuvate poruke u određenu fasciklu (*u formatu .eml*) ili da se uverite da znate u kojoj fascikli vaš program za e-poštu čuva poruke. Zatim izaberite ***Fascikla sa EML datotekama***, što će vam u 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



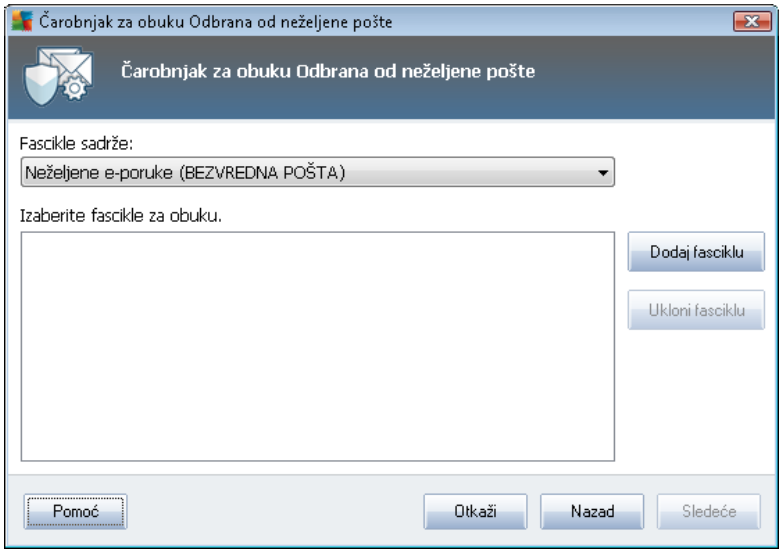
U ovom dijalogu izaberite fasciklu koja sadrži poruke koje želite da upotrebite za obuku. Kliknite na dugme ***Dodaj fasciklu*** da biste pronašli fasciklu koja sadrži .eml datoteke (*sačuvane e-poruke*). Izabrana fascikla biće prikazana u dijalogu.

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

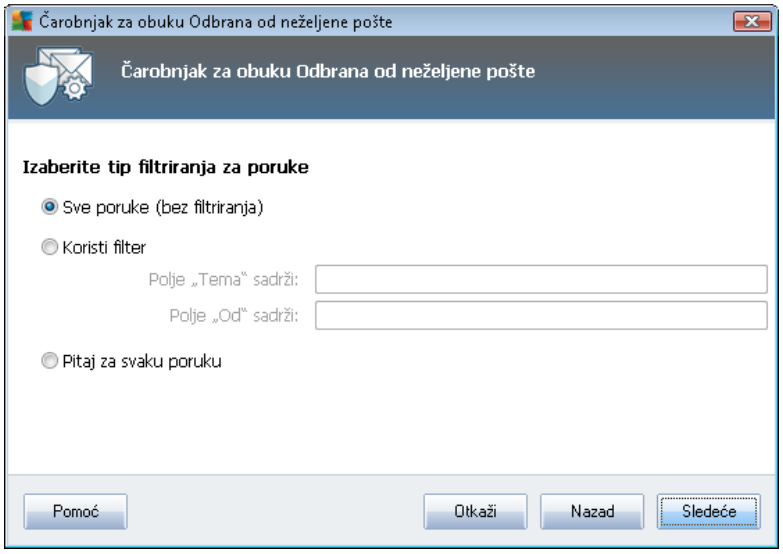
Nakon što potvrdite neku do opcija, pojaviće se novi dijalog.



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.

Ako ste sigurni da izabrana fascikla sadrži samo e-poruke koje želite da upotrebite za obuku, izaberite opciju ***Sve poruke (bez filtriranja)***.

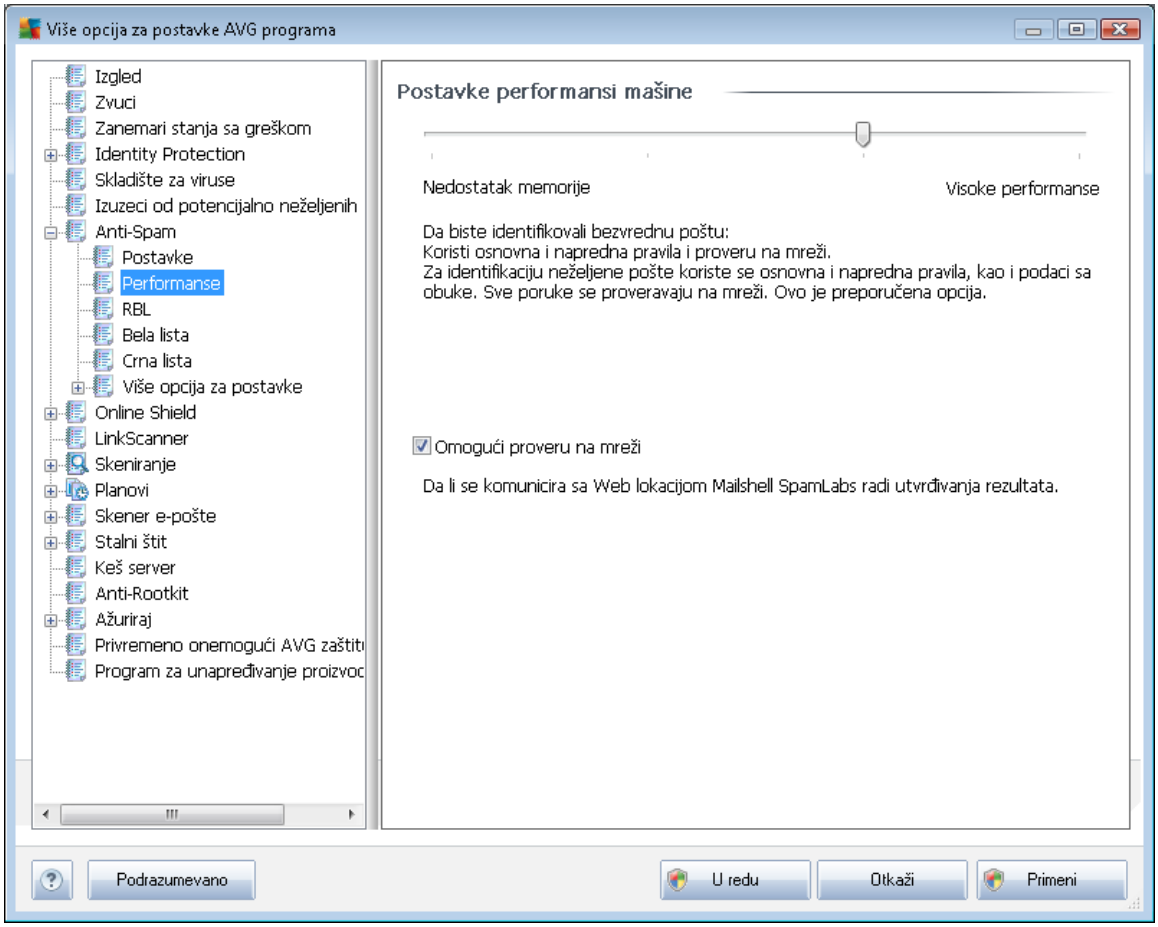
Ako niste sigurni koje poruke se nalaze u fascikli i želite da vas čarobnjak pita za svaku pojedinačnu poruku (da biste utvrdili da li želite da je koristite za obuku), izaberite opciju ***Pitaj za svaku poruku***.

Ako želite naprednije filtriranje, izaberite opciju ***Upotrebi 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.

Pažnja!: *Kada popunite oba okvira za tekst, koristiće se i adrese koje ispunjavaju jedan od dva uslova.*

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.

9.7.2. Performanse



U dijalogu ***Podešavanja performansi mašine***, (*koji je povezan preko stavke* ***Performanse*** *sa leve strane za navigaciju*) nalaze se postavke performansi komponente ***Odbrana od neželjene pošte*** . Pomerajte klizač nalevo ili nadesno da biste promenili nivo performansi skeniranja, koji se kreće između režima ***Nedostatak memorije*** / ***Visoke performanse***.

- ***Nedostatak memorije*** - u toku procesa skeniranja u cilju prepoznavanja neželjene pošte neće se koristiti nikakva pravila. Za identifikaciju se koriste samo podaci za obuku. Ovaj režim nije preporučljiv za uobičajenu upotrebu, osim ukoliko hardver računara nije veoma loš.

- ***Visoke performanse*** - ovaj režim koristi veliku količinu memorije. U toku procesa skeniranja u cilju prepoznavanja neželjene pošte, koristiće se sledeće funkcije: pravila i keš baze podataka o neželjenim porukama, osnovna i napredna pravila, IP adrese pošiljalaca neželjene pošte i baze podataka pošiljalaca neželjene pošte.

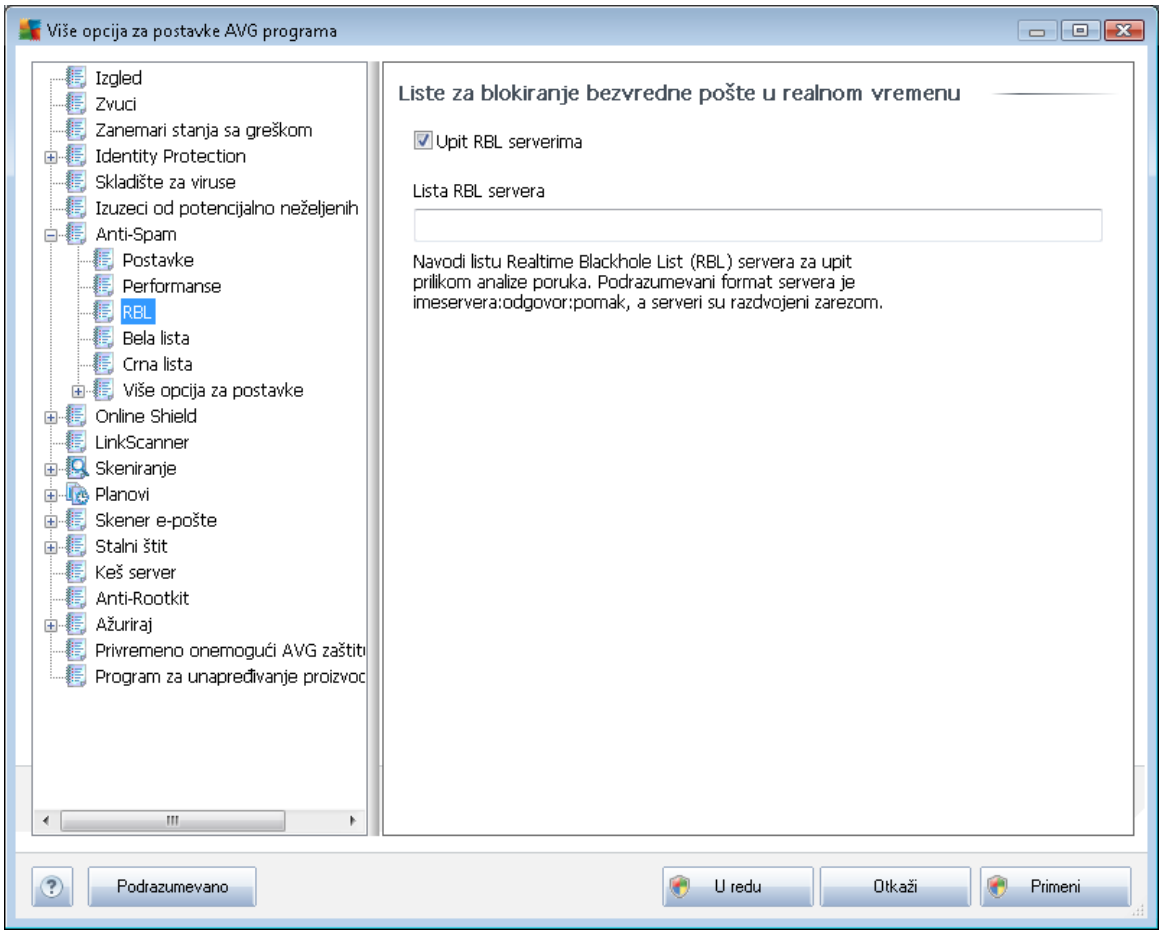
Stavka ***Omogući proveru na mreži*** podrazumevano je uključena. Rezultat je preciznija detekcija neželjene pošte uz pomoć komunikacije sa Mailshell serverima, tj. skenirani podaci će se upoređivati sa Mailshell bazama podataka na mreži.

Uglavnom se preporučuje se da zadržite podrazumevana podešavanja, osim ako nemate

dobar razlog da ih menjate. Ovu konfiguraciju smeju da menjaju samo iskusni korisnici!

9.7.3. RBL

Stavka ***RBL*** otvara dijalog po imenu***Liste za blokiranje neželjene pošte u realnom vremenu***:



U ovom dijalogu možete uključiti/isključiti funkciju ***Upit RBL serverima***.

RBL (*Lista 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 neželjenih poruka radi obezbeđivanja najboljeg i najtačnijeg otkrivanja neželjene pošte. Ova funkcija je posebno korisna za korisnike koji dobijaju velike količine neželjene pošte koju mašina Odbrana od neželjene pošte obično ne otkriva.

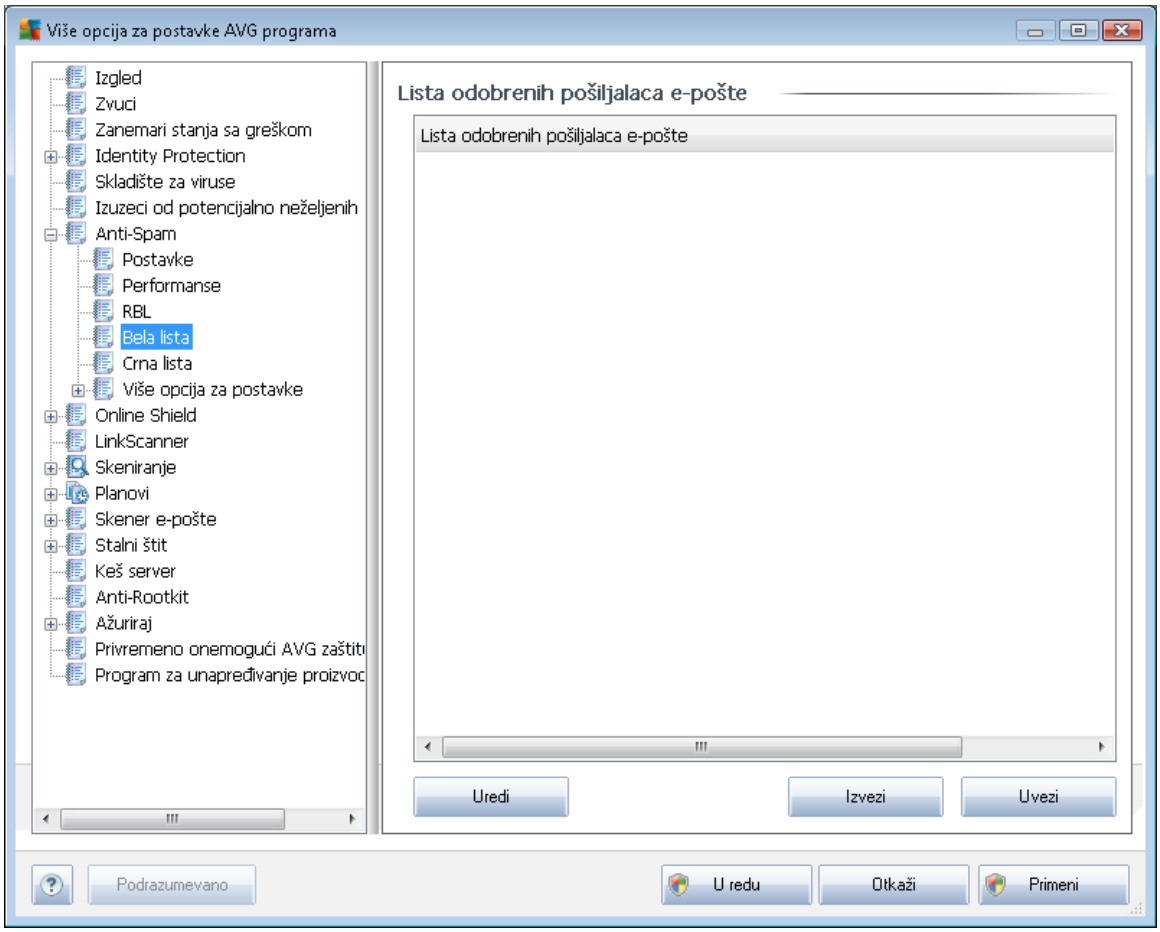
Lista RBL servera omogućava vam da definišete lokacije određenih RBL servera.

Napomena: *Omogućavanje ove funkcije može da uspori proces primanja e-pošte na nekim sistemima i konfiguracijama jer se svaka poruka mora proveriti u bazi podataka RBL servera.*

Lični podaci se ne šalju serveru!

9.7.4. Bela lista

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.

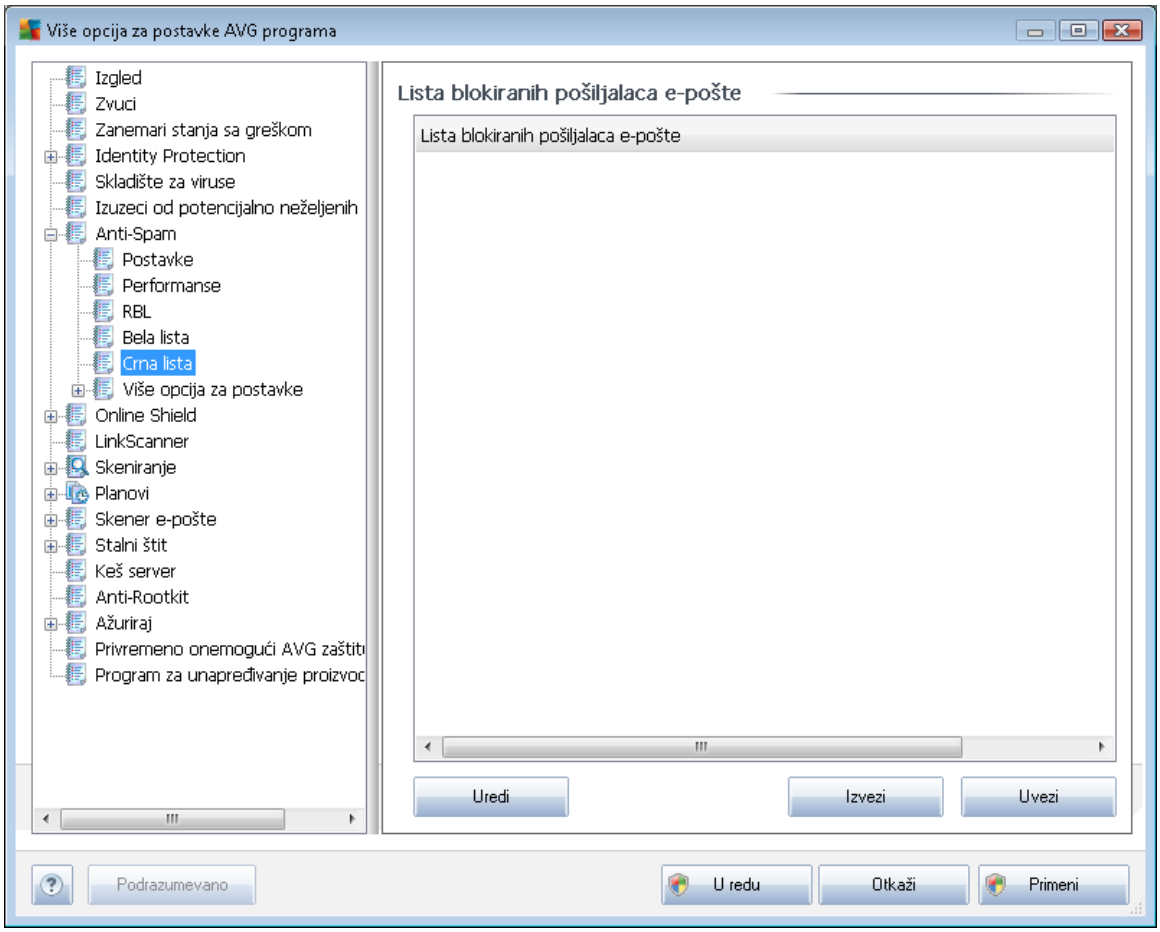
Kada pripremite takvu listu pošiljalaca i/ili imena domena, možete je uneti pomoću sledećih metoda: direktnim unošenjem svake e-adrese ili uvoženjem čitave liste adresa odjednom. Dostupna su sledeća kontrolna dugmad:

- ***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.

9.7.5. Crna lista

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 (bezvredne poruke). Takođe možete da sastavite listu punih imena domena (*npr. preduzeće_koje_šalje_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. 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.

9.7.6. Napredna podešavanja

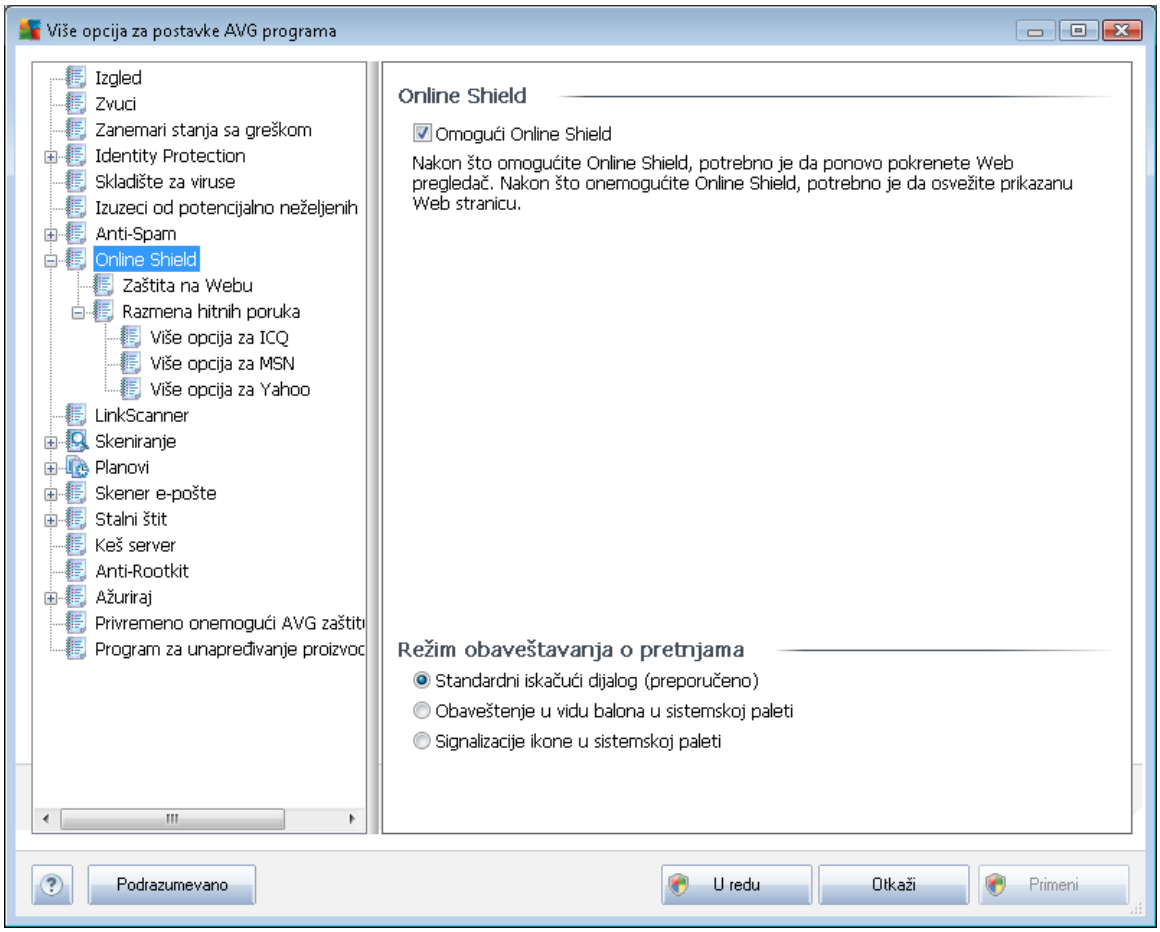
Grana Napredna podešavanja sadrži detaljne opcije za podešavanje komponente Odbrana od neželjene pošte. Ova podešavanja namenjena su za iskusne korisnike, obično za administratore mreže koji treba detaljno da konfigurišu zaštitu od bezvredne pošte kako bi se na najbolji način zaštitili serveri e-pošte. 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 menjate 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

9.8. Online Shield



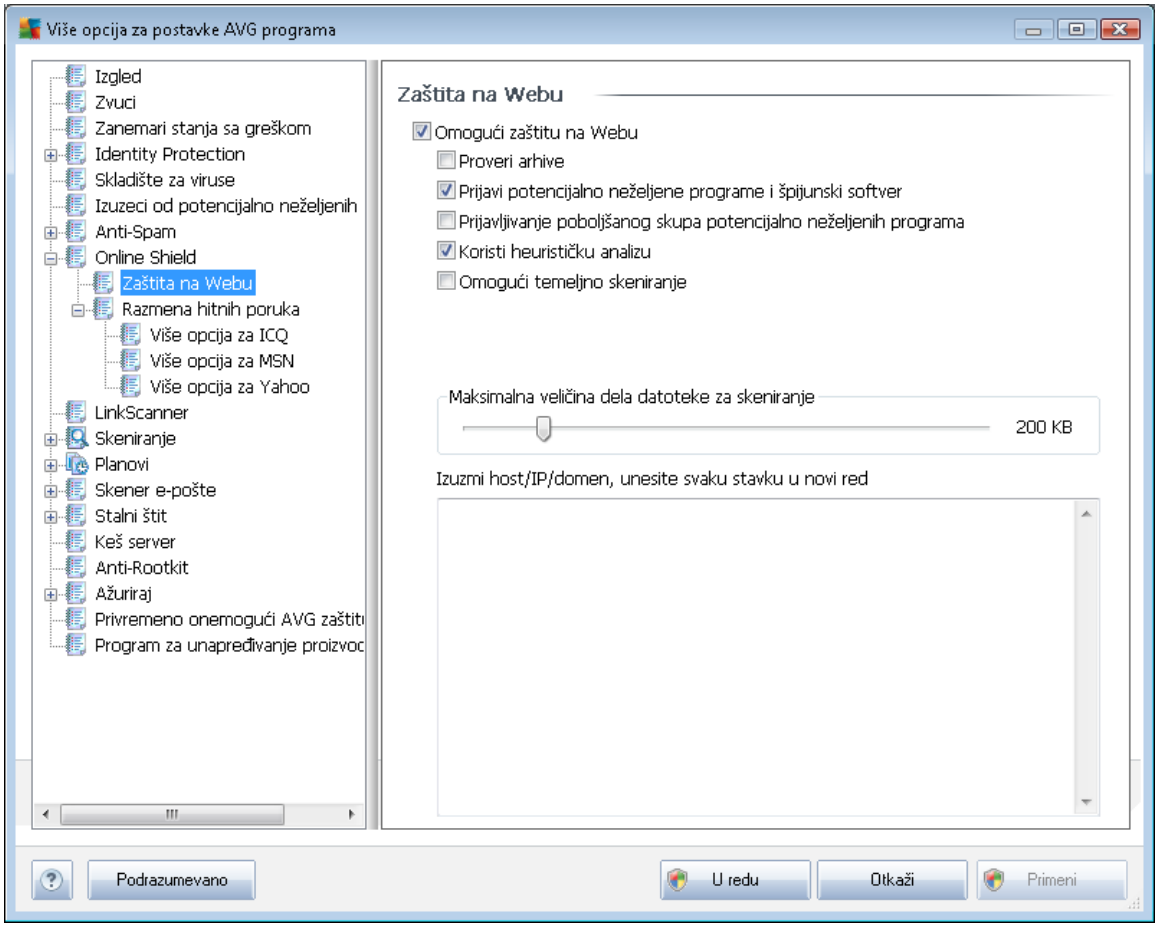
Dijalog ***Online Shield*** vam omogućava da aktivirate/deaktivirate celu komponentu ***Online Shield*** putem opcije ***Omogući Online Shield*** (*aktivirana je podrazumevano*). Za napredna podešavanja ove komponente, otvorite naredne dijaloge na stablu za navigaciju:

- ***Zaštita na Webu***
- ***Razmena hitnih poruka***

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.

9.8.1. Zaštita na Webu



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 špijunski softver*** - (*podrazumevano je uključeno*): potvrdite izbor u ovom polju za potvrdu da biste aktivirali ***Antispajver*** mehanizam i obavili skeniranje u potrazi za špijunskim programima 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.

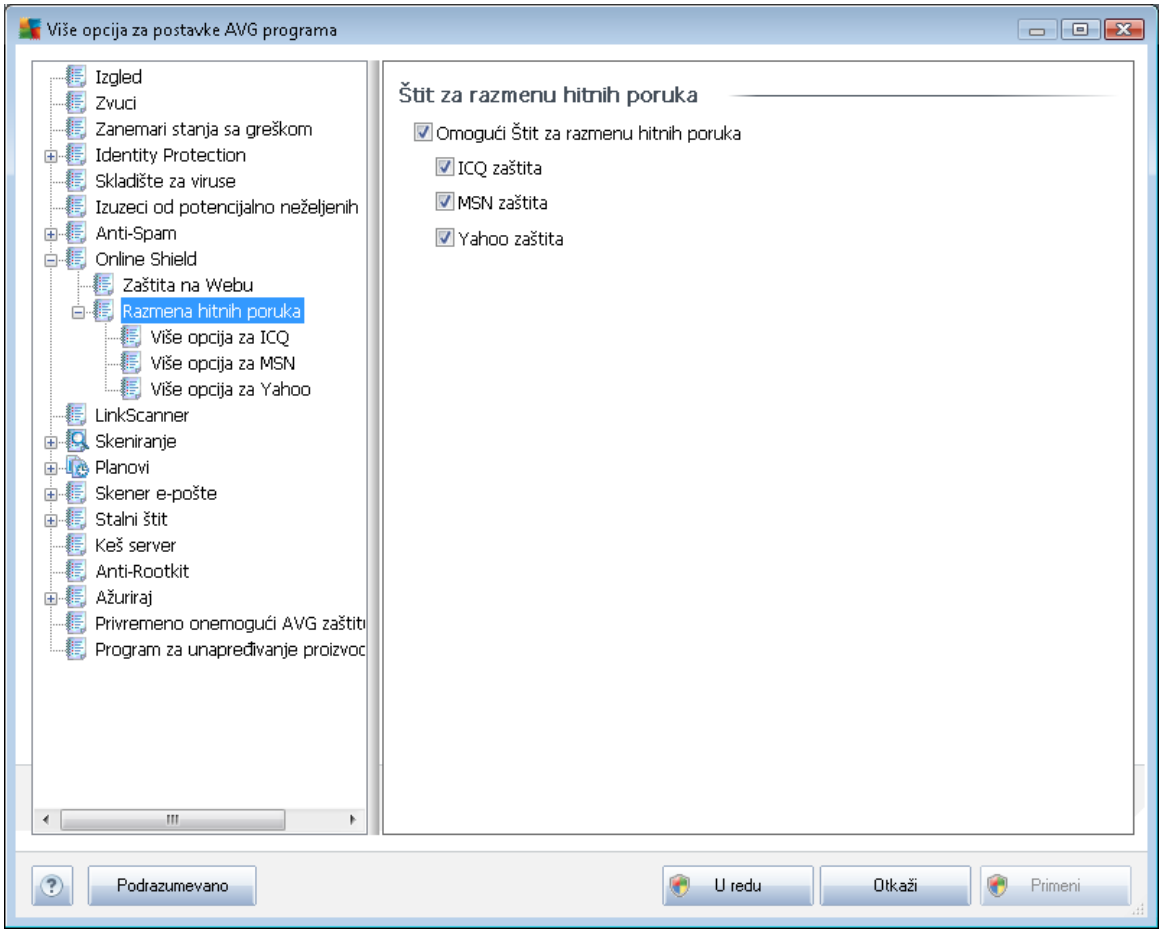
- ***Koristi heurističku analizu***- (*podrazumevano uključeno*): skeniranje sadržaja stranice koja se prikazuje pomoću metoda heurističke analize(*dinamičke emulacije naredbi skeniranog objekta u virtualnom računarskom okruženju*).

- ***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 predviđeno, pa je Online Shield neće skenirati, ipak ćete biti zaštićeni: ako je datoteka zaražena, ***Online Shiled*** 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.

9.8.2. Razmena hitnih poruka

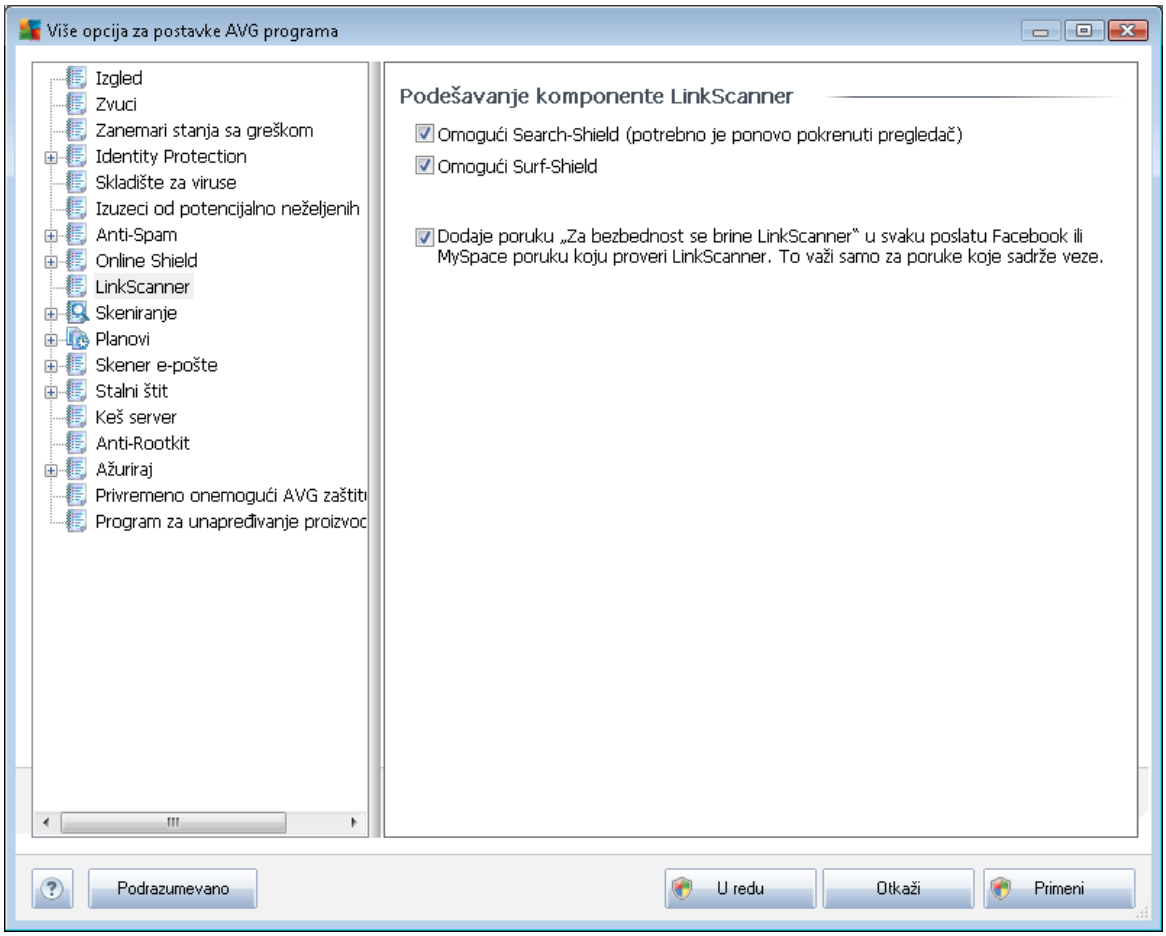


U dijalogu ***Štit za razmenu hitnih poruka***, možete urediti podešavanja komponente ***Online Shield*** koja se odnose na skeniranje hitnih poruka. Trenutno su podržana tri programa za razmenu hitnih poruka: ***ICQ***, ***MSN*** i ***Yahoo*** - potvrdite izbor u odgovarajućem polju za potvrdu pored svake stavke ako želite da ***Online Shield*** proverava da li se komunikacija na mreži odvija bez virusa.

Za detaljno podešavanje dozvoljenih/blokiranih korisnika, možete otvoriti i urediti odgovarajući dijalog (***Napredna podešavanja za ICQ***, ***Napredna podešavanja za MSN, Napredna podešavanja za Yahoo***) i definisati ***belu listu***(*lista korisnika kojima je dozvoljeno da komuniciraju sa vama*) i ***crnu listu*** (*korisnici koje treba blokirati*).

9.9. Skener linkova

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



- ***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*).

- ***Dodaj "Obezbeđeno Skenerom linkova" ...*** - označite ovu stavku da potvrdite da želite da uneste sertifikujuću napomenu o proveri ***Skenerom linkova*** u sve poruke koje sadrže aktivne hiperveze, koje su poslate sa Facebook i MySpace društvenih mreža.

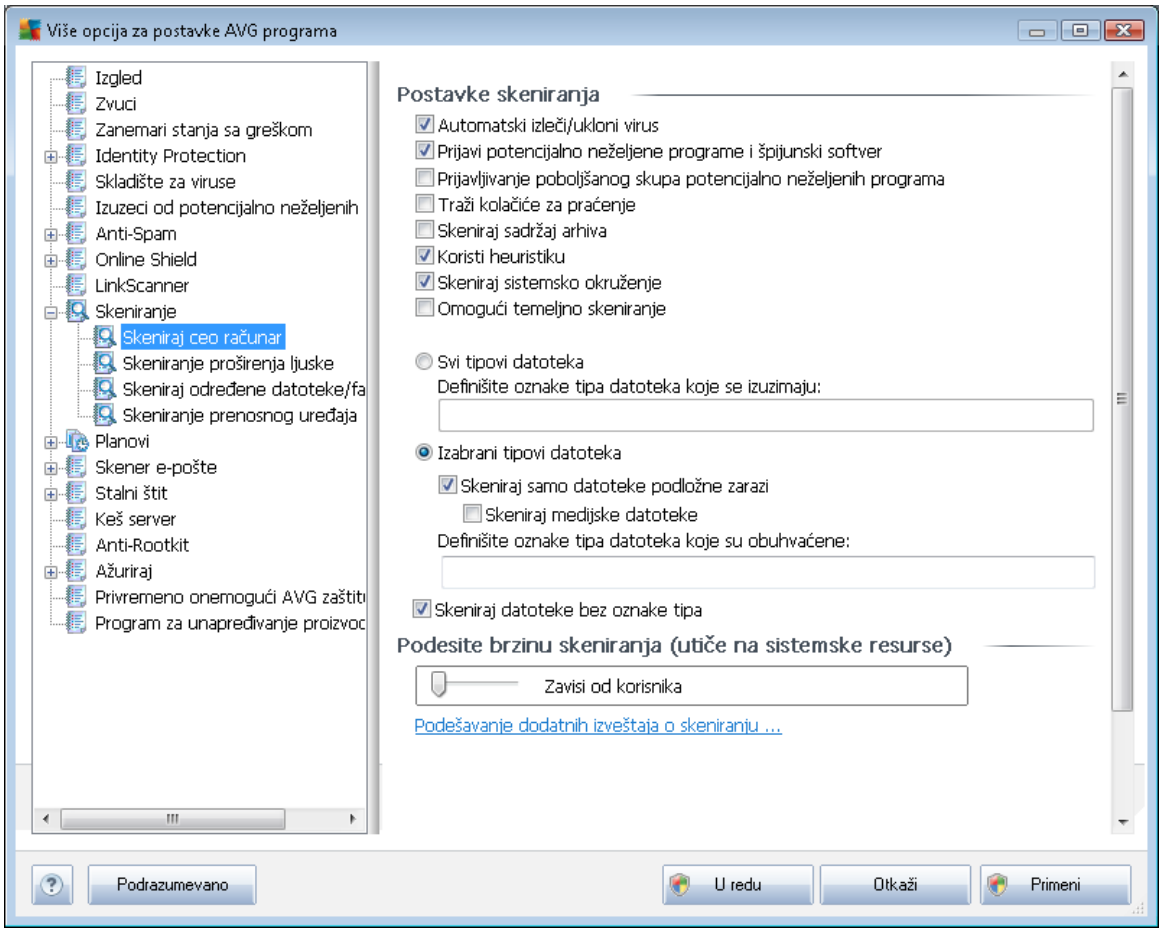
9.10. Skeniranje

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
- ***Skeniraj određene datoteke i fascikle*** - standardno unapred definisano skeniranje izabranih oblasti računara
- ***Skeniranje prenosnog uređaja*** - posebno skeniranje prenosnih uređaja povezanih na računar

9.10.1. Skeniraj ceo računar

Opcija ***Skeniraj ceo računar*** omogućava uređivanje parametara unapred definisanog procesa skeniranja od strane proizvođača softvera, ***Skeniraj ceo računar***:



Podešavanja skeniranja

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

- ***Automatski izleči/ukloni infekciju*** (*podrazumevano uključeno*) - ako tokom skeniranja bude otkriven virus, moguće ga je automatski oporaviti 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 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.

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 datoteke možete označiti datoteke koje treba uvek skenirati.

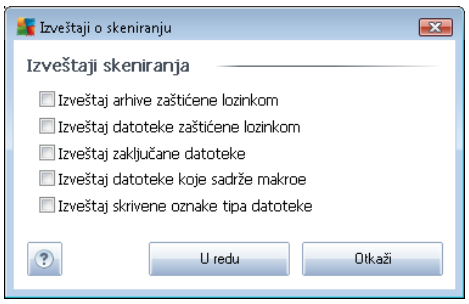
- Možete i da izaberete opciju ***Skeniraj datoteke bez oznake tipa datoteke*** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.

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.

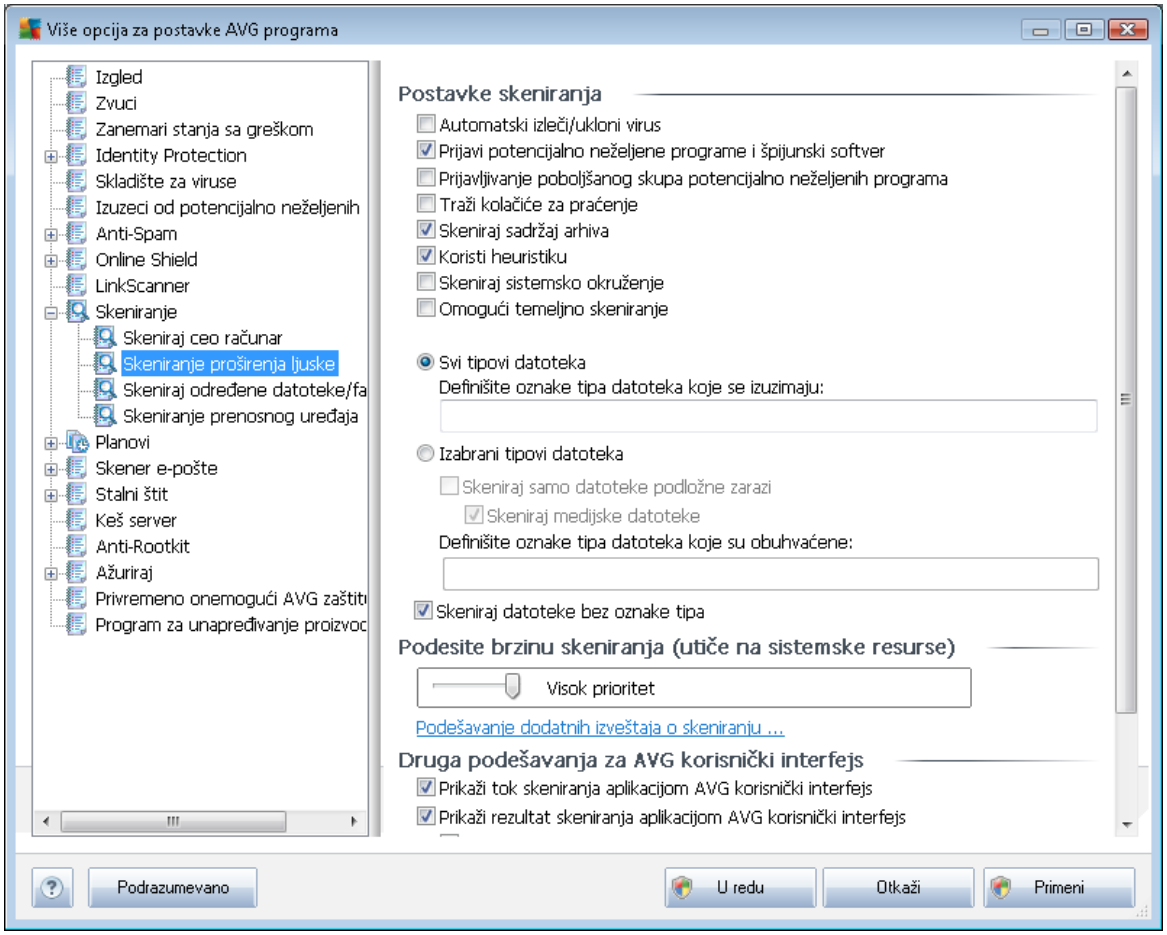
Podešavanje dodatnih izveštaja o skeniranju ...

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:



9.10.2. 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***:



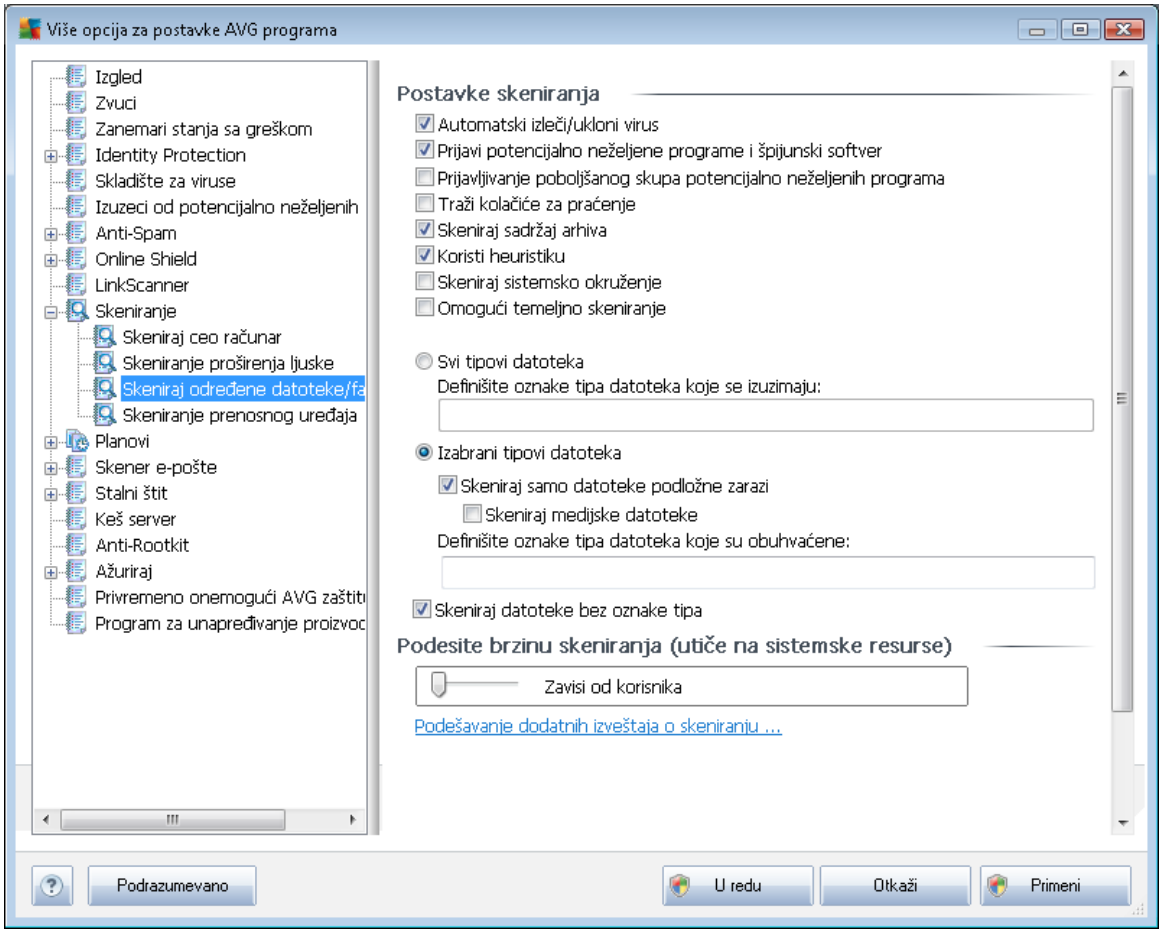
Lista parametara identična je listi koja je dostupna za opciju ***Skeniranje celog računara***. Međutim, podrazumevana podešavanja variraju (*na primer, skeniranje celog računara ne proverava podrazumevano arhive, ali skenira sistemsko okruženje, dok je sa skeniranjem proširenja ljuske stvar drugačija*).

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***takođe uključuje odeljak nazvan ***Druga podešavanja u vezi sa AVG korisnički interfejsom***, gde možete da odredite da li želite da tok i rezultati skeniranja budu pristupačni iz AVG korisničkog interfejsa. Takođe, možete definisati da se rezultati skeniranja prikazuju samo u slučaju ako je infekcija detektovana tokom skeniranja.

9.10.3. Skeniraj određene datoteke ili fascikle

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***:

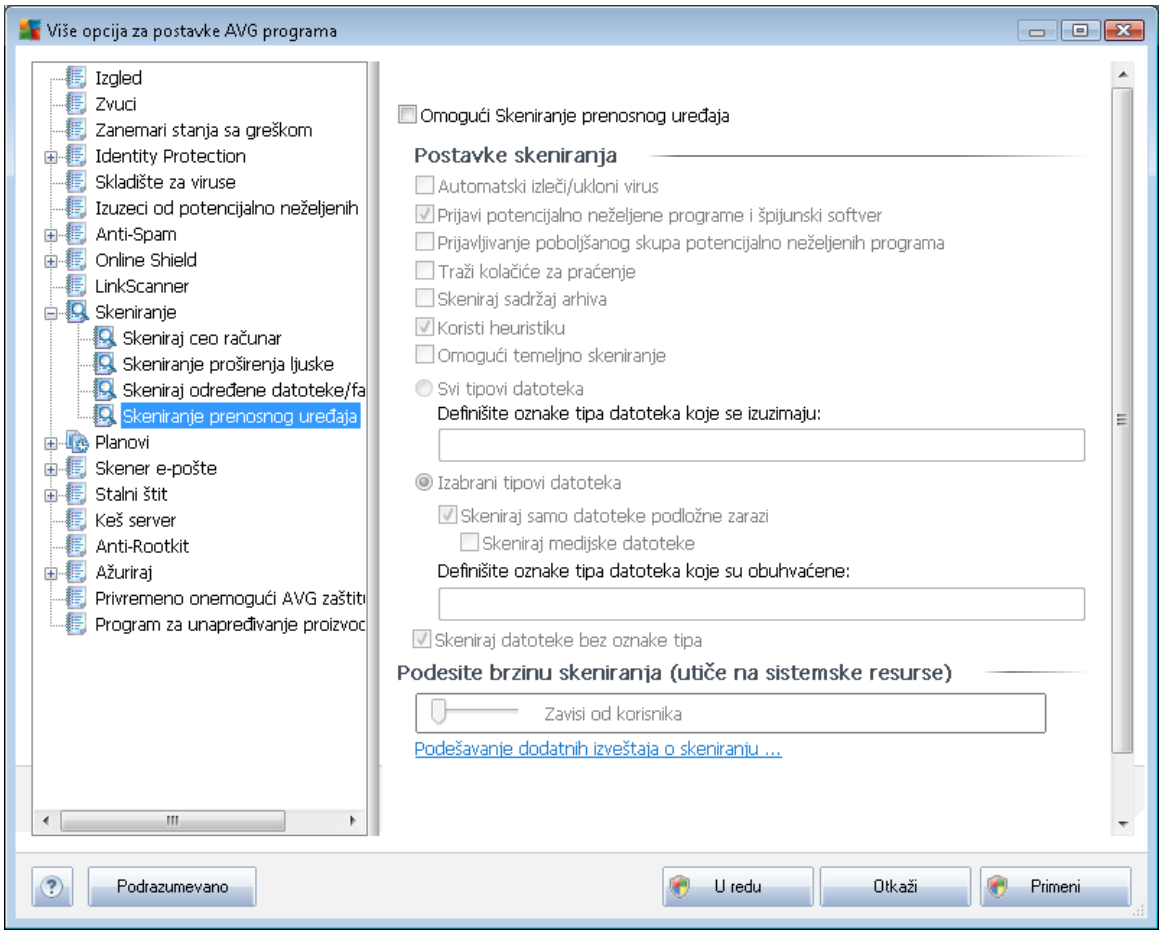


Svi parametri koji su definisani u ovom dijalogu za konfiguraciju odnose se samo na oblasti koje će se skenirati postavkom ***Skeniraj određene datoteke ili fascikle***!

Napomena: *Opis pojedinačnih parametara potražite u poglavlju* ***AVG napredna podešavanja / Skeniranje / Skeniraj ceo računar***.

9.10.4. 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****.*

9.11. Planovi

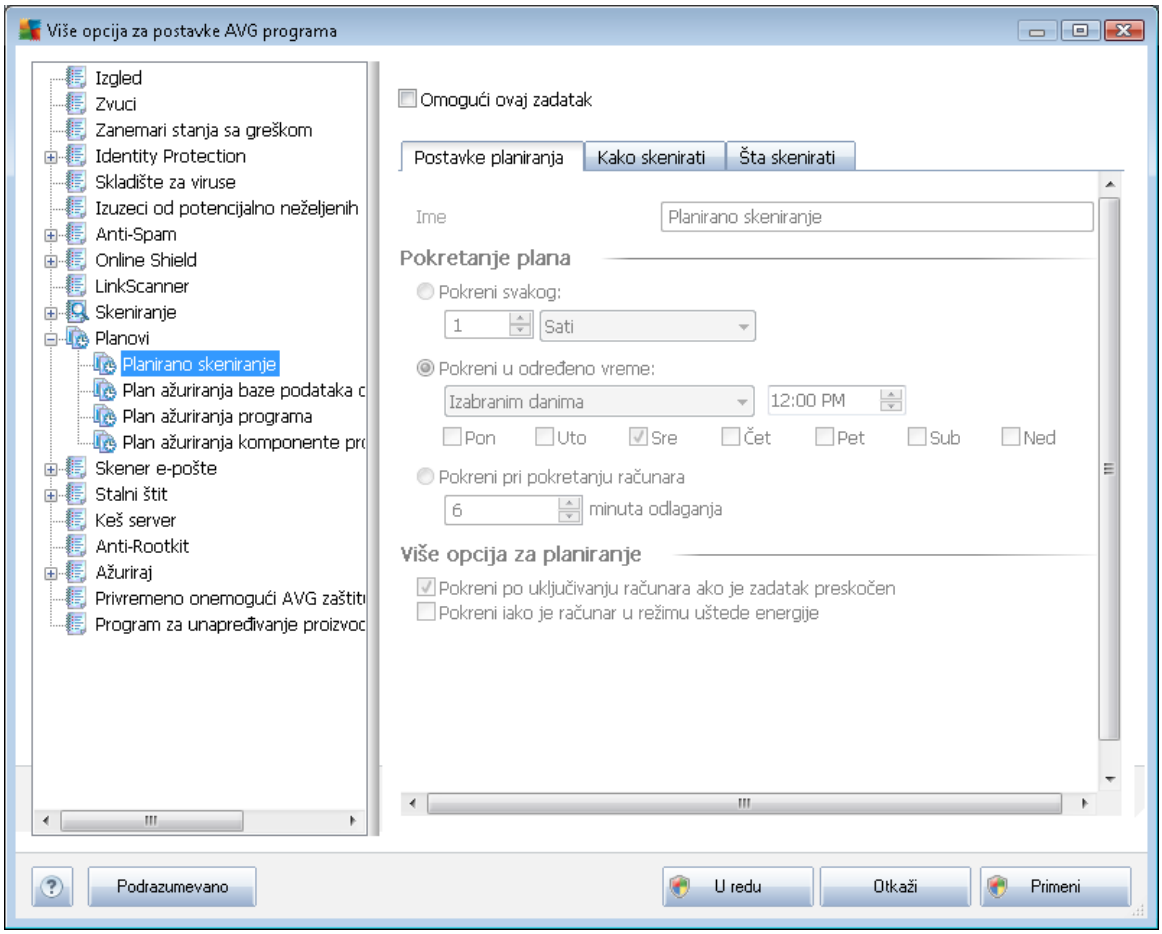
U odeljku ***Planovi*** možete urediti podrazumevane postavke za:

- Planirano skeniranje
- Plan ažuriranja baze podataka o virusima

- Plan ažuriranja programa
- Plan ažuriranja komponente Odbrana od bezvredne pošte

9.11.1. Planirano skeniranje

Parametri planiranog skeniranja mogu se uređivati (*ili se može kreirati novi plan*) na tri kartice. Na svakoj kartici možete prvo označiti/poništiti izbor stavke ***Omogući 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 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

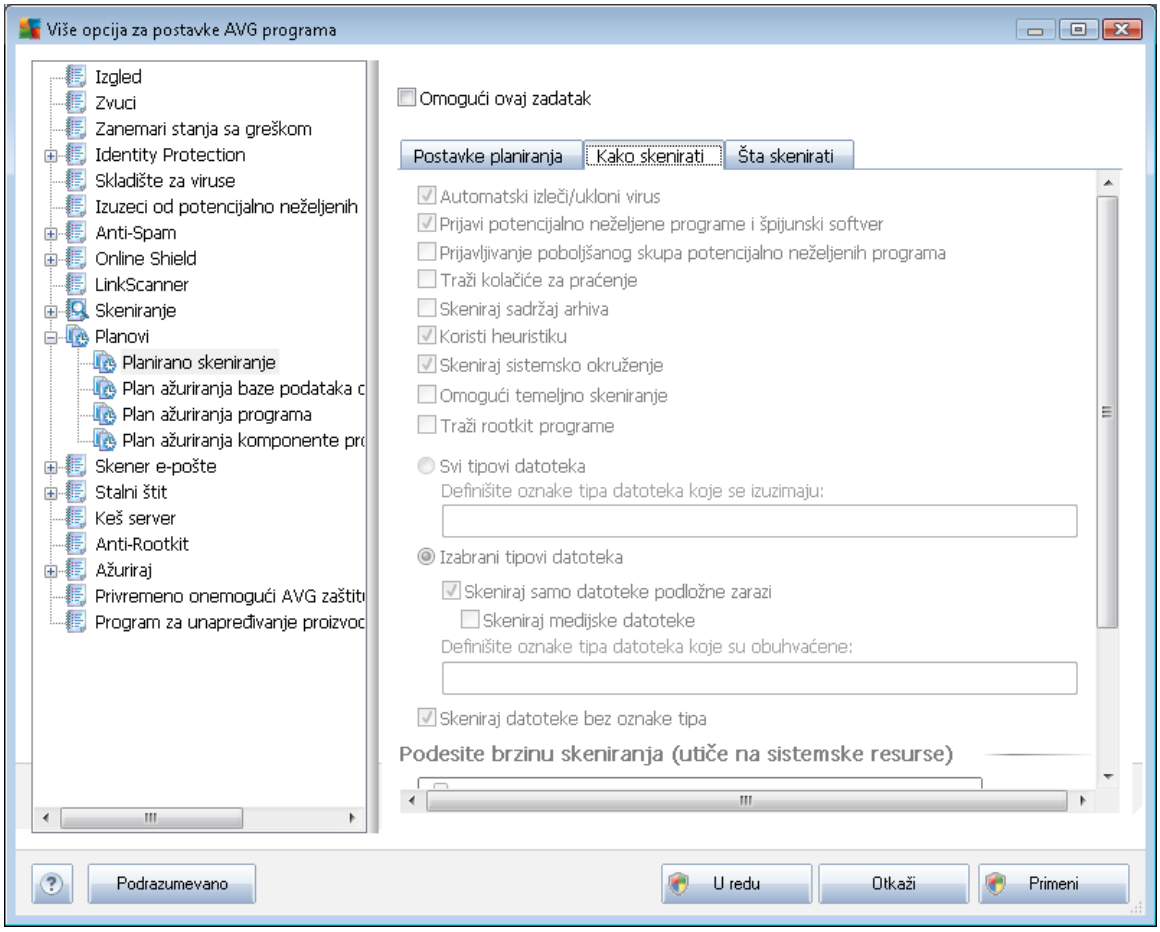
Ovde možete da navedete vremenske intervale za pokretanje novog planiranog skeniranja. Vremenski interval je moguće definisati uzastopnim pokretanjem skeniranja nakon određenog vremenskog perioda (***Pokreni svakih ...***), definisanjem tačnog datuma i vremena (***Pokreni u određeno vreme ...***) ili definisanjem događaja sa kojim bi trebalo povezati pokretanje skeniranja (***Radnja zasnovana na pokretanju računara***).

Više opcija 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 iskačućeg 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 dugmetom miša na ikonu pokrenutog AVG skeniranja da otvorite 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:

- ***Automatski izleči/ukloni infekciju*** *(podrazumevano uključeno):* ako tokom skeniranja bude otkriven virus, moguće ga je automatski oporaviti 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.

- ***Traži rootkit programe*** (*podrazumevano isključeno*): označite ovu stavku ako želite da uključite detekciju rootkit programa u skeniranje celog računara. Detekcija rootkit programa dostupna je i samostalno, u okviru ***Anti-Rootkit*** komponente;

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 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.

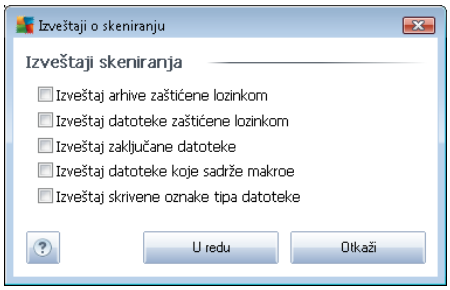
Podesite željenu brzinu završetka skeniranja

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.

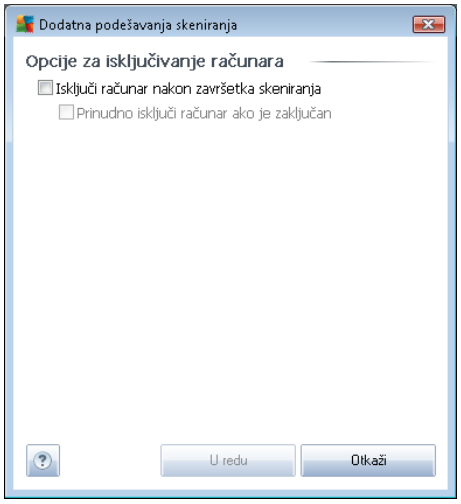
Podešavanje dodatnih izveštaja o skeniranju

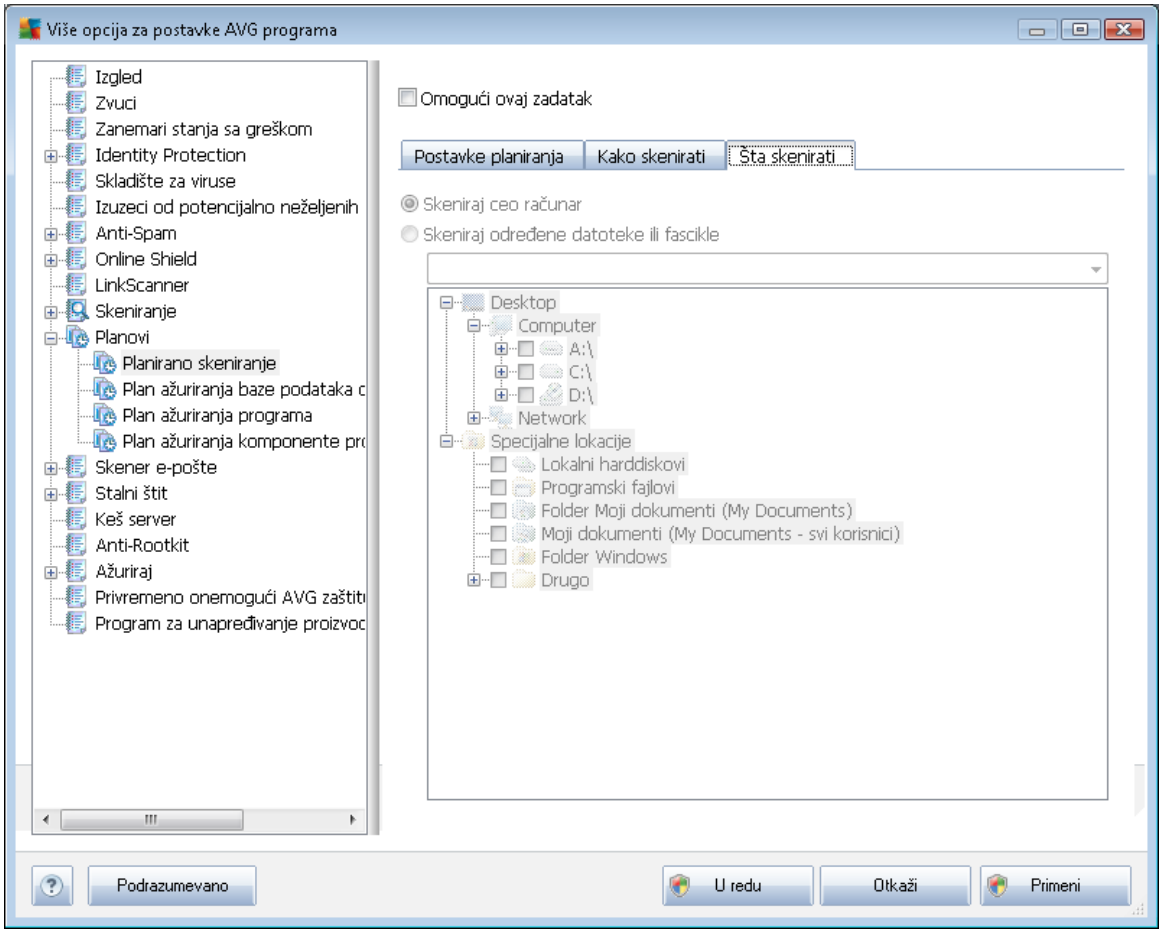
Kliknite na link ***Podešavanje dodatnih izveštaja o skeniranju ...*** da biste otvorili samostalan dijalog po imenu ***Izveštaji skeniranja*** u kojem možete označiti nekoliko stavki kako biste definisali koji će se rezultati prijavljivati:



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***).

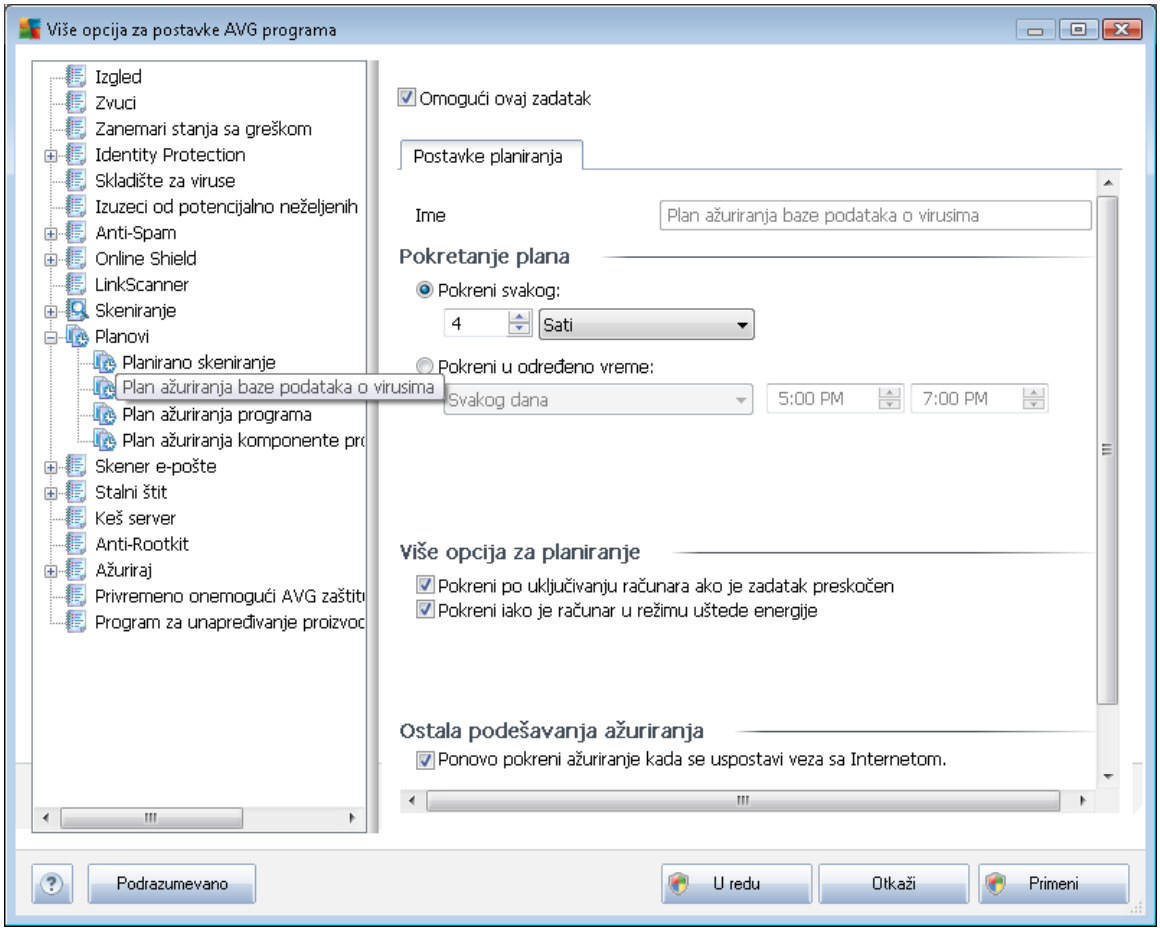




Na kartici ***Šta skenirati*** , možete definisati da li želite da zakažete skeniranje celog računara ili skeniranje određenih datoteka ili fascikli. Ako izaberete skeniranje određenih datoteka ili fascikli, aktiviraće se struktura stabla u donjem delu dijaloga, pa možete navesti koje fascikle želite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

9.11.2. Plan ažuriranja baze podataka o virusima

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



Osnovno planiranje ažuriranja baze podataka o virusima moguće je obaviti unutar komponente ***Upravljanje ažuriranjem***. U ovom dijalogu možete podesiti neke detaljne parametre planiranja ažuriranja baze podataka o virusima. 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 vremenski interval za pokretanje novog planiranog ažuriranja baze podataka o virusima. 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 se okolnostima pokreće/ne pokreće ažuriranje baze podataka o virusima ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

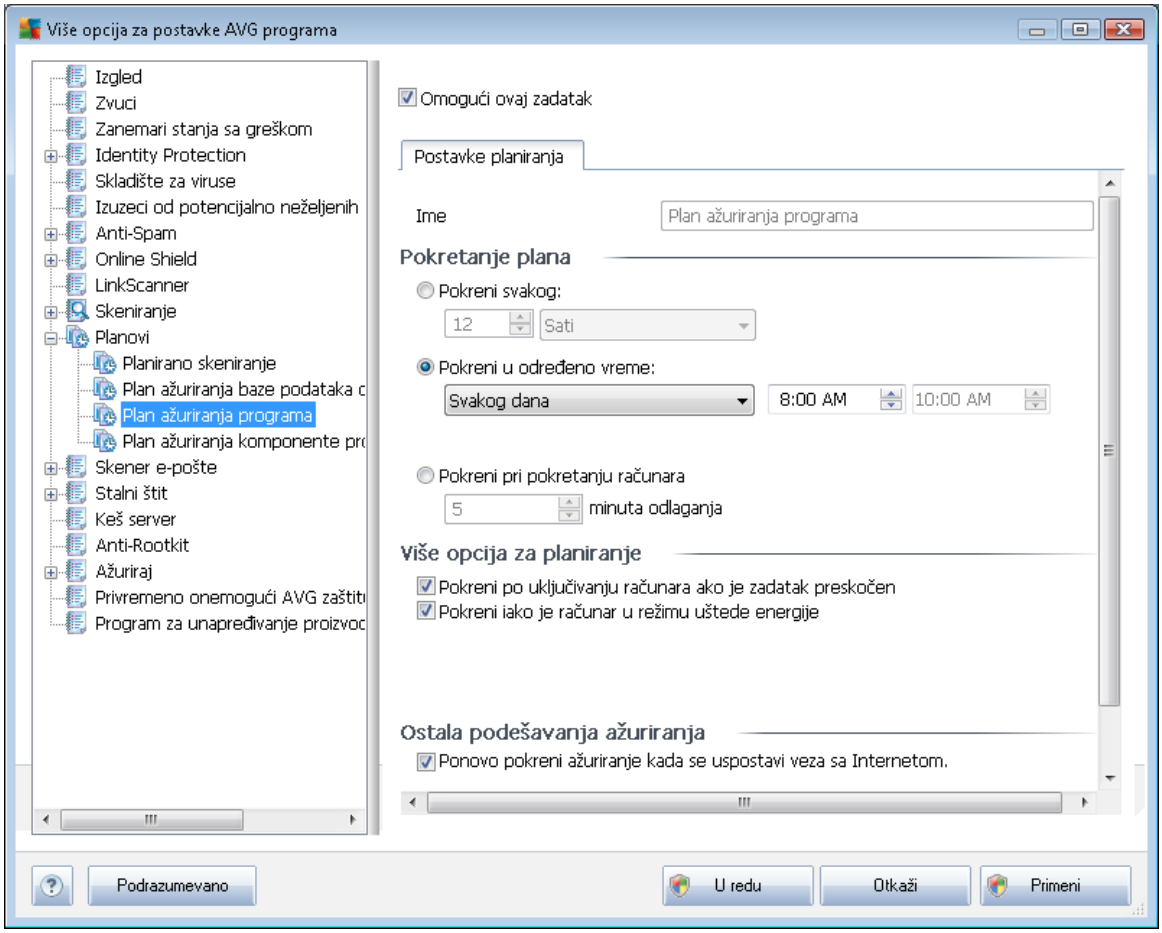
Ostala podešavanja ažuriranja

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 iskačućeg prozora koji se otvorio iznad AVG ikone na sistemskoj paleti(*pod uslovom da niste menjali podrazumevanu konfiguraciju u dijalogu* ***Napredna podešavanja/Izgled***).

9.11.3. 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

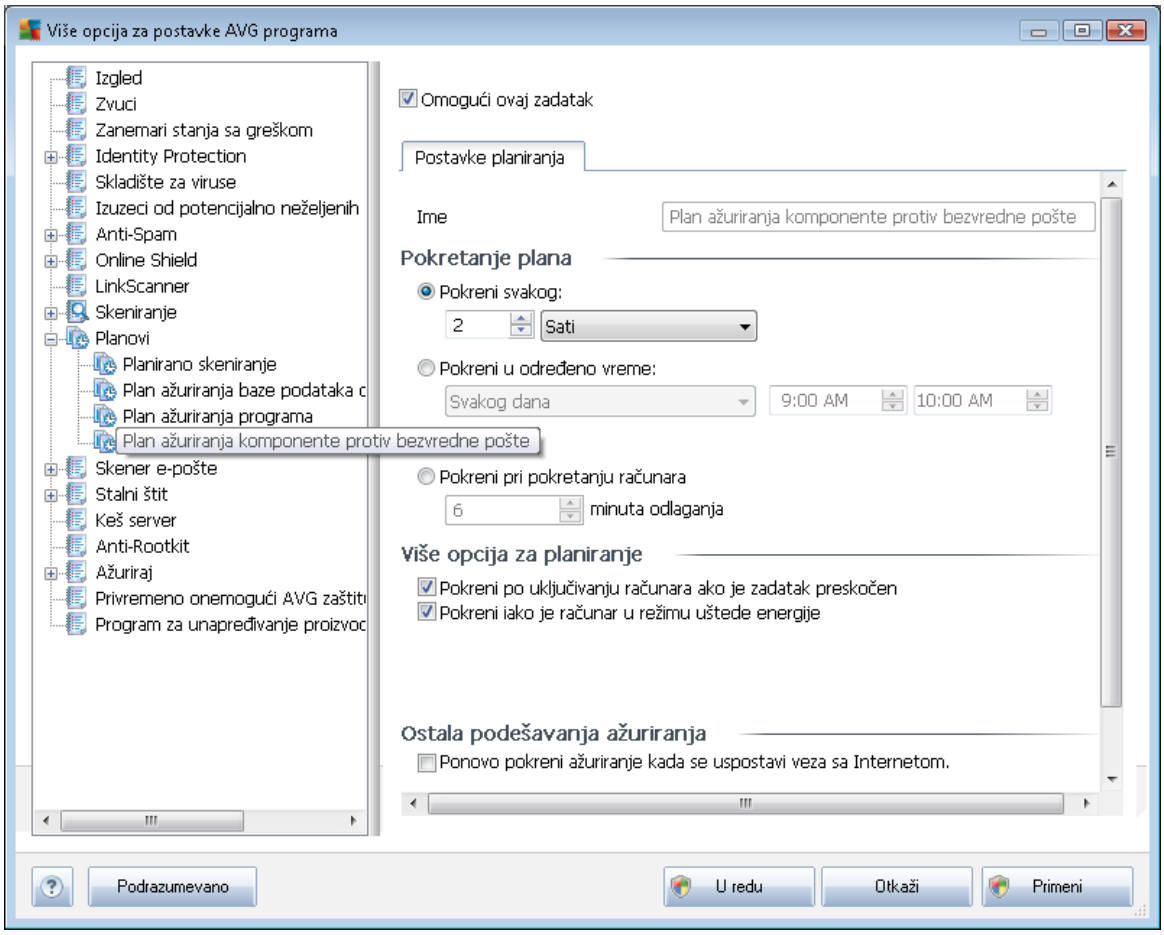
Izaberite opciju ***Ponovo pokreni ažuriranje čim se uspostavi veza sa Internetom*** da biste bili sigurni da će, ako dođe do prekida procesa ažuriranja usled prekida veze sa Internetom, taj proces biti odmah ponovo pokrenut nakon ponovnog uspostavljanja veze sa Internetom.

Kada se pokrene planirano skeniranje u navedenom vremenskom periodu, bićete obavešteni putem iskačućeg prozora koji se otvorio 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, prosec ažuriranja ima veći prioritet pa će skeniranje biti prekinuto.*

9.11.4. Plan ažuriranja Anti-Spam komponente

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



Osnovno planiranje ažuriranja komponente ***Anti-Spam*** obrađeno je u okviru komponente ***Menadžer ažuriranja***. 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 neželjene pošte***. Vremenski interval se može definisati kao redovno pokretanje ažuriranja komponente ***Anti-Spam***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 se okolnostima pokreće/ne pokreće ažuriranje komponente ***Odbrana od neželjene pošte*** ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

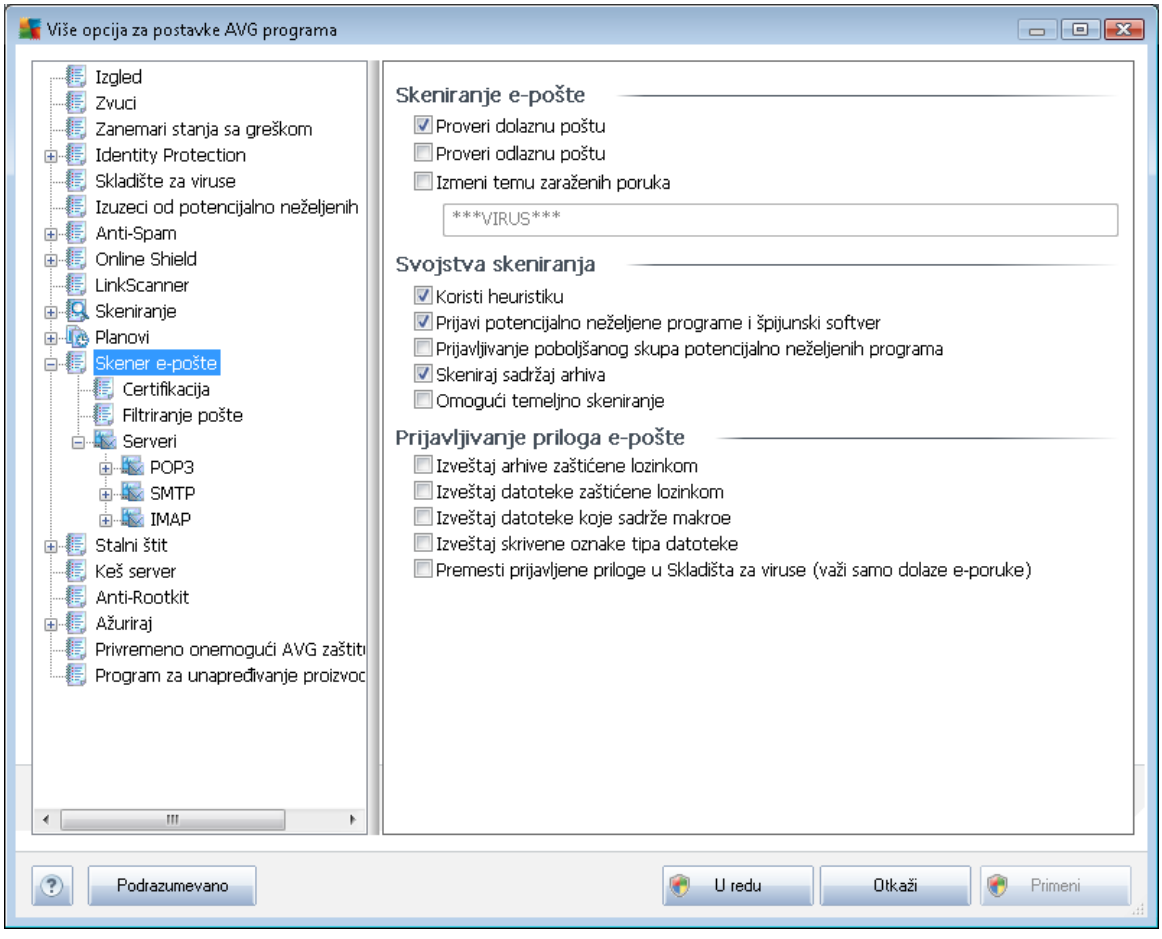
Ostala podešavanja ažuriranja

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 neželjene 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 iskačućeg prozora koji se otvorio iznad AVG ikone na sistemskoj paleti (*pod uslovom da niste menjali podrazumevanu konfiguraciju u dijalogu **Napredna podešavanja/Izgled***).

9.12. 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 paketašpijunskih 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 unutar arhiva*** (*podrazumevano uključeno*) - označite ovo polje radi skeniranja sadržaja arhiva prikačenih 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.

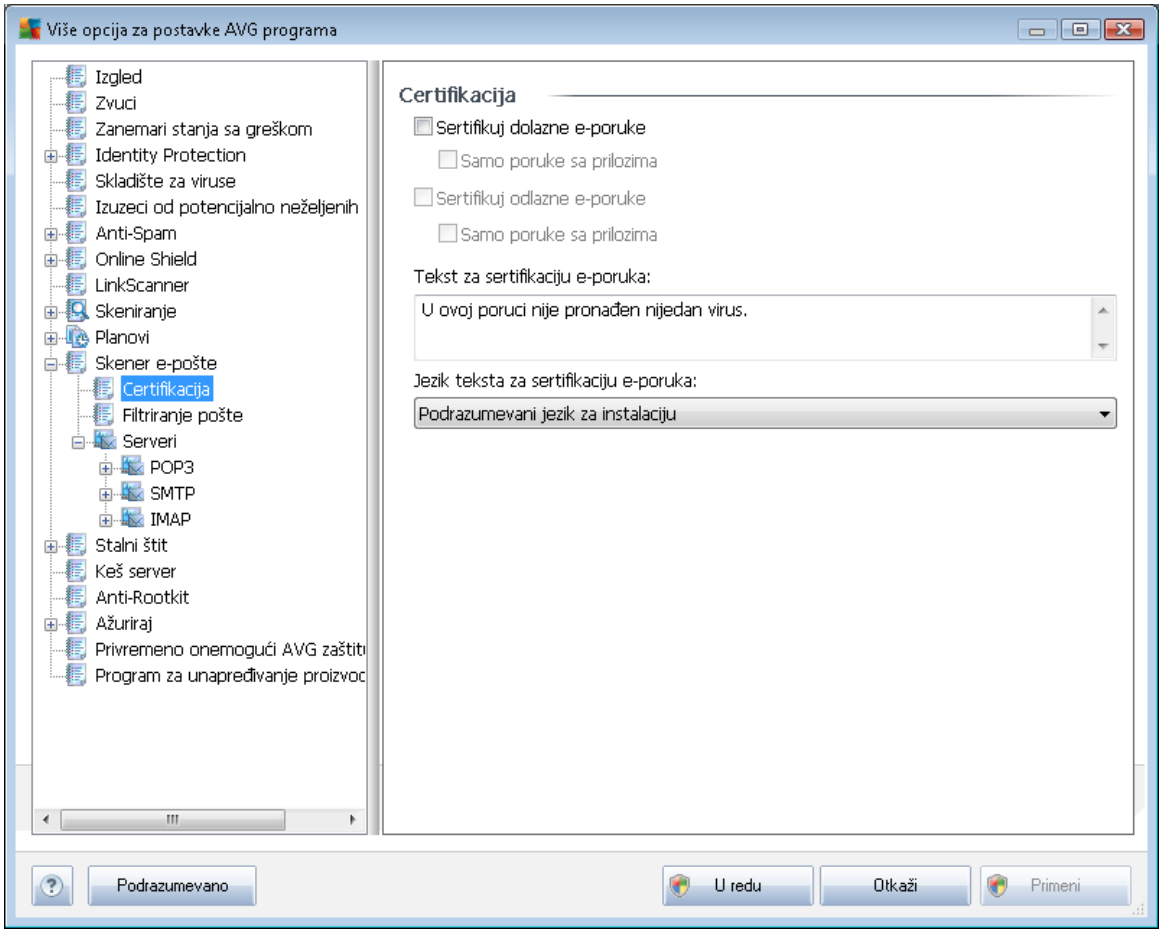
Prijavljivanje priloga e-pošte

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 makroe*** - 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 želeti 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 viruset*** - 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***.

9.12.1. Sertifikacija

U dijalogu ***Sertifikacija*** možete označiti tekst i jezik sertifikacije i za dolaznu i za odlaznu poštu:



Tekst sertifikacije se sastoji iz dva dela, korisničkog dela i sistemskog dela - videti sledeći primer: prva linija predstavlja korisnički deo, ostatak se generiše automatski:

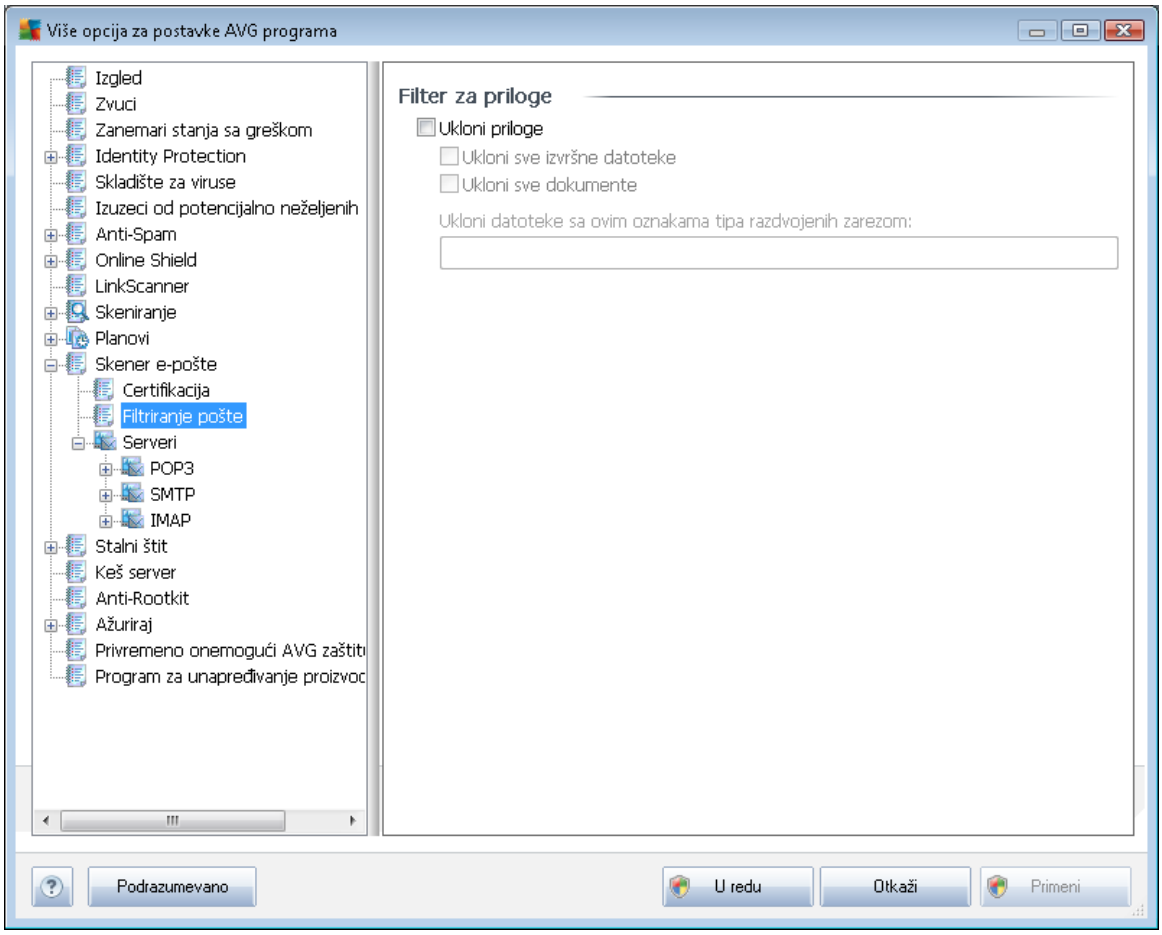
U ovoj poruci nije pronađen nijedan virus.

Proveru obavio AVG.

Verzija: x.y.zz / Baza podataka o virusima: xx.y.z - Datum izdavanja: 12/9/2010

Ako odlučite da koristite sertifikaciju dolaznih ili odlaznih poruka e-pošte, dalje u ovom dijalogu možete označiti tačan sadržaj korisničkog dela teksta sertifikacije (***Tekst sertifikacije e-pošte***) i odabrati koji će se jezik koristiti za automatski generisan deo sertifikacije (***Jezik korišćen za tekst sertifikacije e-pošte***).

9.12.2. Filtriranje pošte

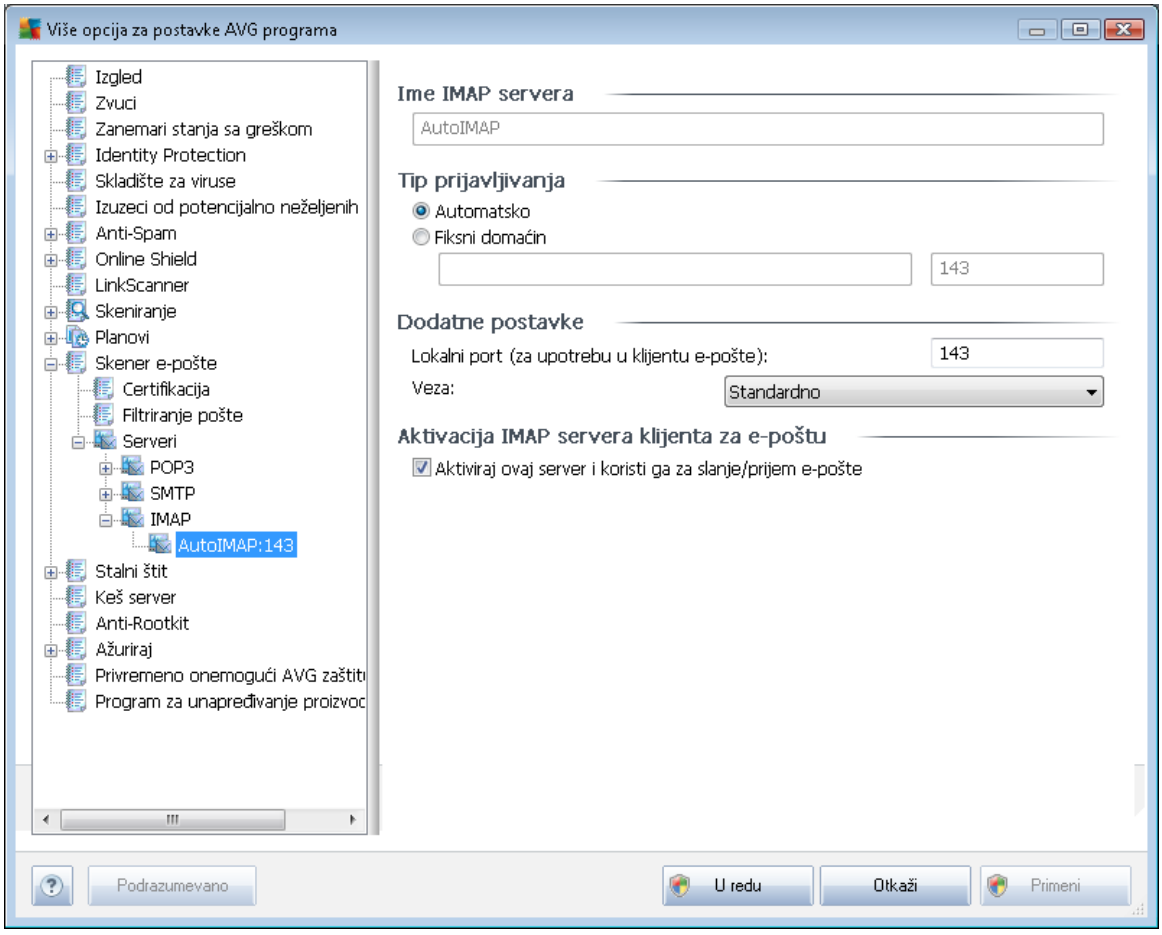


Dijalog ***Filter za priloge*** omogućava vam da podesite parametre za skeniranje priloga e-poruka. Podrazumevano, opcija ***Ukloni priloge*** je isključena. Ako odlučite da je aktivirate, svi prilozi e-poruka koji se prepoznaju kao zarazni ili potencijalno opasni biće automatski uklonjeni. Ako želite 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

9.12.3. Serveri

U odeljku ***Serveri*** možete urediti parametre servera komponente ***Skener e-pošte***, a možete podesiti i novi server 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.

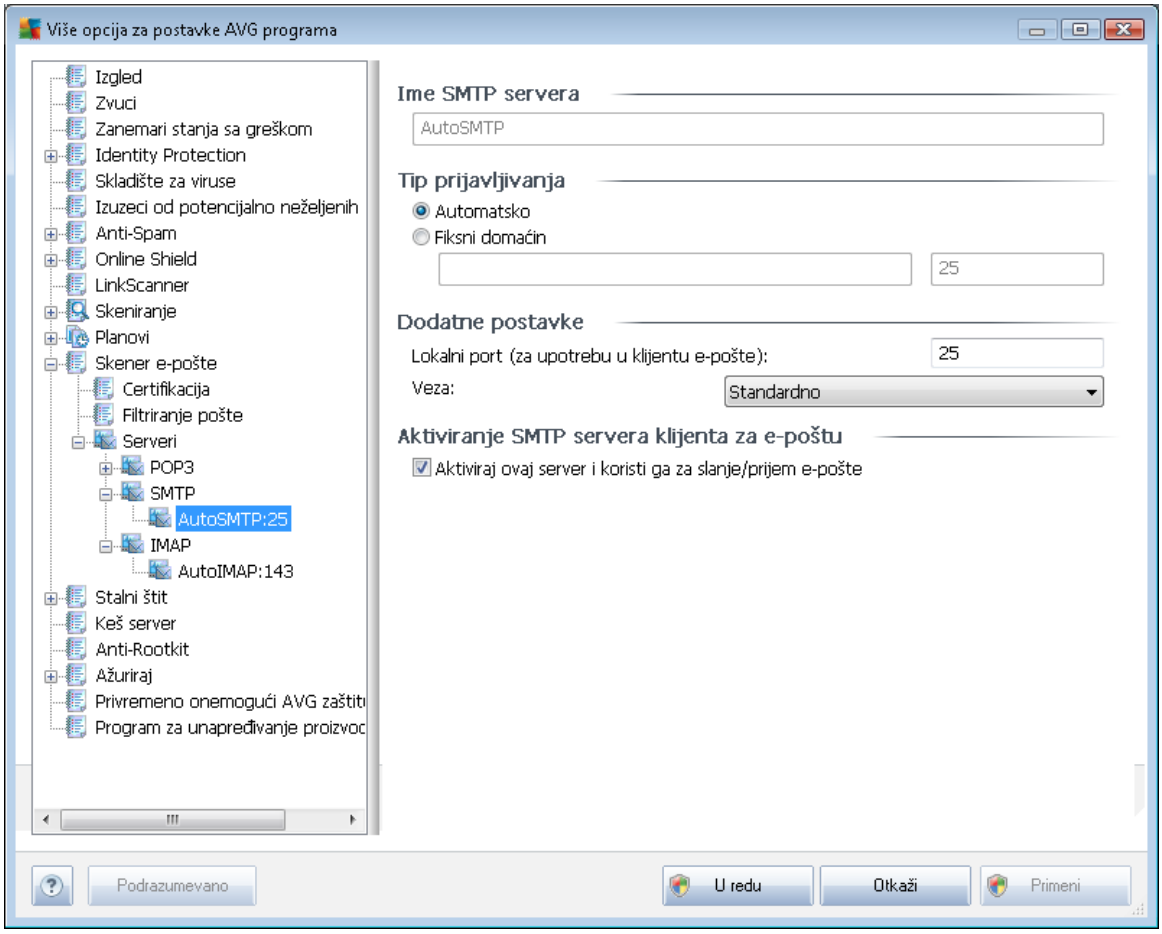
    - ***Fiksni host*** - u ovom slučaju, program će uvek koristiti server koji je ovde naveden. Navedite adresu ili ime svog servera za poštu. Korisničko ime ostaje nepromenjeno. Kao ime možete da koristite ime domena (*na primer, pop.acme.com*) kao i IP adresu (*na primer, 123.45.67.89*). Ako server za 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 odredišni 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

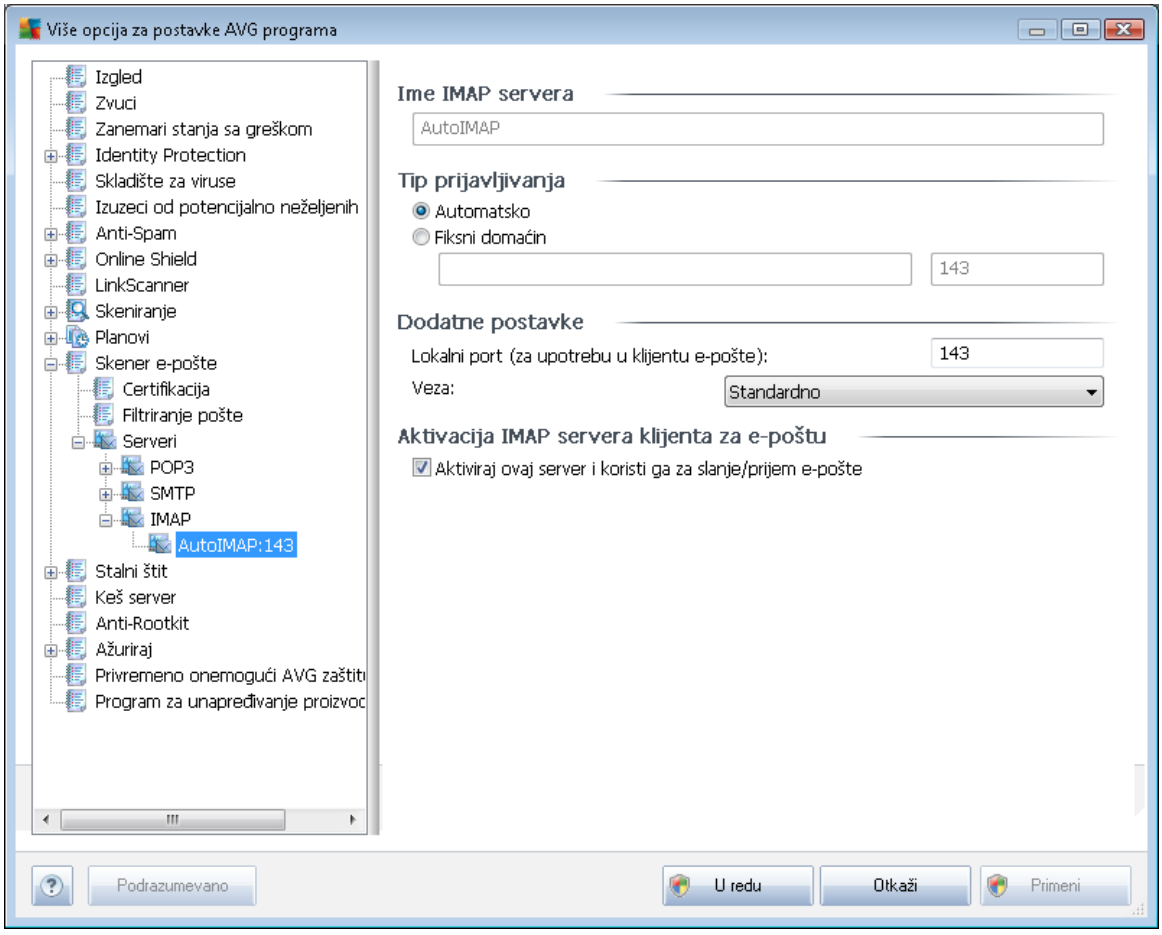
    - ***Fiksni host*** - u ovom slučaju, program će uvek koristiti server koji je ovde naveden. Navedite adresu ili ime svog servera za poštu. Možete da koristite ime domena (*na primer, smtp.acme.com*) kao i IP adresu (*na primer, 123.45.67.89*) kao naziv. Ako server za poštu koristi port koji nije standardan, 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 odredišni 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 dodatih 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:

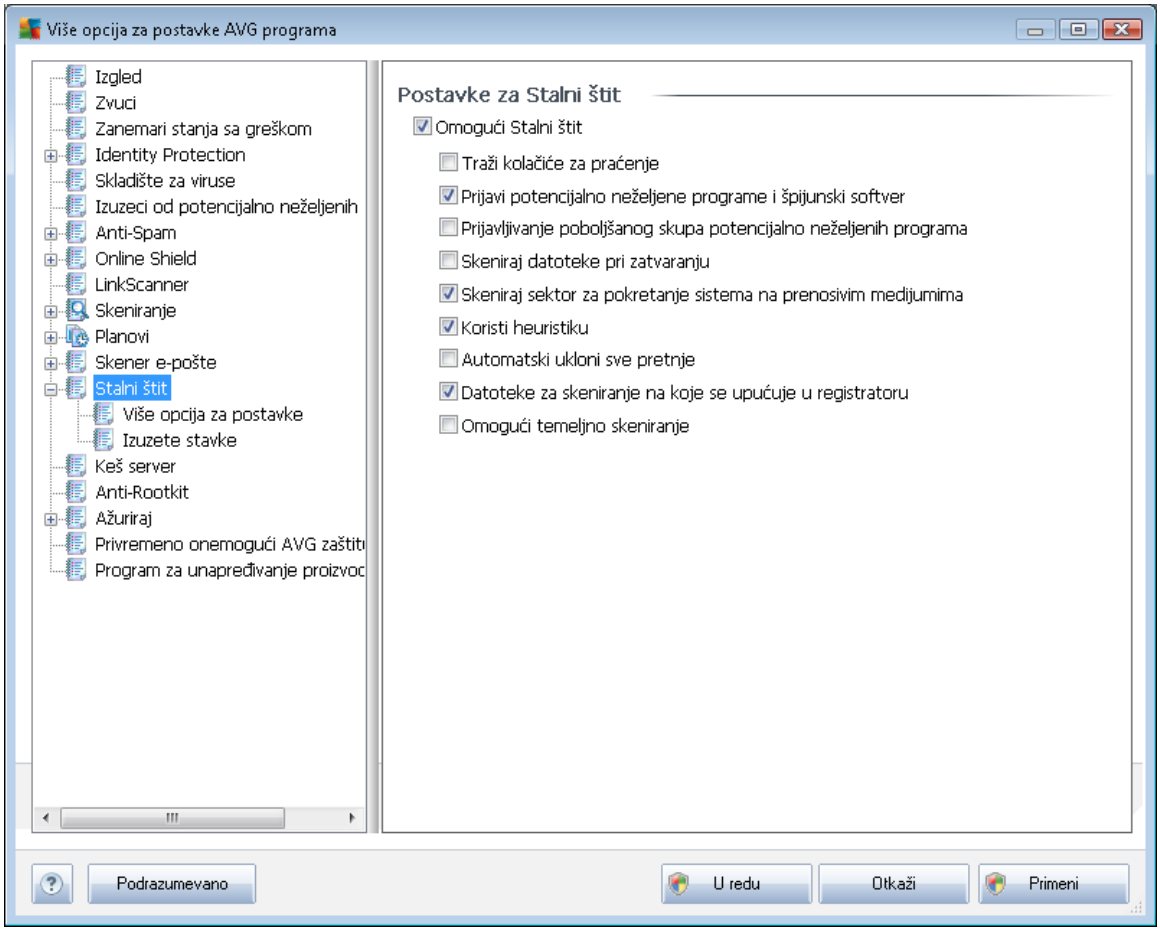
  - ***Lokalni port*** - određuje port na kojem treba očekivati komunikaciju aplikacije za e-poštu. Zatim morate u aplikaciji za poštu da navedete ovaj port kao port za IMAP komunikaciju.

  - ***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 odredišni server za poštu podržava.

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

9.13. Stalni štit

Komponenta ***Stalni štit*** aktivno štiti datoteke i fascikle od virusa, špijunskog softvera i drugog zlonamernog softvera.



U dijalogu ***Podešavanja stalnog štita*** možete aktivirati ili deaktivirati ***Stalni štit*** tako što ćete potvrditi/opozvati izbor u polju za potvrdu ***Omogući Stalni štit*** (*ova opcija je podrazumevano uključena*). Takođe, možete izabrati funkcije ***Stalnog štita*** koje bi trebalo aktivirati:

- ***Traži kolačiće za praćenje*** (*podrazumevano isključeno*) - pomoću ovog parametra definiše se da bi tokom skeniranja trebalo 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 špijunski softver*** - (*podrazumevano je uključeno*): potvrdite izbor u ovom polju za potvrdu da biste aktivirali ***Antispajver*** mehanizam i obavili skeniranje u potrazi za špijunskim programima 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 datoteke pri zatvaranju*** (*podrazumevano isključeno*) - skeniranje po zatvaranju omogućava AVG softveru da skenira aktivne objekte (npr. aplikacije, dokumente ...) pri otvaranju i pri zatvaranju; ova funkcija pomaže u zaštiti računara od nekih tipova složenih virusa

- ***Skeniraj sektor za pokretanje sistema na prenosivim medijumima*** (*podrazumevano uključeno*)

- ***Koristi heuristiku*** - (*podrazumevano uključeno*) heuristička analiza koristiće se za otkrivanje (*dinamičke emulacije instrukcija skeniranih objekata u virtuelnom računarskom okruženju*)

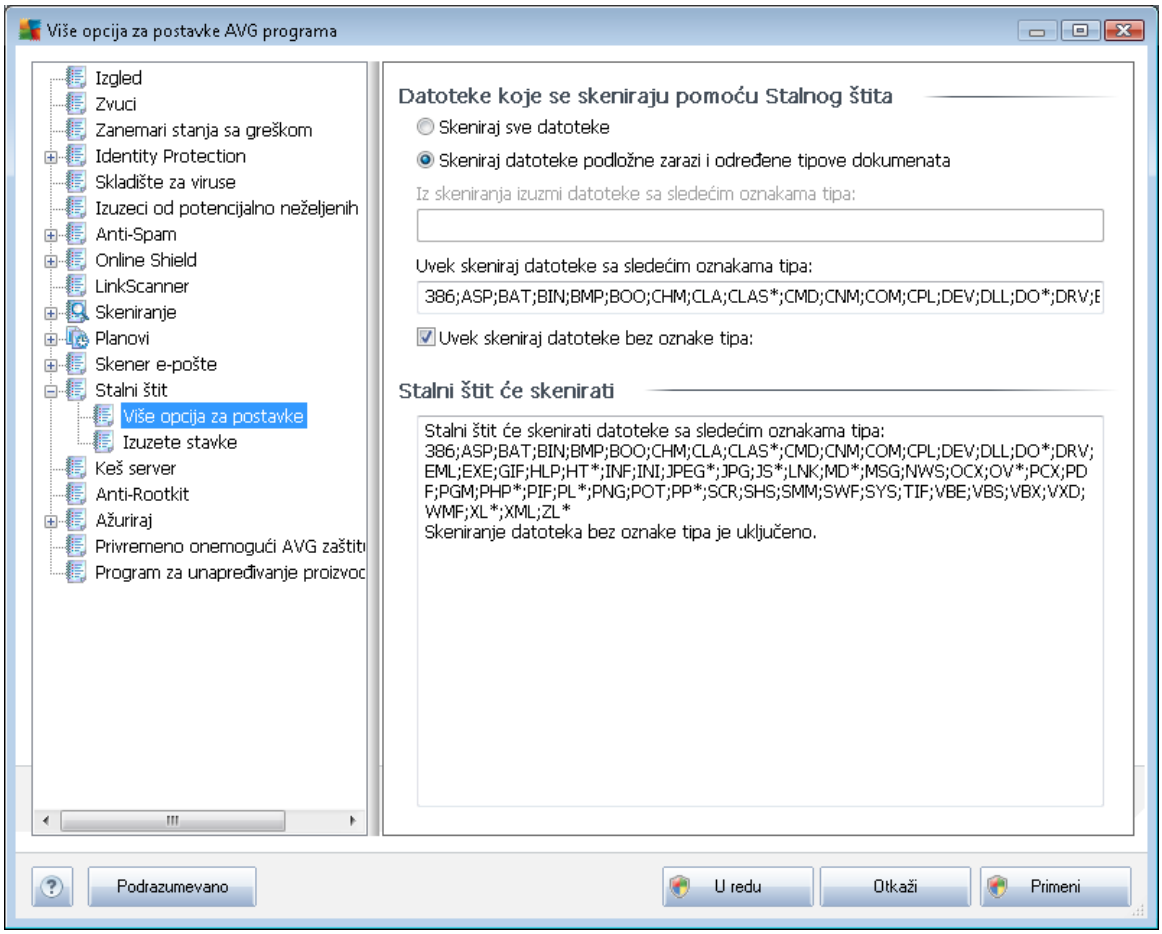
- ***Automatski ukloni sve pretnje***(*podrazumevano isključeno*) - svaka otkrivena zaraza će automatski biti izlečena ako postoji lek i sve zaraze koje se ne mogu izlečiti biće uklonjene.

- ***Skeniraj zapise o datotekama u registratoru*** (*podrazumevano uključeno*) - ovaj parametar definiše da AVG skenira sve izvršne datoteke dodate u početni registrator radi izbegavanja izvršenja poznate infekcije pri sledećem pokretanju računara.

- ***Omogući temeljno skeniranje*** (*podrazumevano isključeno*) - u određenim situacijama (*u stanju krajnje nužde*) možete označiti ovu opciju da aktivirate najtemeljnije algoritme koji će proveriti dubinski sve potencijalne objekte pretnje. Ipak, zapamtite da ovaj metod prilično dugo traje.

9.13.1. Napredna podešavanja

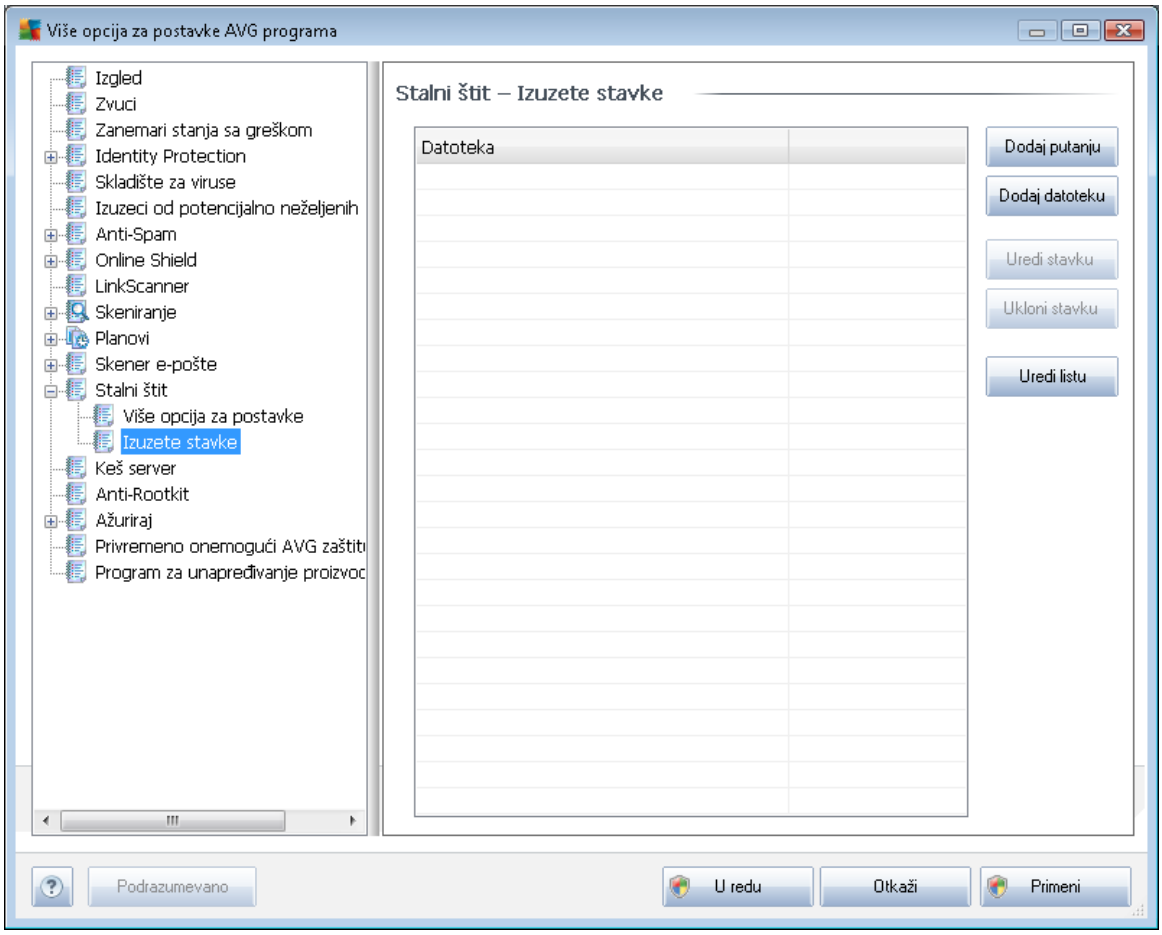
U dijalogu ***Datoteke koje se skeniraju pomoću Stalnog štita*** možete konfigurisati koje će se datoteke skenirati (*na osnovu njihove oznake tipa*):



Odlučite da li želite da se skeniraju sve datoteke ili samo datoteke podložne zarazi - dalje možete definisati listu oznaka tipa datoteke koje se neće skenirati, kao i listu oznaka tipa datoteke koje se obavezno moraju skenirati.

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

9.13.2. Izuzete stavke



Dijalog ***Stalni štit - Isključene stavke***nudi mogućnost definisanja datoteka i/ili fascikli koje treba izuzeti iz skeniranja komponentom ***Stalni štit***.

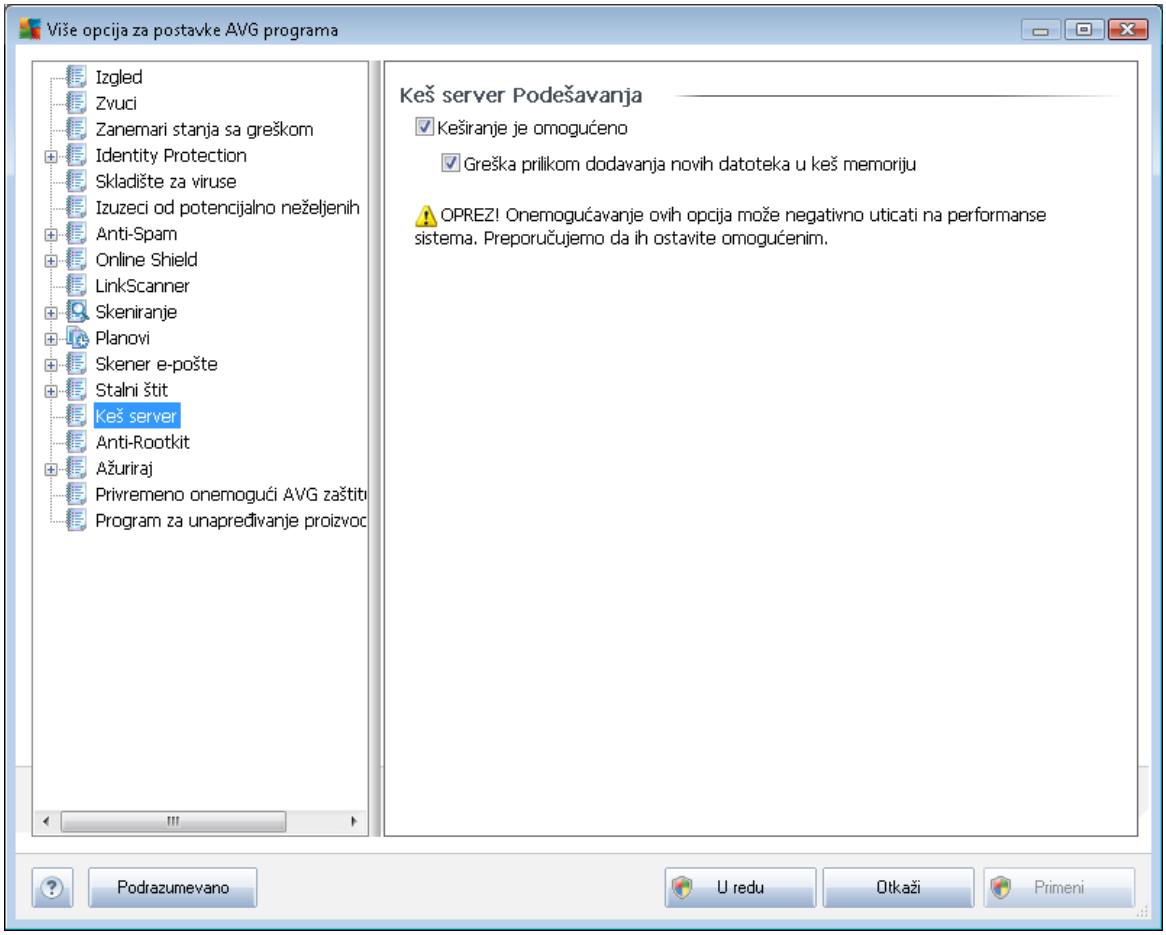
Preporučujemo vam da ne izuzimate nijednu stavku ako to nije neophodno!

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

9.14. Keš server

Keš server je proces osmišljen tako da ubrza različite vrste skeniranja (*skeniranje na zahtev, planirano skeniranje celog računara, skeniranje komponentom Stalni štit*). On prikuplja i čuva informacije o pouzdanim datotekama (*(sistemskim datotekama sa digitalnim potpisom itd.*): Te datoteke se smatraju bezbednim i preskaču se tokom skeniranja.



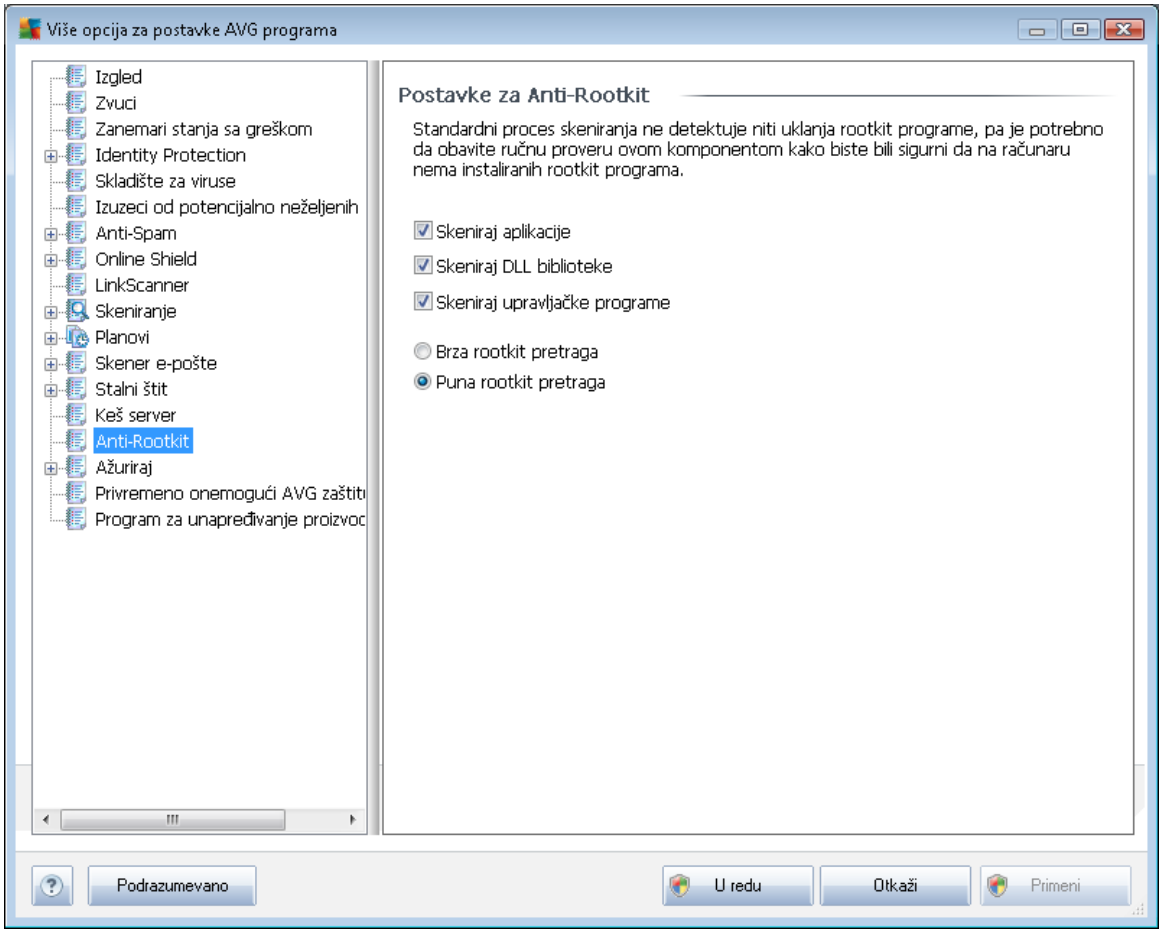
U dijalogu za podešavanje na raspolaganju imate dve opcije:

- ***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.

9.15. Anti-Rootkit

U ovom dijalogu možete urediti konfiguraciju komponente ***Anti-Rootkit***:



Uređivanje svih funkcija komponente ***Anti-Rootkit***navedenih u ovom dijalogu moguće je i direktno iz ***interfejsa komponente Anti-Rootkit***.

Potvrdite izbor u odgovarajućim poljima za potvrdu da biste označili objekte koje treba skenirati:

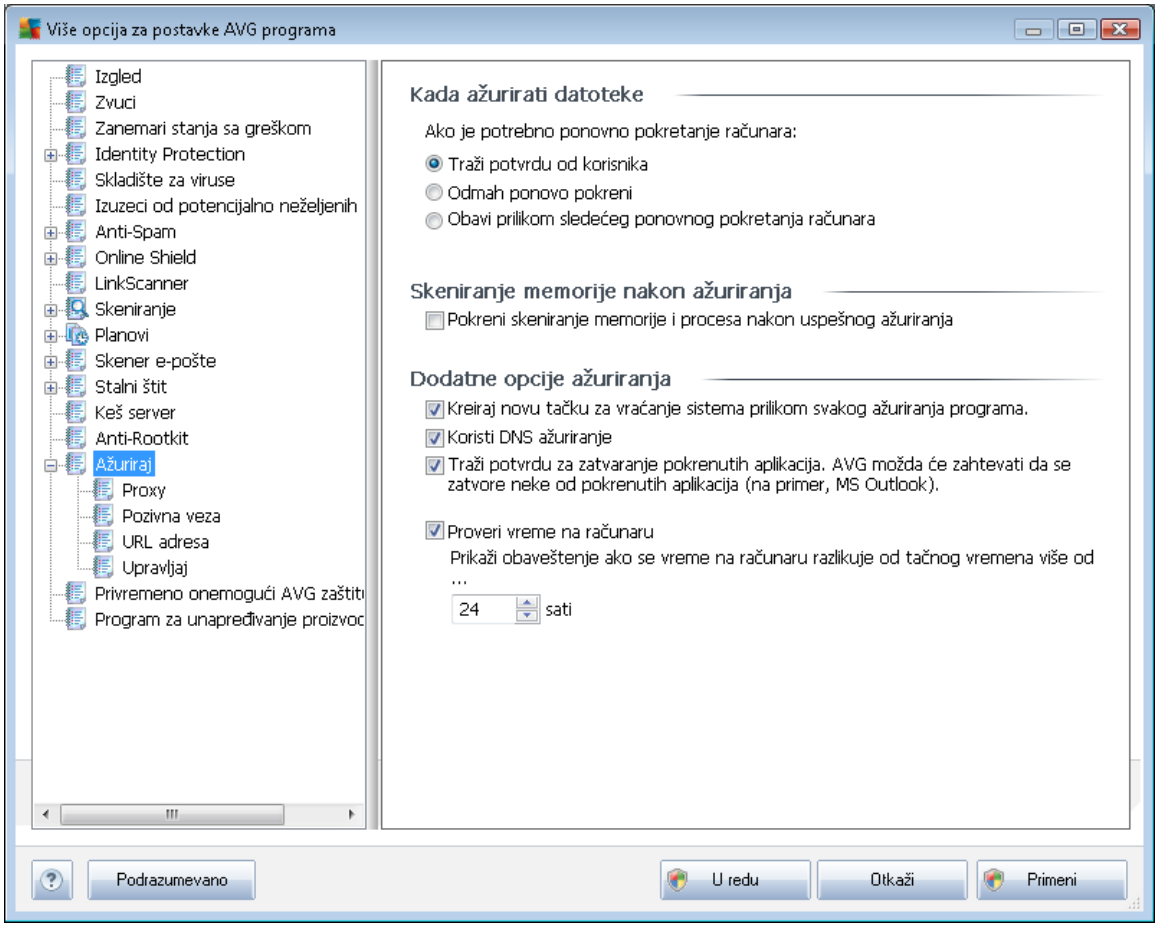
- ***Skeniraj aplikacije***
- ***Skeniraj DLL biblioteke***
- ***Skeniraj upravljačke programe***

Zatim možete izabrati 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*)

9.16. 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:

- ***Traži potvrdu od korisnika*** *(podrazumevana opcija)* - od vas će se tražiti da odobrite ponovno pokretanje računara koje je potrebno da bi se proces ažuriranja dovršio
- ***Odmah ponovo pokreni*** - računar će se automatski ponovo pokrenuti nakon završetka procesa ažuriranja, a vaše odobrenje neće biti potrebno

- ***Obavi prilikom sledećeg ponovnog pokretanja računara*** - dovršavanje procesa ažuriranja biće odloženo 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

Potvrdite izbor u ovom polju za potvrdu ako želite da se novo skreniranje 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

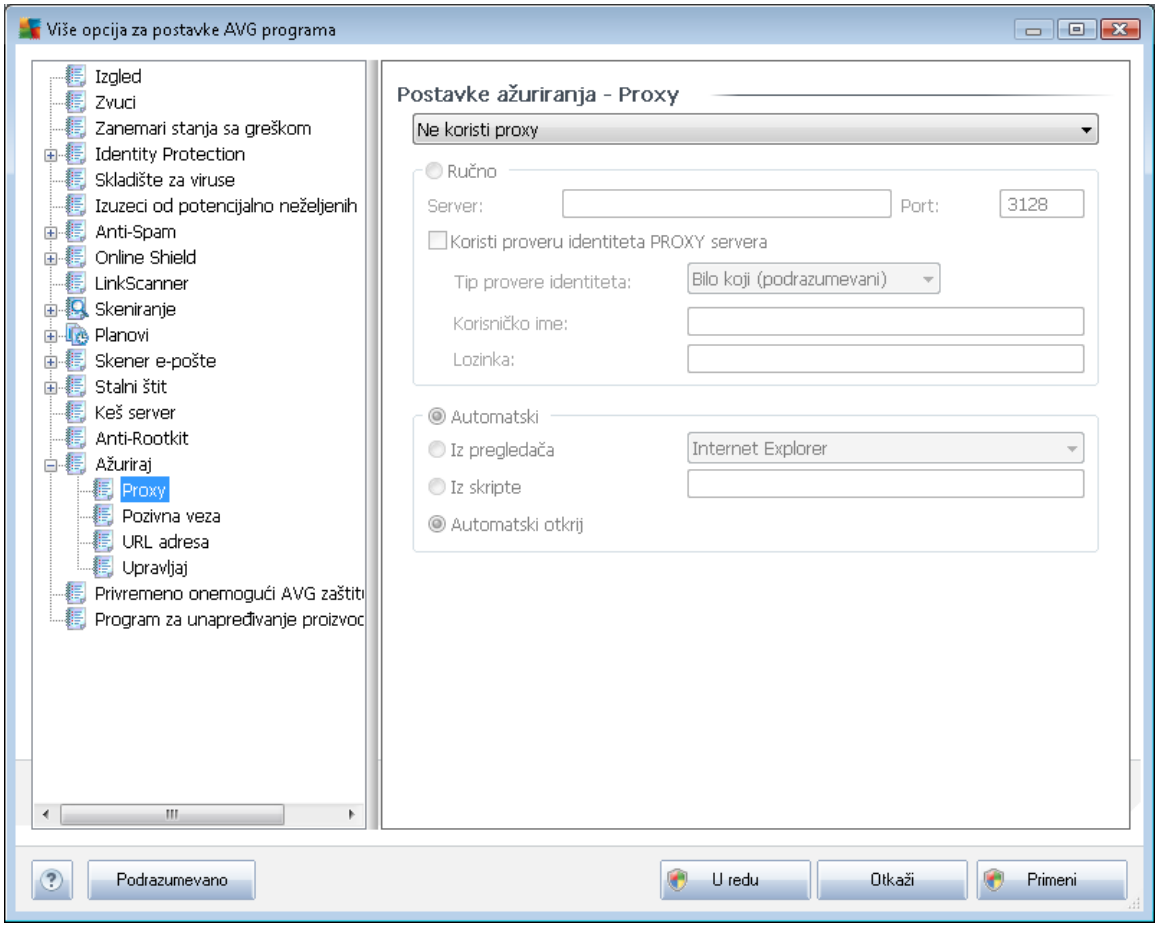
- ***Kreiraj novu tačku za vraćanje sistema nakon svakog ažuriranja programa*** - pre svakog pokretanja ažuiriranja programa AVG, kreira se tačka za vraćanje sistema. Ako proces ažuriranja ne uspe i dođe do pada operativnog sistema, možete ga uvek vratiti u stanje prvobitne konfiguracije. Ovoj opciji možete pristupiti ako kliknete na Start / Svi programi / Pribor / Sistemske alatke / 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 2011** 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.

9.16.1. 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 server*** - podrzumevano podešavanje
- ***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*)

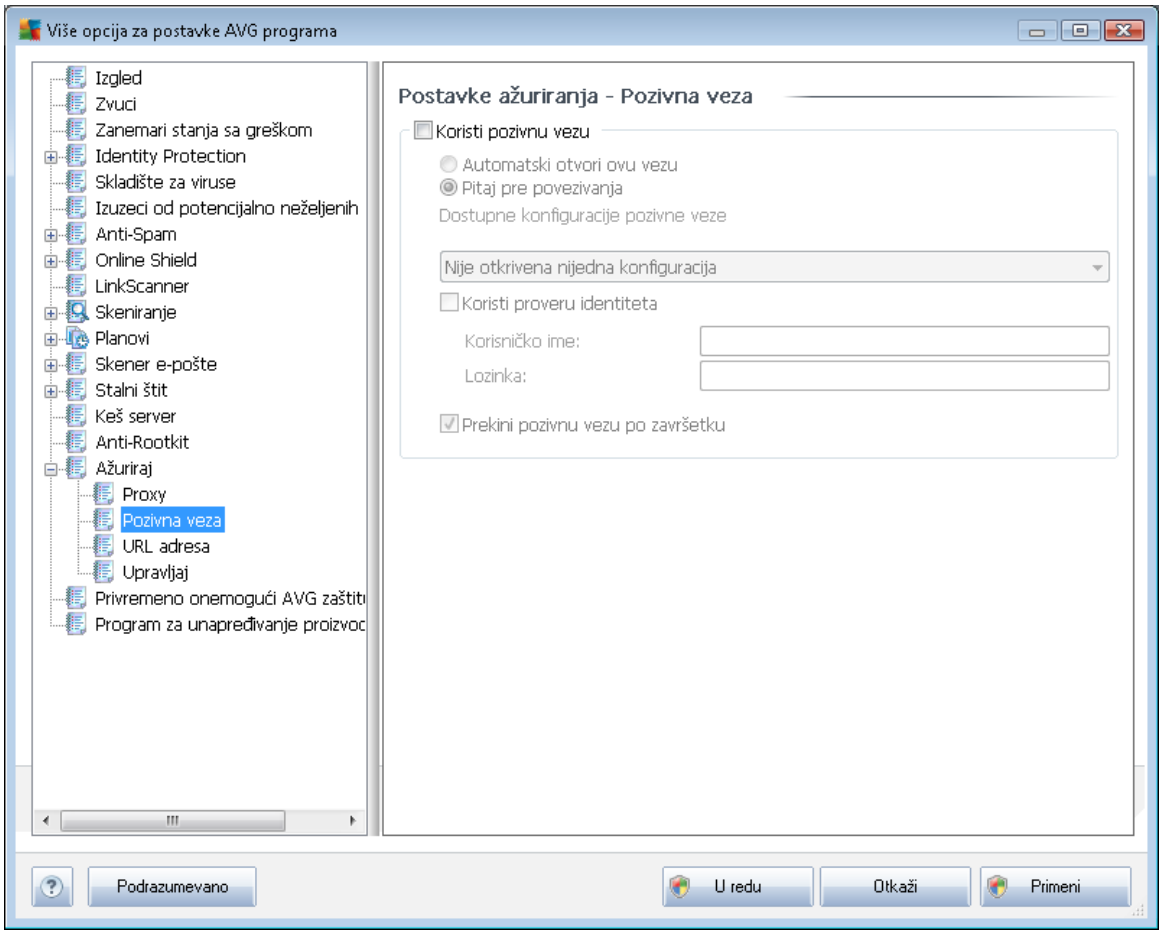
Proxy server takođe može da ima konfigurisana određena pravila za svakog korisnika. Ako je vaš proxy server podešen na ovaj način, uključite opciju ***Koristi proveru identiteta PROXY servera*** da biste proverili da li su vaše korisničko ime i lozinka važeći za povezivanje na Internet pomoću proxy servera.

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 skriprte koja sadrži funkciju davanja adrese proxy servera
- ***Automatski otkrij*** - konfiguracija će biti automatski otkrivena direktno sa proxy servera

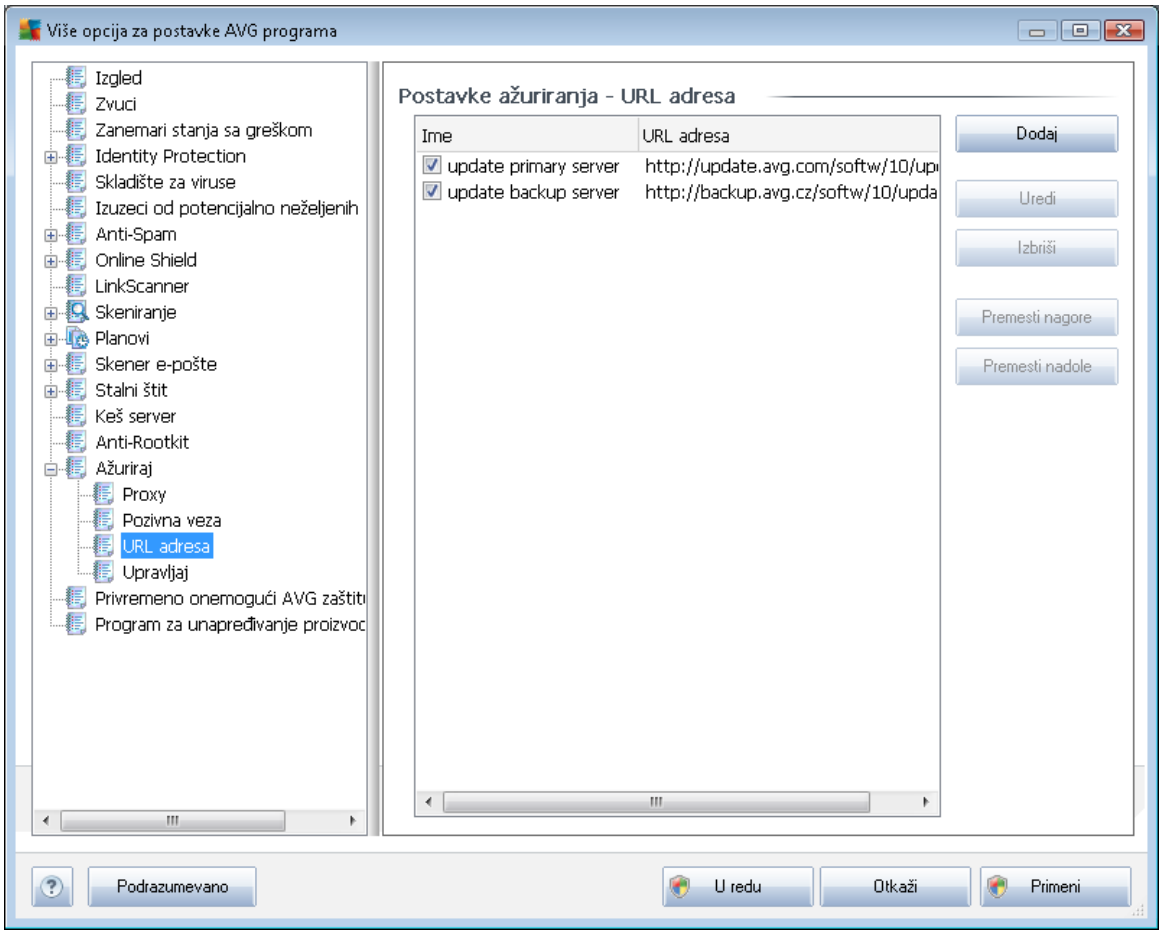
9.16.2. Pozivna veza



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***).

9.16.3. URL adresa

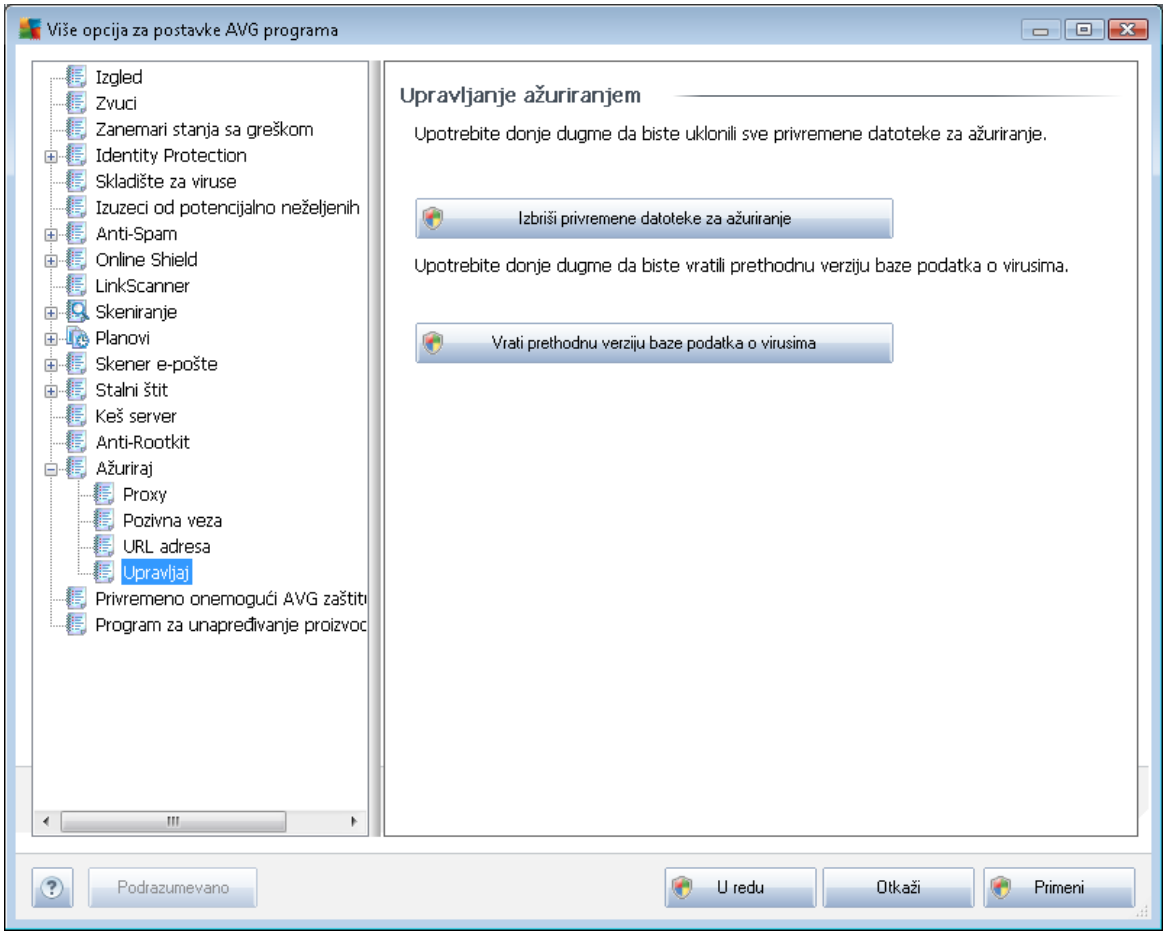


Dijalog ***URL adresa*** nudi listu Internet adresa sa kojih možete da preuzmete datoteke ispravki. Ova lista i njene stavke mogu se izmeniti pomoću sledeće kontrolne dugmadi:

- ***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

9.16.4. Upravljanje

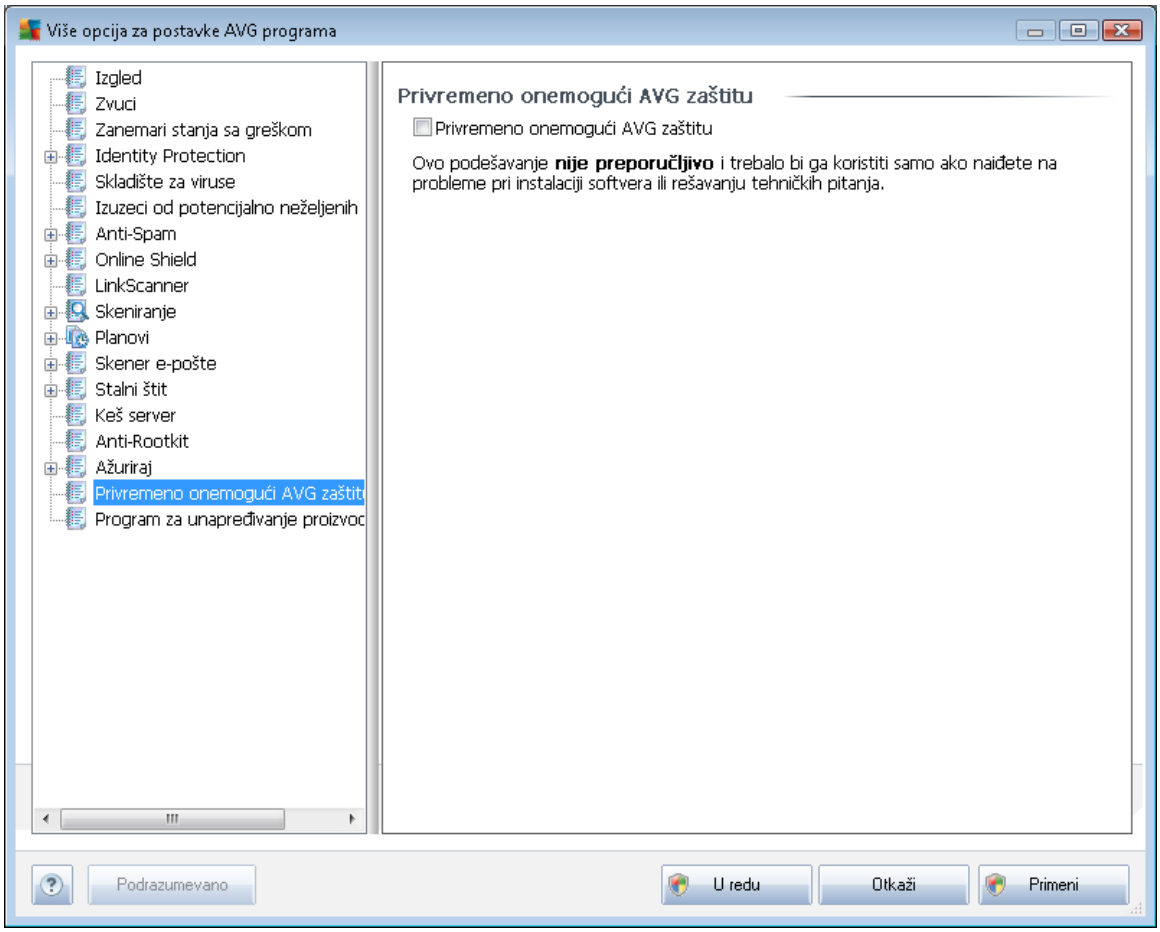
Dijalog ***Upravljaj*** nudi dve opcije kojima se pristupa pomoću dva dugmeta.



- ***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 podatka o virusima preuzeće se prilikom sledećeg ažuriranja*)

9.17. Privremeno onemogući AVG zaštitu



U dijalogu ***Privremeno onemogući AVG zaštitu***imate opciju isključivanja celokupne zaštite od strane vašeg**AVG Internet Security 2011** odjednom.

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

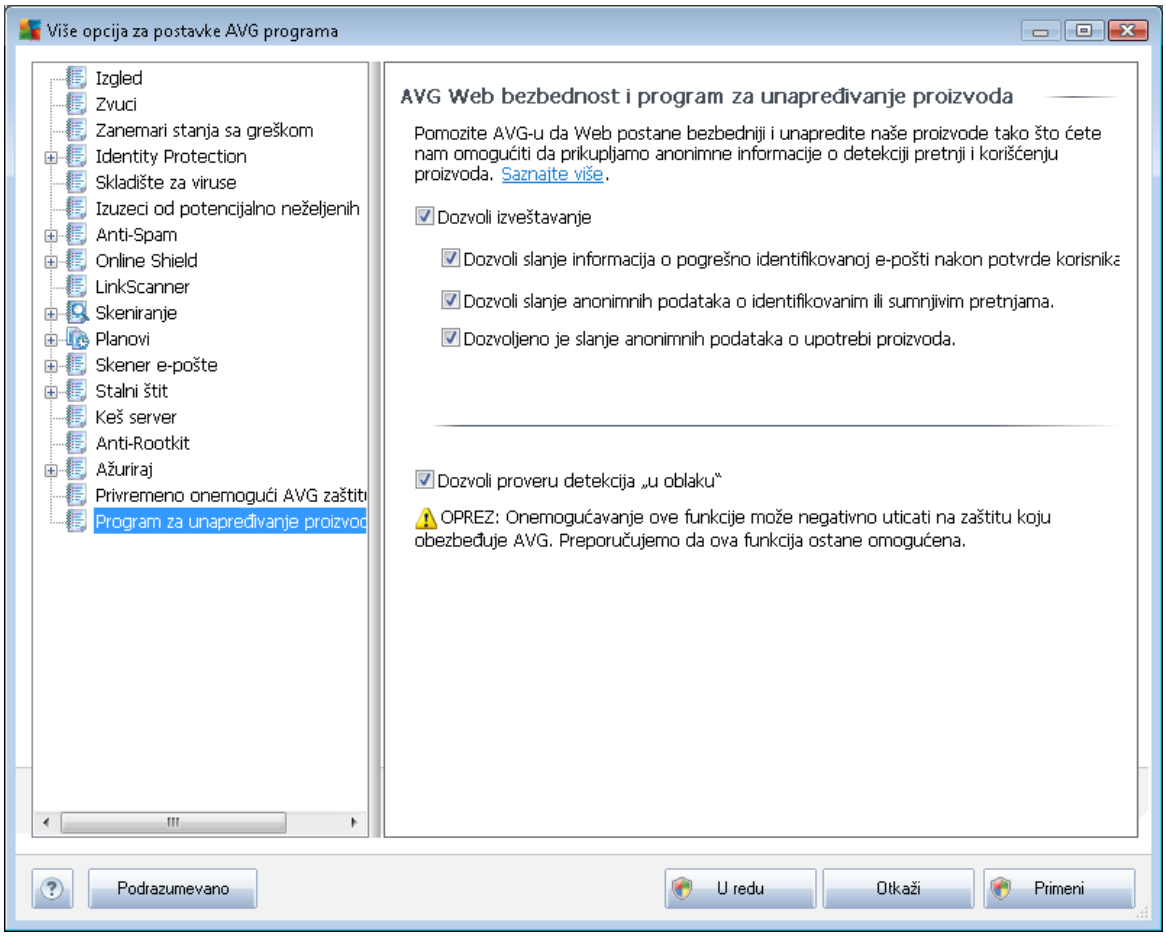
U većini slučajeva, neće biti ***neophodno*** da onemogućite AVG preinstalacije novog softvera ili upravljačkih programa, čak i ako instalator ili čarobnjak softvera predlažu da isključite pokrenute programe i aplikacije da ne bi ometale proces instalacije. Ako stvarno doživite problem tokom instalacije, pokušajte prvo da deaktivirate komponentu ***Stalni štit***. Ukoliko morate da privremeno onemogućite AVG, treba da ga omogućite odmah nakon završetka posla. Ukoliko ste povezani sa Internet ili mrežu tokom vremena u kojem je vaš antivirusni softver onemogućen, vaš računar je podložan napadima.

9.18. Program za unapređivanje proizvoda

Dijalog ***AVG web bezbednost i Program za unapređenje proizvoda*** vas poziva da učestvujete u unapređenju AVG proizvoda i da nam pomognete u podizanju nivoa opšte bezbednosti Interneta. Označite opciju***Dozvoli prijavljivanje***kako biste omogućili prijavljivanje detektovanih pretnji AVG centru. To nam omogućava da prikupljamo ažurirane informacije o najnovijim pretnjama od svih

korisnika širom sveta, kako bismo unapredili zaštitu svih korisnika.

Izveštavanje se obavlja automatski, pa vam neće predstavljati teret, a u izveštajima nema ličnih podataka. Iako je izveštavanje o detektovanim pretnjama opciono, molimo vas da i ova funkcija bude uključena, pošto nam pomaže da poboljšamo zaštitu za vas i sve druge AVG korisnike.



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 velika većina je 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.

- ***Crvi*** predstavljaju potkategoriju virusa kojima, za razliku od običnih virusa, nije potreban „prenosilac" - objekat za koje se moraju prikačiti; oni se sami šalju na druge računare, obično e-poštom, pa često izazivaju preopterećenje servera e-pošte i mrežnih sistema.

- ***Špijunski softver***se obično definiše kao vrsta malvera (*malver = bilo kakav zlonameran 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 opsan po vaš računar. Konkretan primer Potencijalno neželjenog programa je adver, 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 „roditeljskoj" 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 vrsta pretnji, AVG sadrži sledeće specijalizovane komponente:

- ***Antivirusni program*** za zaštitu vašeg računara od virusa,

- ***Antispajver program*** za zaštitu vašeg računara od špijunskog softvera,

- ***Online Shiled*** za zaštitu od virusa i špijunskog softvera dok pregledate Internet,

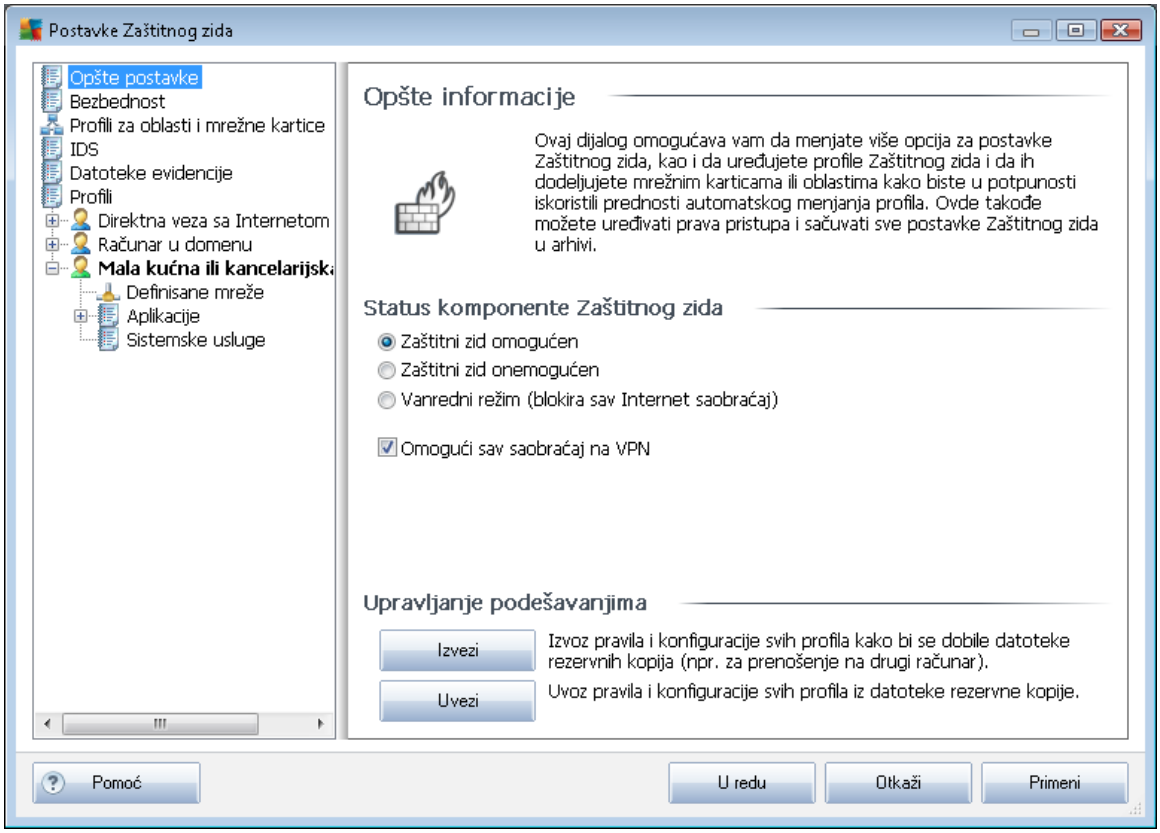
- ***LinkScanner*** vas štiti od ostalih pretnji na mreži pomenutih u ovom poglavlju.

10. 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, uređivanje naprednih podešavanja namenjeno je isključivo stručnjacima i iskusnim korisnicima.***

10.1. 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 omogući komunikaciju aplikacijama koje su označene kao „dozvoljene“ u skupu pravila definisanih za izabrani profil ***zaštitnog zida***
- ***Zaštitni zid onemogućen*** – ova opcija potpuno isključuje ***Zaštitni zid***, pa je sav mrežni saobraćaj dozvoljen, ali se ne proverava!
- ***Vanredni 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

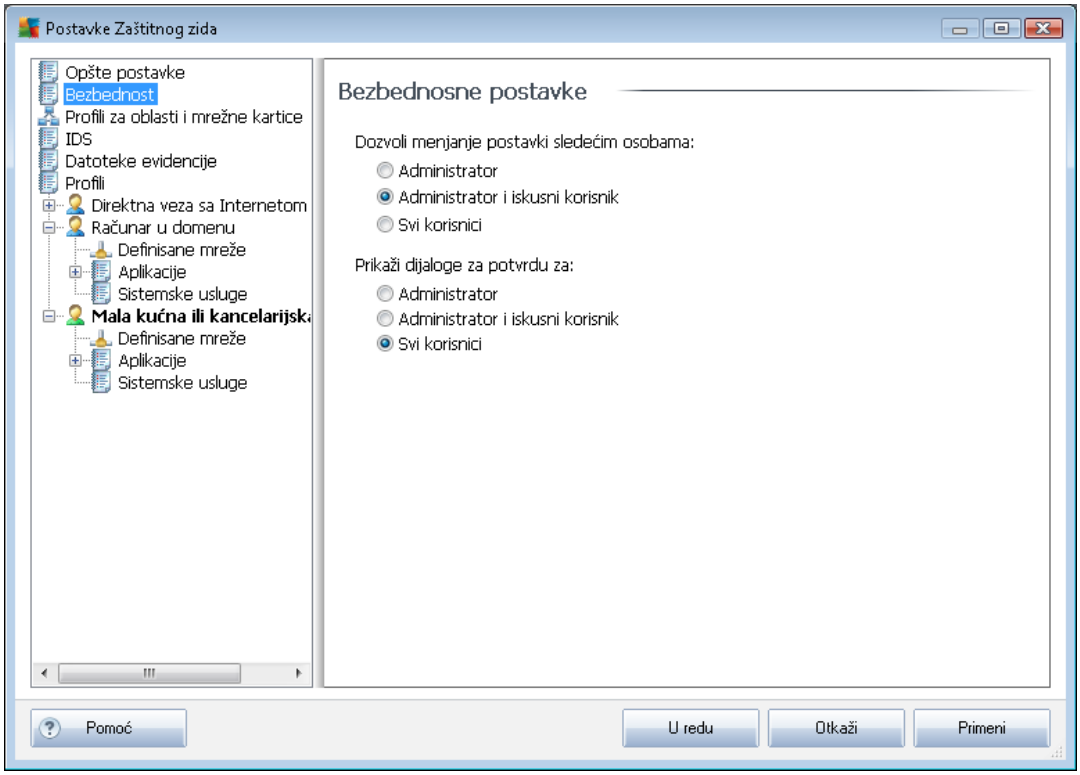
- ***Omogući sav saobraćaj na VPN*** – ako koristite VPN *(virtuelna privatna mreža)* vezu, npr. za povezivanje sa kancelarijskom mrežom od kuće, preporučujemo da označite ovo polje. ***AVG Zaštitni zid*** će automatski pretražiti vaše mrežne adaptere, pronaći one koji se koriste za VPN vezu i dozvoliti 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*** / ***uvezete konfiguraciju komponente*** ***Zaštitni zid***; npr. da izvezete definisana pravila i postavke komponente ***Zaštitni zid*** u datoteke za rezervne kopije ili da uvezete celu datoteku za rezervnu kopiju.

10.2. Bezbednost



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

- ***Dozvoli menjanje postavki sledećim osobama*** - navedite kome je dozvoljeno da menja konfiguraciju komponente ***Zaštitni zid***.

- ***Prikaži dijalog za potvrdu za*** - navedite kome će se prikazivati dijalozi za potvrdu (*dijalozi koji od vas traže da odlučite ako situacija nije pokrivena pravilima komponente* ***Zaštitni zid***)

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

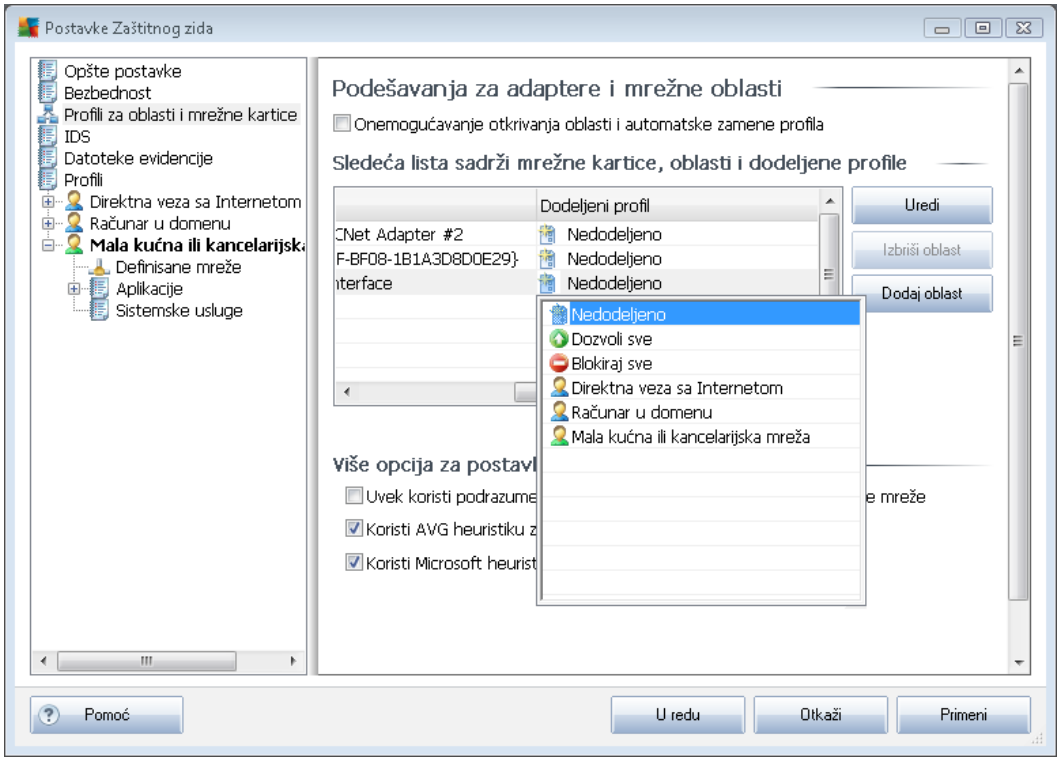
- ***Administrator*** – u potpunosti kontroliše računar i ima pravo da svakog korisnika dodeli grupi sa posebno definisanim ovlašćenjima

- ***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

10.3. Profili za oblasti i adaptere

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



- ***Onemogući otkrivanje oblasti i automatsku zamenu profila*** - neki 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 ***Onemogući otkrivanje oblasti i automatsku zamenu profila***.

- ***Lista adaptera, oblasti i dodeljenih profila*** - na ovoj listi se nalazi pregled detektovanih adaptera i oblasti. Svakoj od ovih stavki možete dodeliti određeni profil iz menija definisanih profila. Da biste otvorili ovaj meni, kliknite na odgovarajuću stavku sa liste adaptera i izaberite željeni profil.

Napredna podešavanja

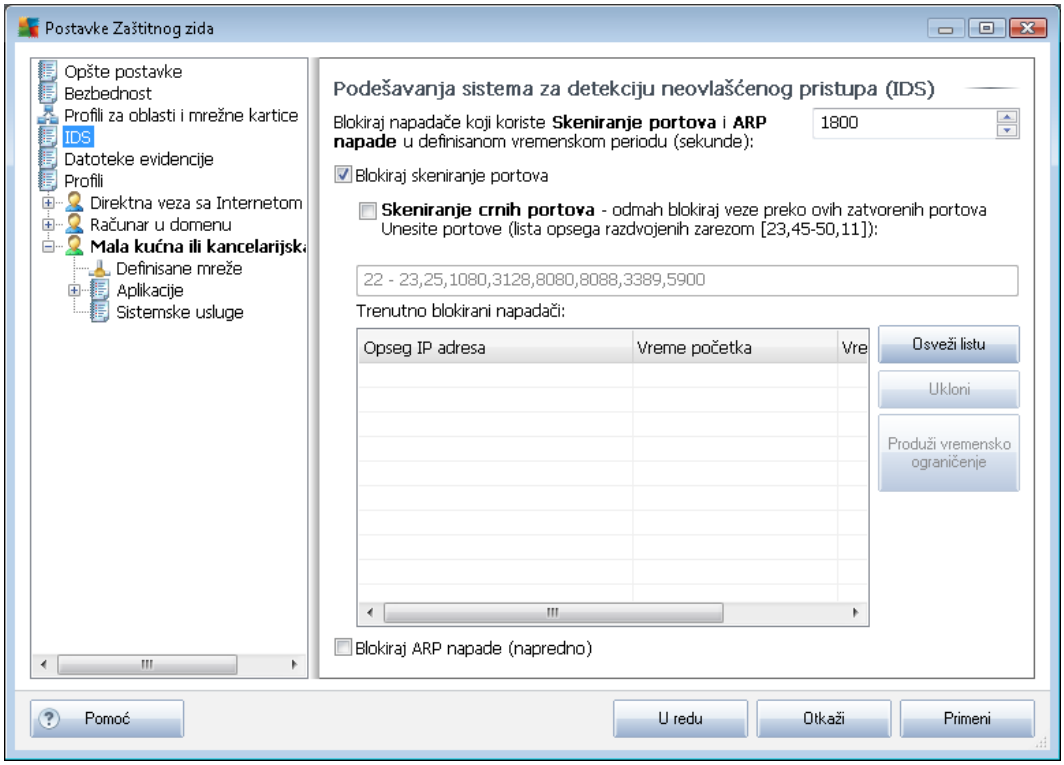
- ***Uvek koristi podrazumevani profil i ne prikazuj dijalog o detekciji nove mreže*** - kad god se vaš računar poveže na novu mrežu, ***Zaštitni zid*** će vas obavestiti i prikazati dijalog u kojem se od vas traži da izaberete tip mrežne veze, kao i da joj dodelite***Profil zaštitnog zida***. Ako ne 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 novoj otkrivenoj mreži iz Windows usluge (*ova opcija je dostupna samo u operativnom sistemu Windows Vista i novijim verzijama*).

10.4. 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. Možete konfigurisati parametre Sistema za detekciju neovlašćenog pristupa u okviru sledećeg interfejsa:



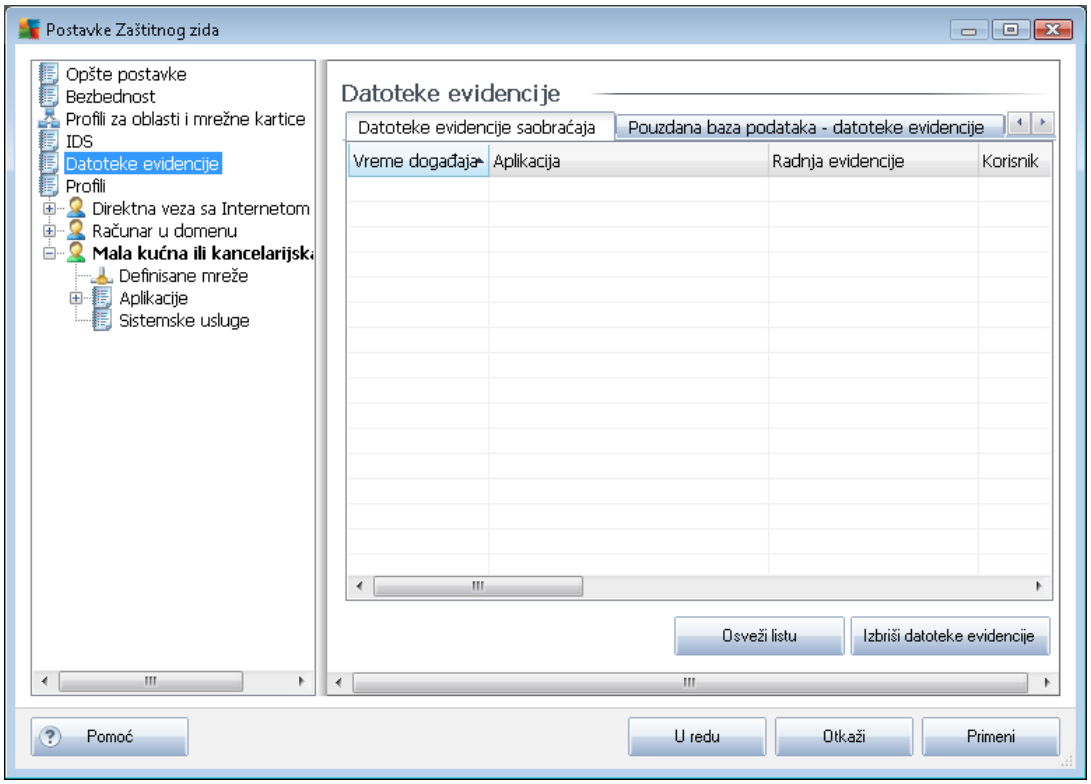
Dijalog ***Podešavanja sistema za detekciju neovlašćenog pristupa*** nudi sledeće opcije za konfiguraciju:

- ***Blokiraj napadače u definisanom vremenskom periodu*** - ovde možete odrediti koliko će sekundi port biti blokiran, kada se na njemu detektuje sumnjiv pokušaj komunikacije. Podrazumevano, vremenski interval je podešen na 1800 sekundi (*30 minuta*).
- ***Blokiraj skeniranje portova*** – označite ovo polje da biste blokirali spoljne pokušaje komunikacije na svim TCP i UDP portovima na računaru. U slučaju takvih veza, dozvoljeno je pet pokušaja, dok će šesti pokušaj biti blokiran.
    - ***Skeniranje crnih portova*** – označite ovo polje da biste smesta blokirali sve pokušaje komunikacije preko portova navedenih u tekstualnom polju 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***. Punu istoriju blokiranih pokušaja možete pogledati u dijalogu ***Evidencije*** (*kartica Evidencija skeniranja portova*).
- ***Blokiraj ARP napade*** aktivira blokiranje posebnih vidova pokušaja komunikacije u okviru lokalne mreže koje detektuje ***IDS*** 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.

10.5. 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 certifikovanim 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.

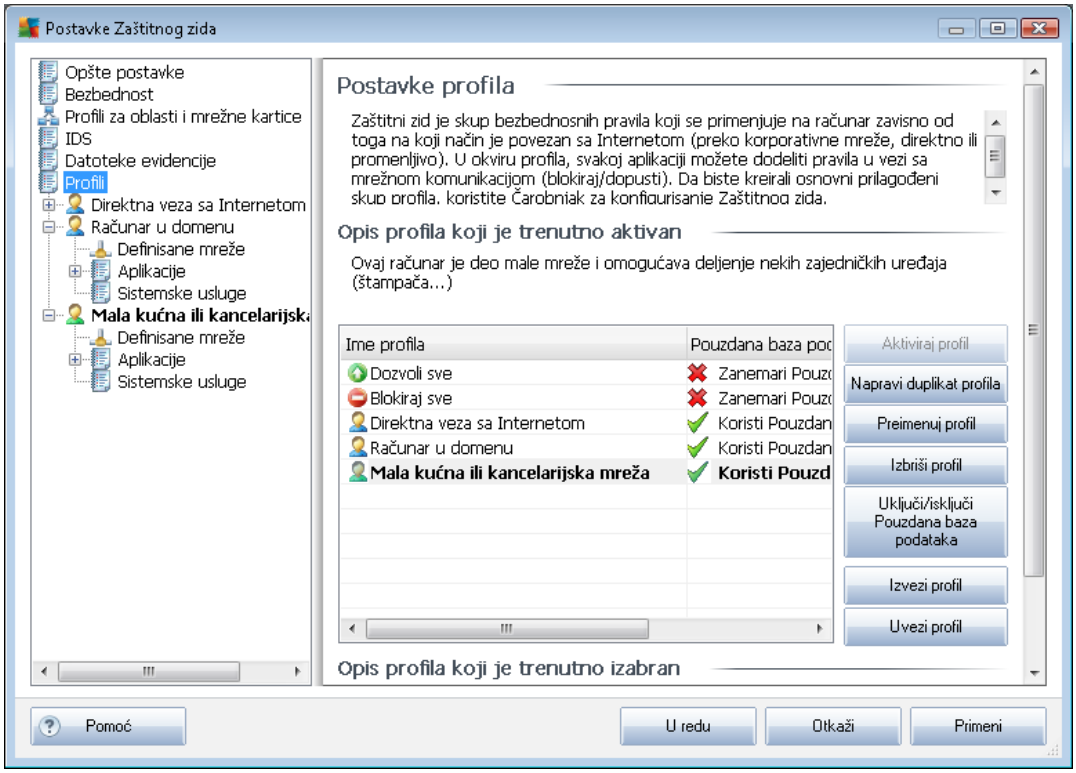
Kontrolna dugmad

- ***Osveži listu*** – svi evidentirani parametri mogu se rasporediti prema izabranom atributu: hronološki (*datumi*) ili po abecednom redosledu (*ostale kolone*) – dovoljno je da kliknete na zaglavlje odgovarajuće kolone. Upotrebite dugme ***Osveži listu*** da biste ažurirali informacije koje se trenutno prikazuju.

- ***Isprazni listu*** – brisanje svih stavki na grafikonu.

10.6. Profili

U dijalogu ***Podešavanja profila*** nalazi se lista svih dostupnih profila.



Ostale profile, osim sistemskih, možete urediti direktno u ovom dijalogu pomoću sledeće kontrolne dugmadi:

- ***Aktiviraj profil*** - ovo dugme postavlja izabrani profil za aktivan, što znači da će konfiguraciju izabranog profila ***Zaštitni zid*** koristiti za kontrolu mrežnog saobraćaja.
- ***Napravi duplikat profila*** - kreiranje identične kopije izabranog profila, koju zatim možete urediti i preimenovati kako biste kreirali novi profil zasnovan na duplikatu originalnog.
- ***Preimenuj profil*** - omogućava vam da definišete novo ime izabranog profila
- ***Izbriši profil*** - briše izabrani profil sa liste
- ***Uključi/isključi pouzdanu bazu podataka*** - za izabrani profil možete odlučiti da koristite informacije *pouzdane baze podataka*(*Pouzdana baza podataka je interna AVG baza podataka u kojoj se prikupljaju podaci o pouzdanim i sertifikovanim aplikacijama kojima uvek možete dozvoliti komunikaciju na mreži.*)
- ***Izvezi profil*** - upisuje konfiguraciju izabranog profila u datoteku koja se zatim čuva za potencijalnu buduću upotrebu
- ***Uvezi profil*** - konfigurisanje podešavanja izabranog profila na osnovu podataka izvezenih iz rezervne kopije datoteke za konfiguraciju

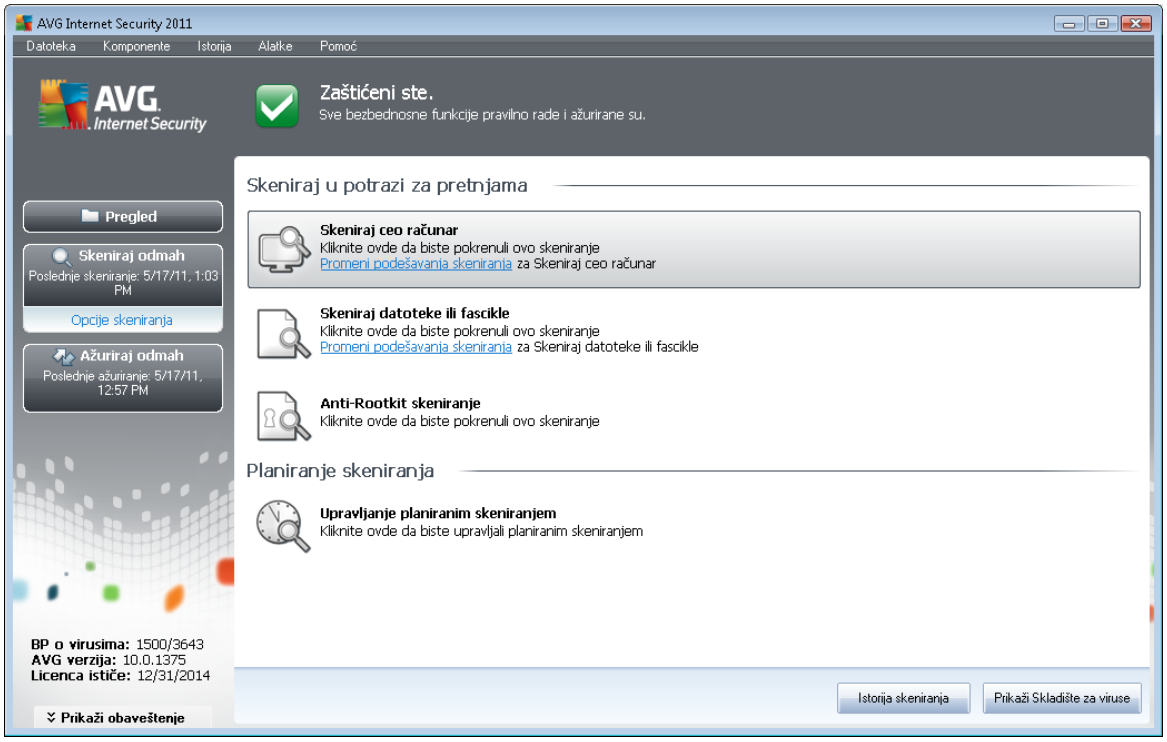
U donjem delu dijaloga nalazi se opis profila koji je trenutno izabran na gornjoj listi.

U zavisnosti od broja definisanih profila na listi u dijalogu ***Profil***, menjaće se i strukura 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. Skeniranje programom AVG

Skeniranje je ključni deo funkcionalnosti programa **AVG Internet Security 2011**. Možete da pokrenete testove na zahtev ili da planirate da se periodično pokreću u vreme koje vam odgovara.

11.1. 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***
  - ***Anti-Rootkit skeniranje***
- odeljak planiranje skeniranja - u kojem možete definisati nove testove i po potrebi 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.

11.2. Unapred definisana skeniranja

Jedna od glavnih funkcija programa **AVG Internet Security 2011** 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.

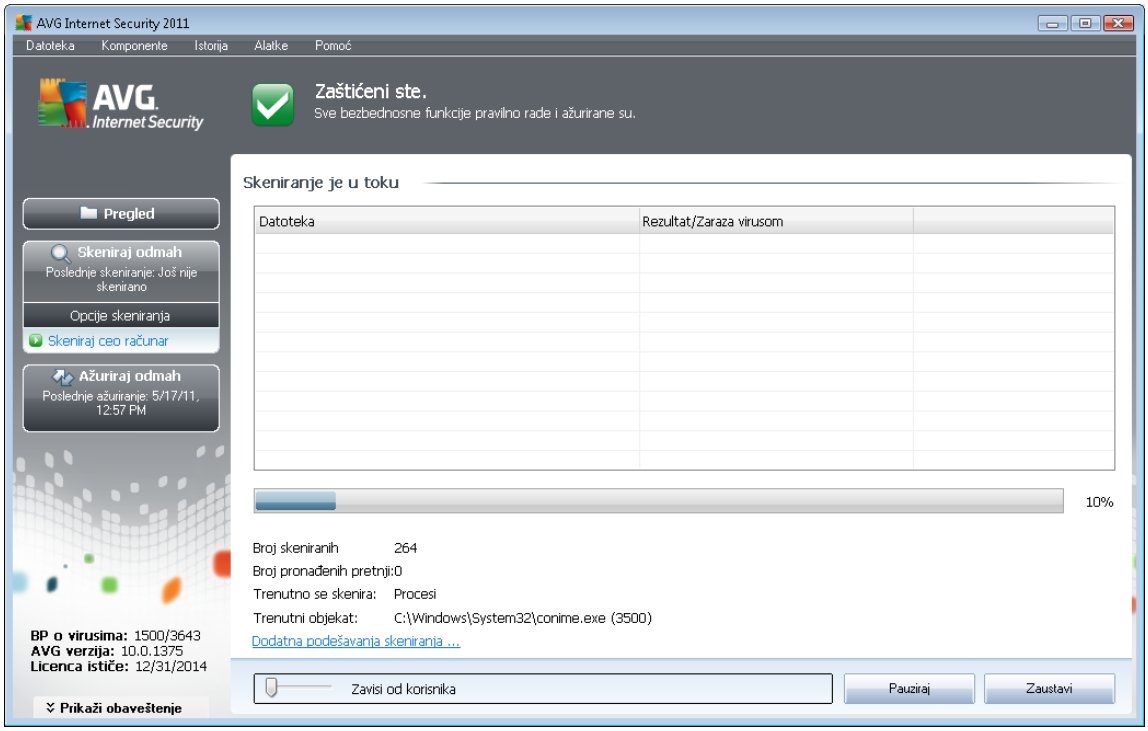
U **AVG Internet Security 2011** naći ćete dve vrste skeniranja koje je unapred definisao distributer softvera:

11.2.1. 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.

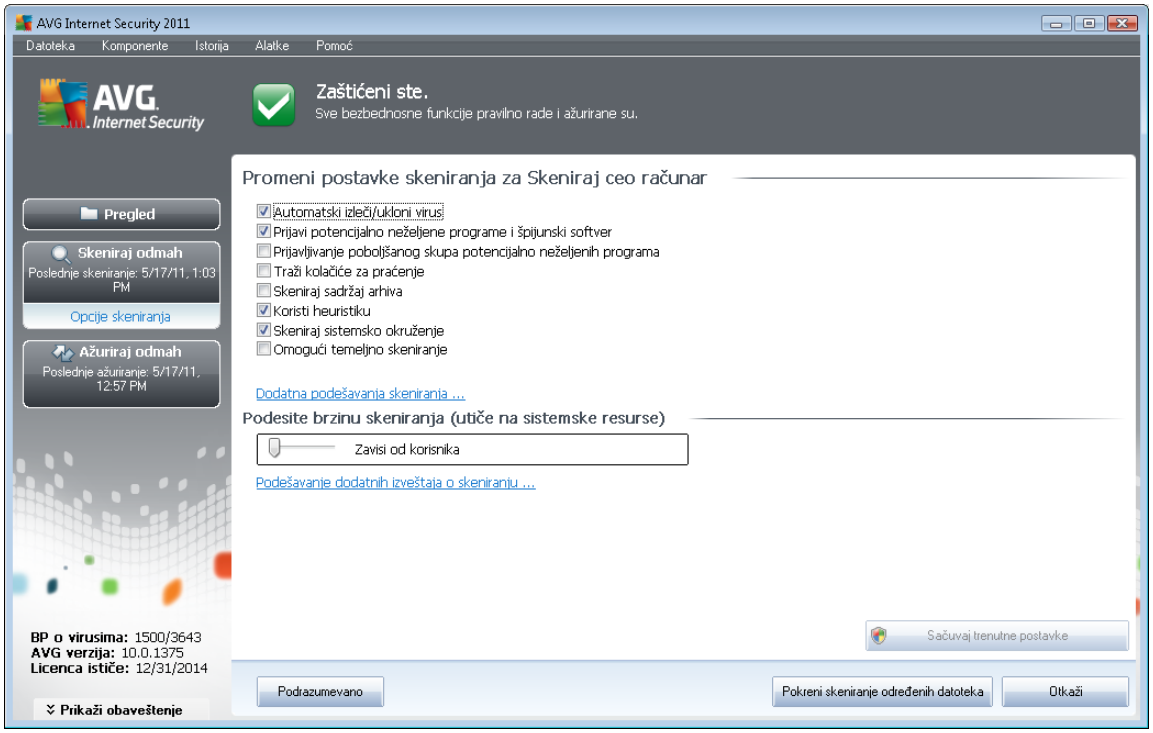
Pokretanje skeniranja

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 zaSkeniranje 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:

  - ***Automatski izleči/ukloni infekciju*** (*podrazumevano uključeno*) - ako tokom skeniranja bude otkriven virus, moguće ga je automatski oporaviti, 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*) - potvrdite radi detekcije proširenog paketaŠpijunskih 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*)*.

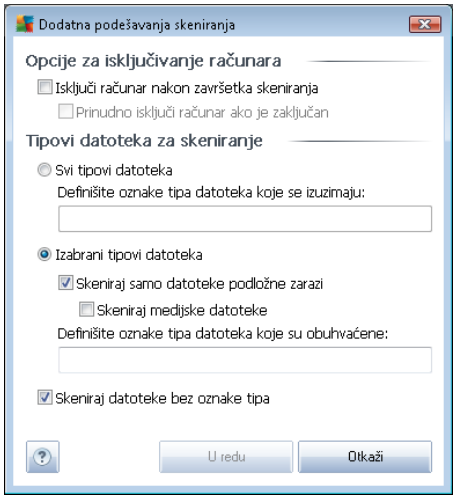
- **Skeniraj sadržaj arhiva** (*podrazumevano isključeno*) - ovaj parametar definiše da bi tokom skeniranja trebalo proveravati sve datoteke koje se nalaze unutar arhiva, npr. ZIP, RAR, ...

- **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 je ovaj metod prilično traje dugo.

- ***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***).

- **Definišite tipove datoteka za skeniranje** - odlučite da li želite da skenirate:

  - ***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;

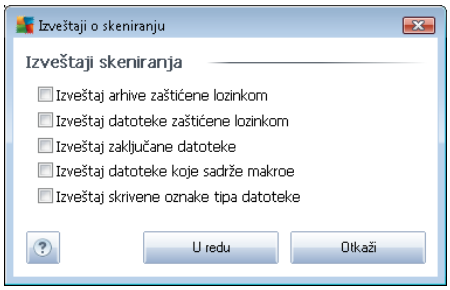
  - ***Izabrane tipove datoteka*** - možete izabrati da skenirate samo datoteke za koje

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.*

11.2.2. Skeniraj određene datoteke ili fascikle

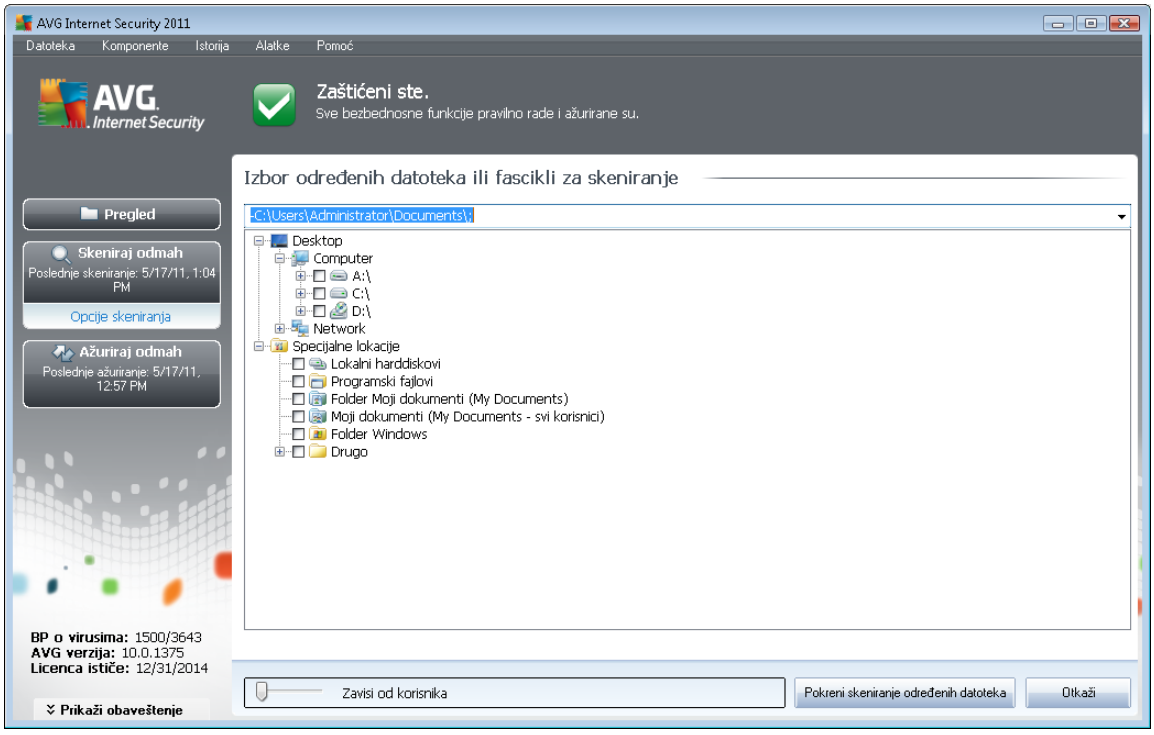
Skeniraj određene datoteke ili fascikle - skeniranje samo onih oblasti računara koje ste izabrali za skeniranje (*izabrane fascikle, čvrsti diskovi, diskete, kompakt diskovi itd.*). Tok skeniranja u slučaju detekcije virusa i tretiranje virusa isti su kao kod skeniranja celog računara: pronađeni virusi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

Pokretanje skeniranja

Skeniranje određenih 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 pojaviće se u polju za tekst u gornjem delu ovog dijaloga.

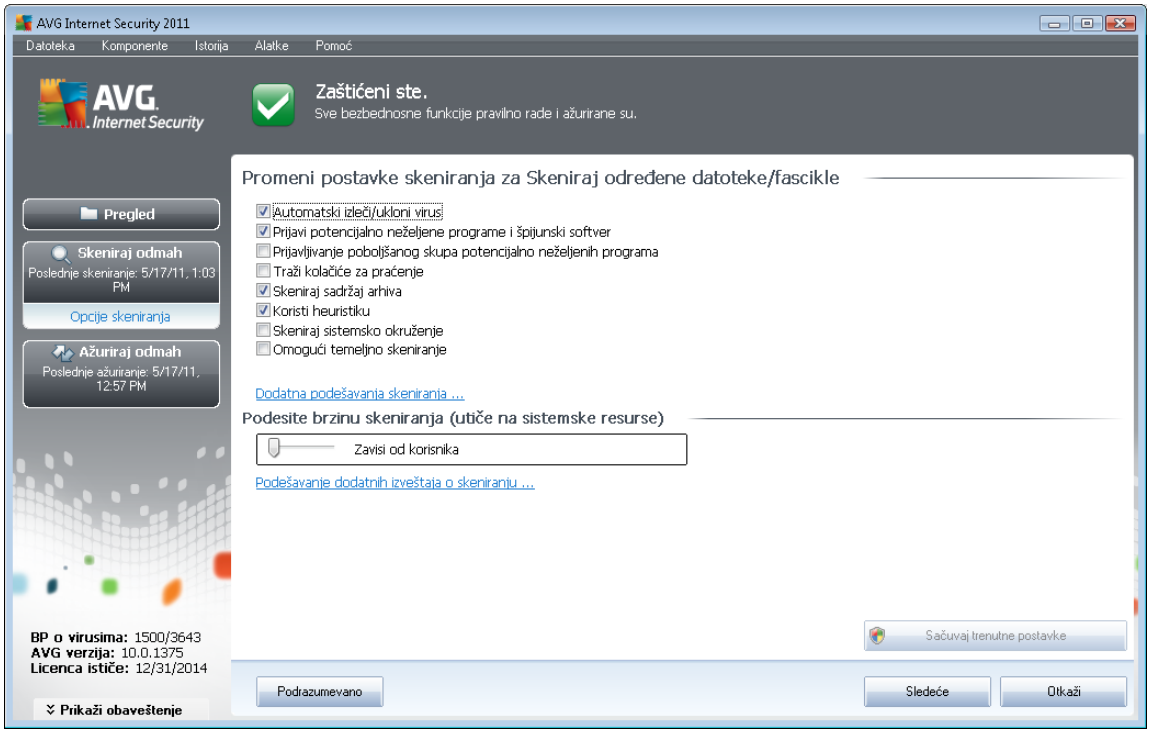
Takođe postoji mogućnost skeniranja određene fascikle, ali ne i njenih podfascikli; da biste to učinili, unesite znak minus „**-**“ ispred automatski generisane putanje (*vidi snimak ekrana*). Da biste celu fasciklu izuzeli iz skeniranja, koristite „**!**“ parametar.

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 određenih datoteka ili fascikli***. Pritisnite link ***Promeni podešavanja skeniranja*** da biste otvorili dijalog ***Promeni podešavanja skeniranja za Skeniranje određenih 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:

  - ***Automatski izleči/ukloni infekciju*** (*podrazumevano uključeno*) - ako tokom skeniranja bude otkriven virus, moguće ga je automatski oporaviti, 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*) - potvrdite radi detekcije proširenog paketaŠpijunskih 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).

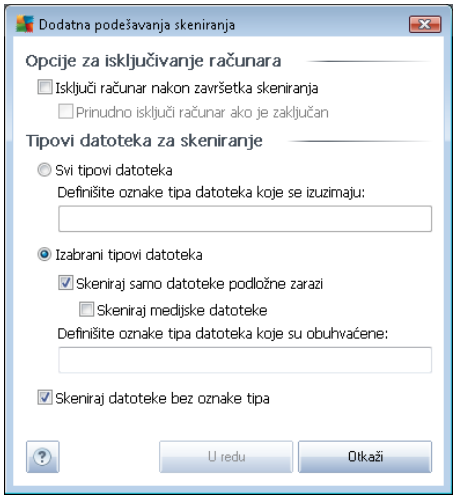
- **Skeniraj sadržaj arhiva** (*podrazumevano uključeno*) - ovaj parametar definiše da bi tokom skeniranja trebalo proveravati sve datoteke, pa čak i one koje se nalaze unutar arhiva, npr. ZIP, RAR, ...

- **Koristi heuristiku** (*podrazumevano isključeno*) - 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***).

- **Definišite tipove datoteka za skeniranje** - odlučite da li želite da skenirate:

  - ***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;

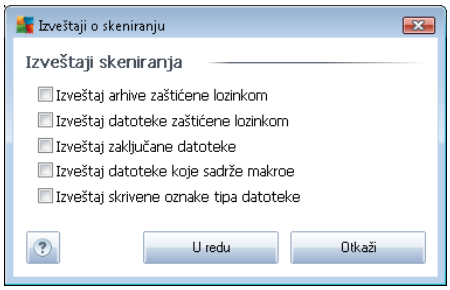
  - ***Izabrane tipove datoteka*** - možete izabrati da skenirate samo datoteke za koje

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:



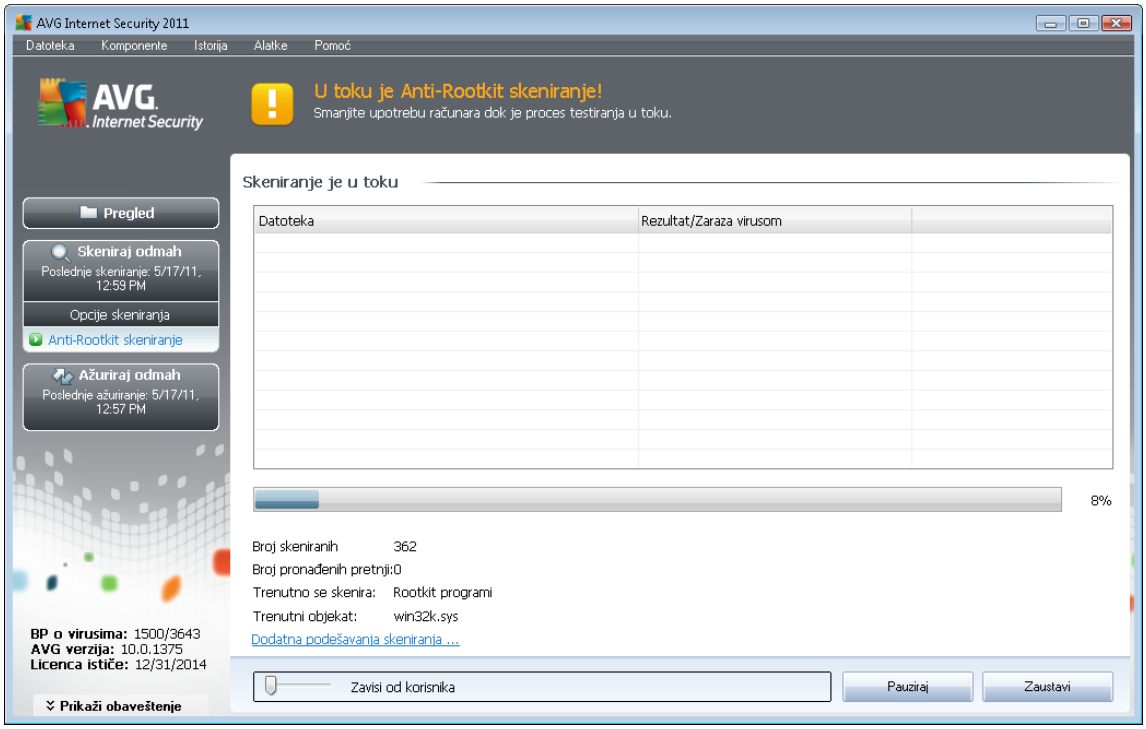
Upozorenje: *Ova podešavanja skeniranja ista su kao parametri najnovijeg definisanog skeniranja - kao što je opisano u poglavlju* ***AVG skeniranje / Planiranje skeniranja/ Kako skenirati****. Ako odlučite da izmenite podrazumevanu konfiguraciju opcije* ***Skeniraj određene datoteke ili fascikle*** *, nova podešavanja možete sačuvati kao podrazumevanu konfiguraciju koja će se koristiti za svako buduće skeniranje određenih 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 određenih datoteka ili fascikli).*

11.2.3. Anti-Rootkit skeniranje

Anti-Rootkit skeniranjem se pretražuje računar u potrazi za rootkit programima (*programi i tehnologije koje mogu da prikriju aktivnost zlonamernih softvera na vašem 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.

Pokretanje skeniranja

Anti-Rootkit skeniranje može se direktno pokrenuti iz interfejsa za skeniranje tako što ćete kliknuti na ikonu za skeniranje. 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.

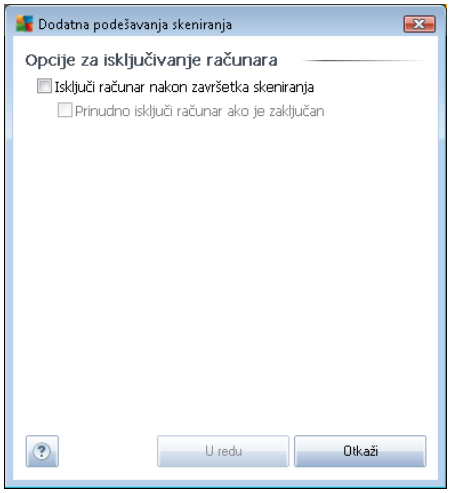


Uređivanje konfiguracije skeniranja

Anti-Rootkit skeniranje se uvek pokreće sa podrazumevanim postavkama, a uređivanje parametara skeniranja je moguće jedino u dijalogu ***AVG napredna podešavanja / Anti-Rootkit***. Sledeća konfiguracija je dostupna u interfejsu za skeniranje, ali samo dok je skeniranje u toku:

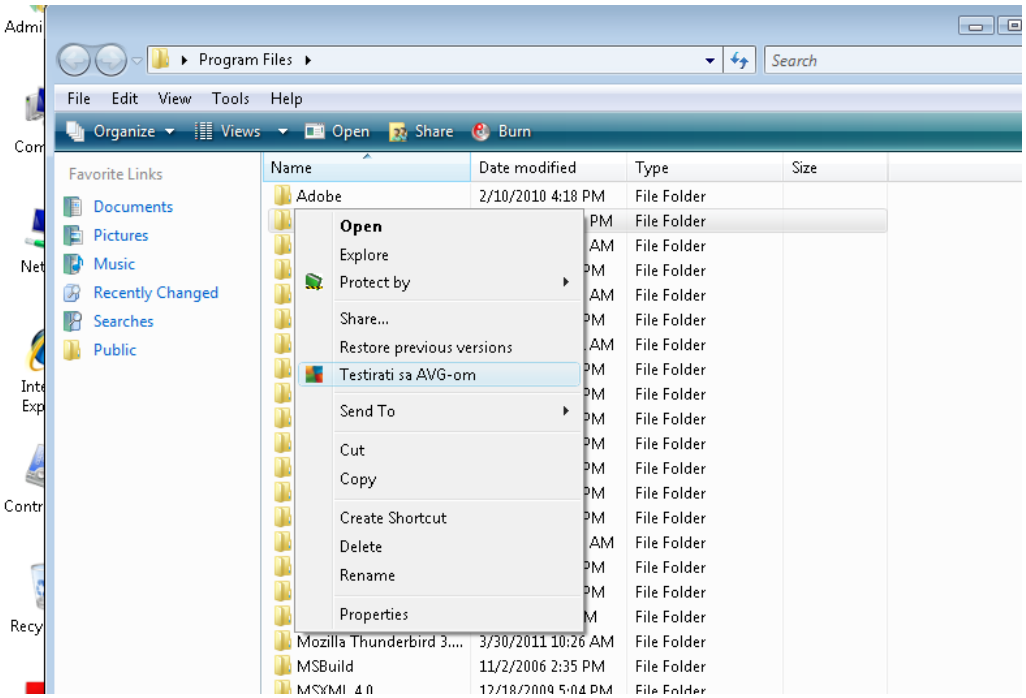
- ***Automatsko skeniranje*** - možete koristiti klizač kako biste promenili prioritet procesa skeniranja. Vrednost ove opcije podrazumevano je postavljena na nivo automatske zauzetosti resursa koja *zavisi od korisnika*. Takođe, proces skeniranja možete usporiti, što znači da će zauzetost sistemskih 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*).

- ***Dodatne postavke skeniranja*** - ovaj link otvara novi dijalog ***Dodatne postavke skeniranja*** u kojem možete da definišete moguće okolnosti za isključivanje računara u vezi sa ***Anti-Rootkit skeniranjem*** (***Isključi računar po završetku skeniranja*** *ili* ***Prinudno isključi računar ako je zaključan***):



11.3. Skeniranje u programu Windows Explorer

Pored unapred definisanog skeniranja celog računara ili izabranih oblasti na njemu, **AVG Internet Security 2011** 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 želeti da je skenirate na zahtev. Pratite sledeće korake:



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

11.4. Skeniranje komandne linije

U programu **AVG Internet Security 2011** 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 operativne sisteme
- ***avgscana*** za 64-bitne operativne 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 seređaju 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.

11.4.1. Parametri za skeniranje iz komandne linije

Sledi lista svih dostupnih parametara za skeniranje iz komandne linije:

- ***/SCAN*** Skeniranje određenih 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 arhive
- ***/CLEAN*** Automatski očisti
- ***/TRASH*** Premesti zaražene datoteke u Skladište za viruse
- ***/QT*** Brzi test
- ***/MACROW*** Prijavi makroe
- ***/PWDW*** Prijavi datoteke zaštićene lozinkom
- ***/IGNLOCKED*** Zanemari 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*** Izveštavanje o „Potencijalno neželjenim programima“
- ***/REG*** Skeniraj registrator
- ***/COO*** Skeniraj kolačiće
- ***/?*** Prikaži pomoć za ovu temu

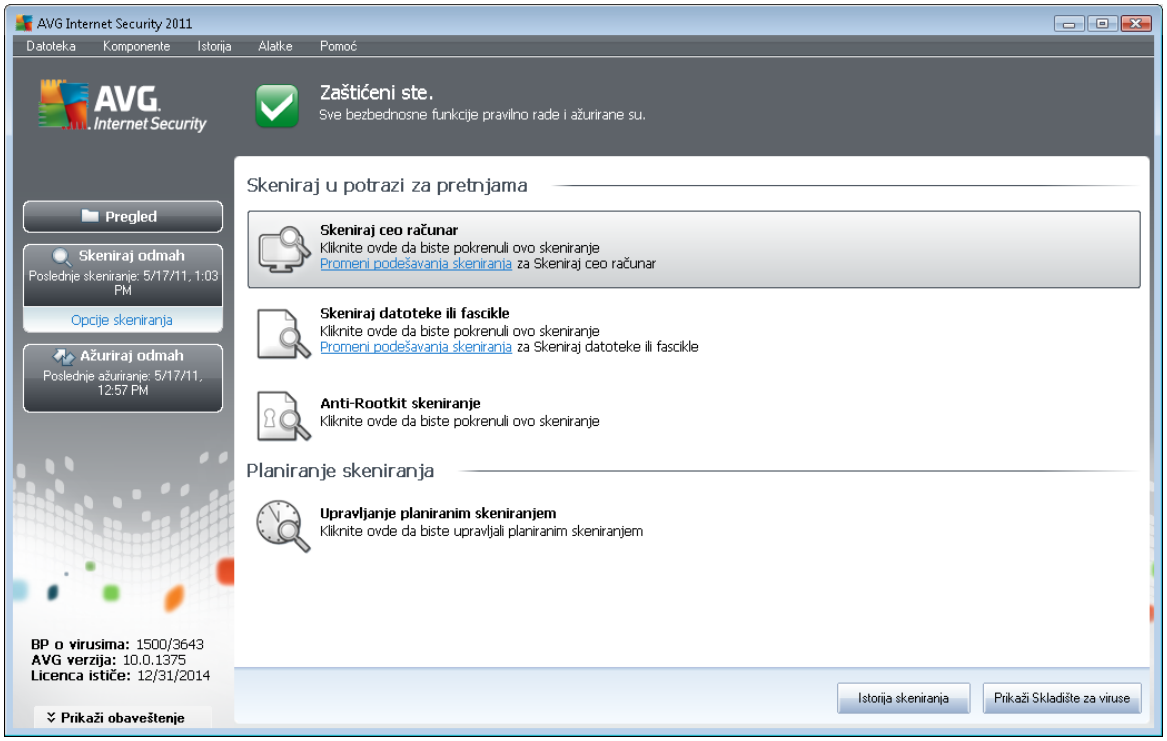
- ***/HELP*** Prikaži pomoć za ovu temu
- ***/PRIORITY*** Podešavanje prioriteta skeniranja /Nizak, automatski, visok/ (pogledajte Napredna podešavanja / Skeniranje)
- ***/SHUTDOWN*** Isključi računar nakon završetka skeniranja
- ***/FORCESHUTDOWN*** Prinudno isključi računar nakon završetka skeniranja
- ***/ADS*** Skeniraj alternativne tokove podataka (samo u NTFS sistemu)
- ***/ARCBOMBSW*** Prijavi ponovo zapakovane datoteke arhive

11.5. Planiranje skeniranja

Program **AVG Internet Security 2011** 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.

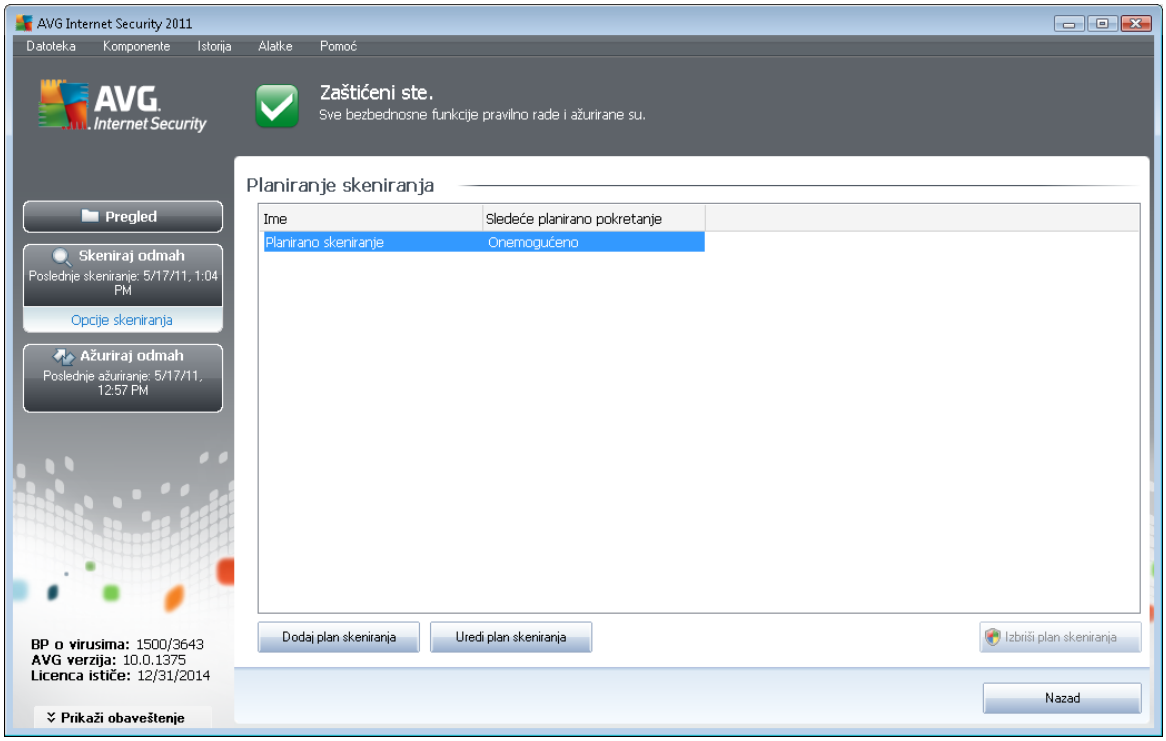
Trebalo bi redovno da pokrećete opciju ***Skeniraj ceo računar***, bar jednom nedeljno. Međutim, ako je moguće, pokrenite skeniranje celog računara jednom dnevno - kao što je podešeno u podrazumevanoj konfiguraciji plana za skeniranje. Ako računar držite stalno uključen, možete napraviti plan za skeniranje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

Da biste kreirali novi plan skeniranja, pogledajteAVG interfejs za skeniranje pa u donjem delu pronađite odeljak ***Plan skeniranja***:



Planiranje skeniranja

Kliknite na grafičku ikonu u odeljku ***Planiranje skeniranja*** da biste otvorili dijalog ***Planiranje skeniranja*** u kojem možete da vidite spisak 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.

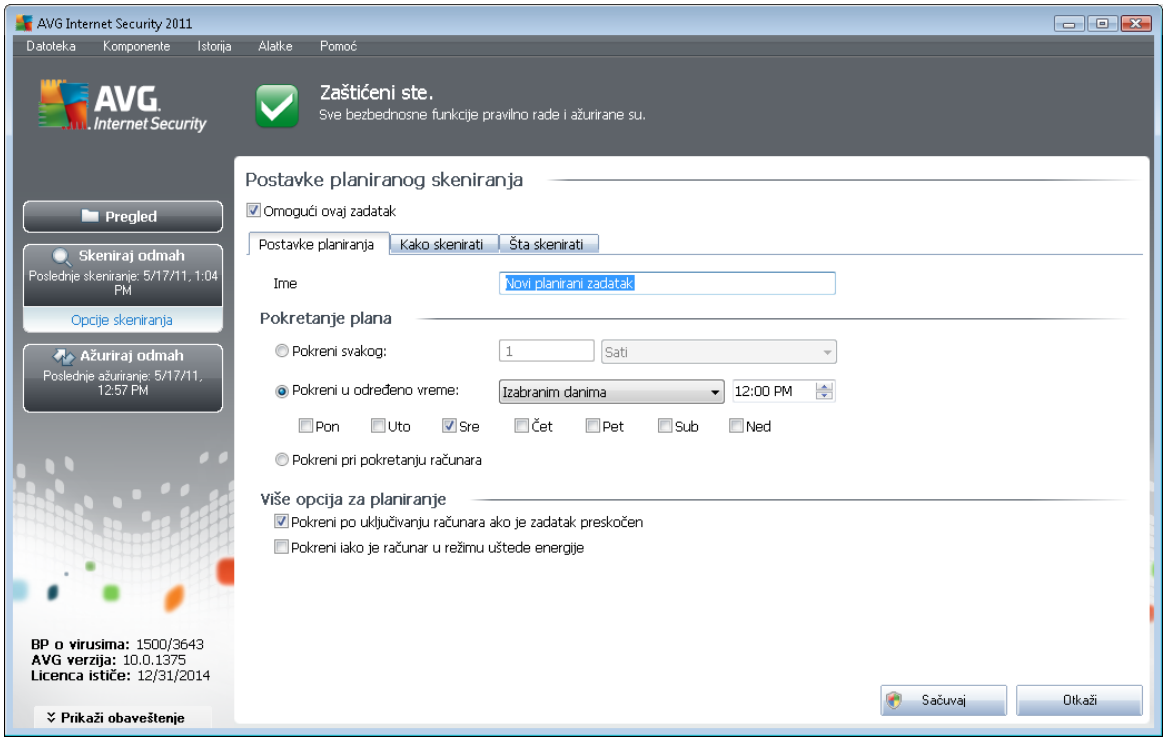
- ***Uredi plan skeniranja*** - ovo dugme možete koristiti samo ako ste prethodno izabrali postojeći test iz liste planiranih testova. U tom slučaju dugme će biti aktivno i moći ćete da kliknete na njega da biste da biste prešli na karticu ***Schedule settings*** u dijalogu ***Podešavanja za planiranje 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

11.5.1. 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***). Dijalog je podeljen na tri kartice: ***Podešavanja planiranja*** - *pogledajte sliku ispod*(*podrazumevana kartica koja će se automatski otvoriti*), ***Kako skenirati*** i ***Šta skenirati***.



Na kartici ***Podešavanja planiranja*** možete prvo označiti/poništiti 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.

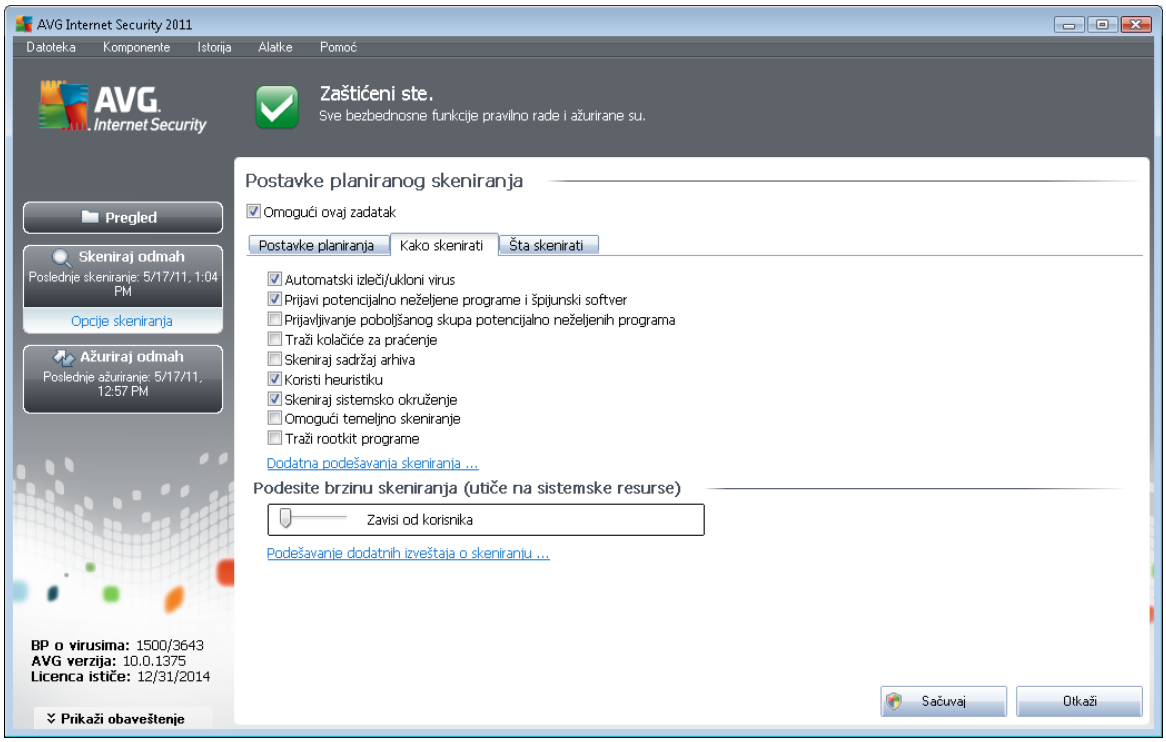
Kontrolna dugmad u dijalogu Podešavanja za planirano skeniranje

Dva kontrolna dugmeta dostupna su na svakoj od tri kartice u dijalogu ***Podešavanje planiranog skeniranja*** (***Podešavanje planiranja***, ***Kako skenirati*** i ***Šta skenirati***), a funkcionalnost im je ista bez obzira na to 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.

- ***Otkaži*** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na podrazumevani dijalog AVG interfejsa za skeniranje..

11.5.2. 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:

- ***Automatski izleči/ukloni infekciju*** (*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, ...

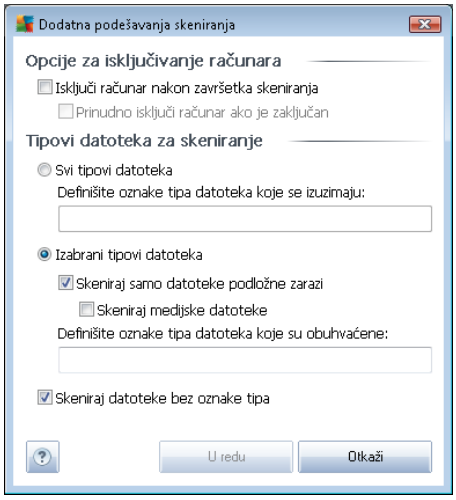
- ***Koristi heuristiku*** (*podrazumevano uključeno*): heuristička analiza (*dinamička emulacija naredbi skeniranih objekata u virtuelnom računarskom okruženju*) biće jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja.

- ***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.

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***).

- ***Definišite tipove datoteka za skeniranje*** - odlučite da li želite da skenirate:

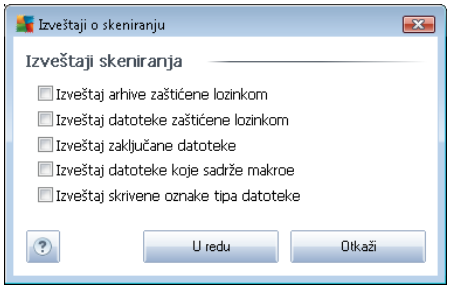
  - ***Sve tipove datoteka*** sa mogućnošću definisanja izuzetaka koji se neće skenirati tako što ćete navesti listu oznaka tipa datoteke razdvojenih zarezima koje ne treba skenirati;

  - ***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 *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:



Napomena: *Podrazumevana podešavanja za konfiguraciju skeniranja su optimalne performanse. Ukoliko nemate određen razlog za menjanje podešavanja skeniranja, preporučuje se da ne menjate unapred definisanu konfiguraciju. Sve promene konfiguracije trebalo bi da obavljaju samo napredni korisnici. Više opcija za konfiguraciju skeniranja potražite u dijalogu* ***Napredna podešavanja*** *koji je dostupan pomoću sistemskog menija* ***Datoteka / Napredna podešavanja*** *.*

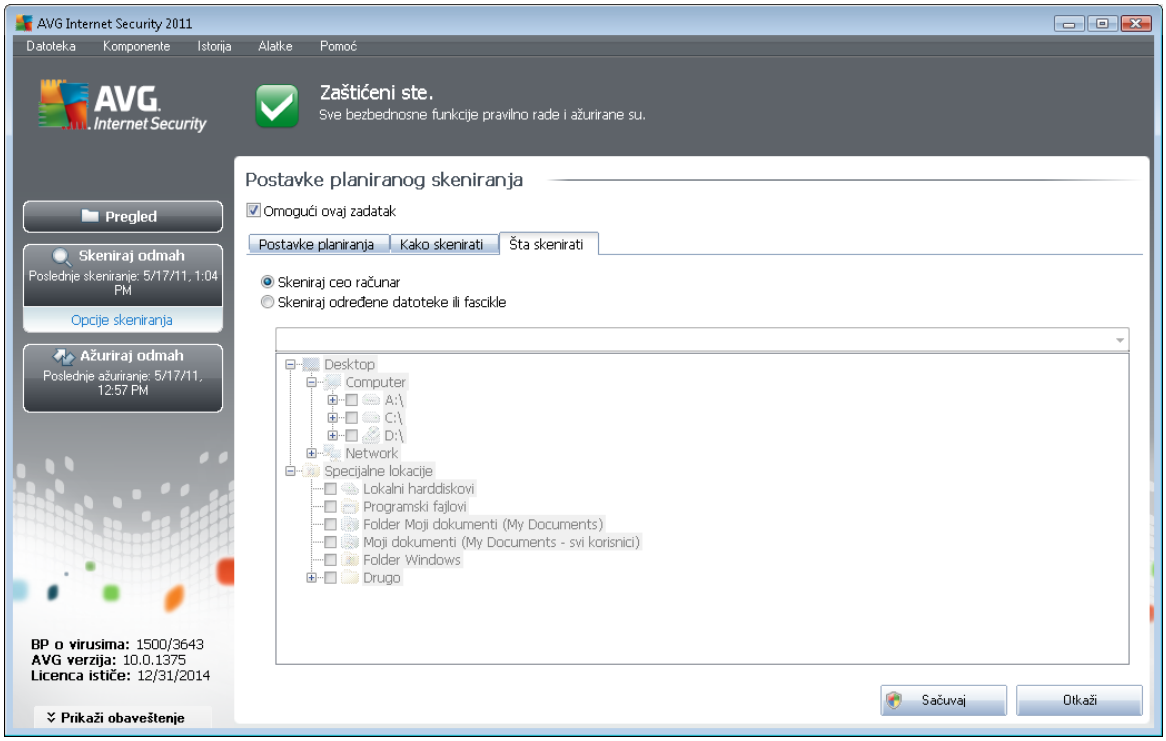
Kontrolna dugmad

Postoje dva kontrolna dugmeta na sve tri kartice u dijalogu ***Podešavanja za planirano skeniranje*** (***Postavke planiranja***, ***Kako skenirati*** i ***Šta skenirati***), a imaju istu funkcionalnost, bez obzira na to na kojoj kartici se nalazete:

- ***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.

- ***Otkaži*** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na podrazumevani dijalog AVG interfejsa za skeniranje..

11.5.3. Šta skenirati



Na kartici ***Šta skenirati*** , možete definisati da li želite da zakažete skeniranje celog računara ili skeniranje određenih 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\

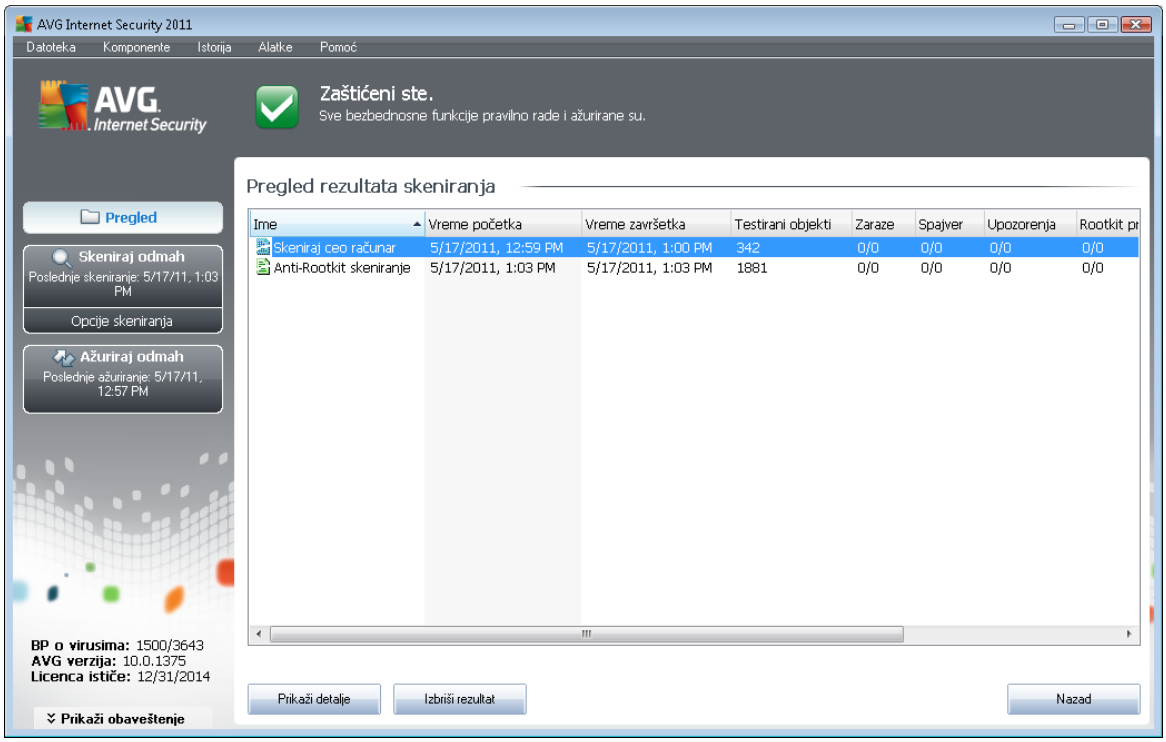
  - ***Drugo***
    - *Sistemska disk jedinica* - čvrsti disk na kojem je instaliran operativni sistem (obično C:)
    - *Sistemska fascikla* - C:\Windows\System32\\
    - *Fascikla za privremene datoteke* - C:\Documents and Settings\User\Local\ (*Windows XP*); ili C:\Users\user\AppData\Local\Temp\ (*Windows 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 u dijalogu Podešavanja za planirano skeniranje

Dva kontrolna dugmeta dostupna su na svakoj od tri kartice u dijalogu ***Podešavanje planiranog skeniranja*** (***Podešavanje planiranja***, ***Kako skenirati*** i ***Šta skenirati***), a funkcionalnost im je ista bez obzira na to 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.
- ***Otkaži*** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na podrazumevani dijalog AVG interfejsa za skeniranje..

11.6. 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 inferkcija, 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

11.7. Detalji rezultata skeniranja

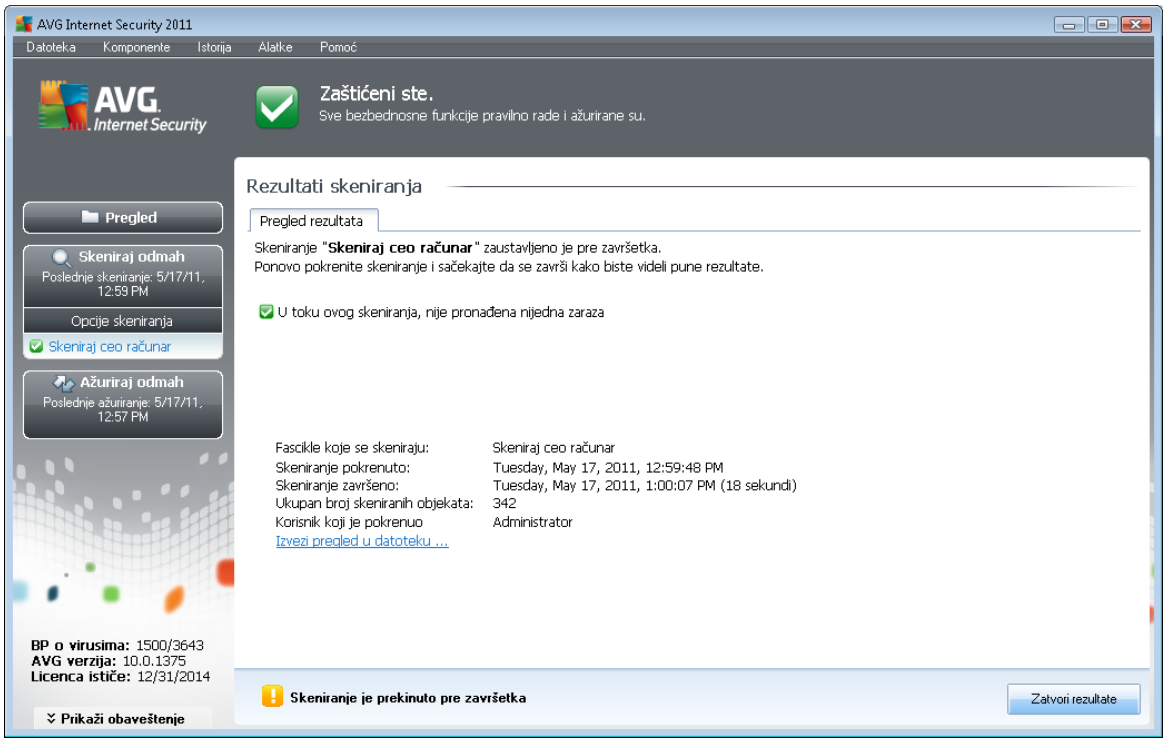
Ako u dijalogu ***Pregled rezultata skeniranja*** izaberite određeni način skeniranja, moći ćete da kliknete na dugme ***Prikaži detalje*** kako biste prešli u dijalog ***Rezultati skeniranja*** koji sadrži detaljne informacije o toku i rezultatu izabranog načina skeniranja.

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 videti informacije o objektima koje nije bilo moguće skenirati (npr. arhivama koje su zaštićene lozinkom).

11.7.1. Kartica Pregled rezultata



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

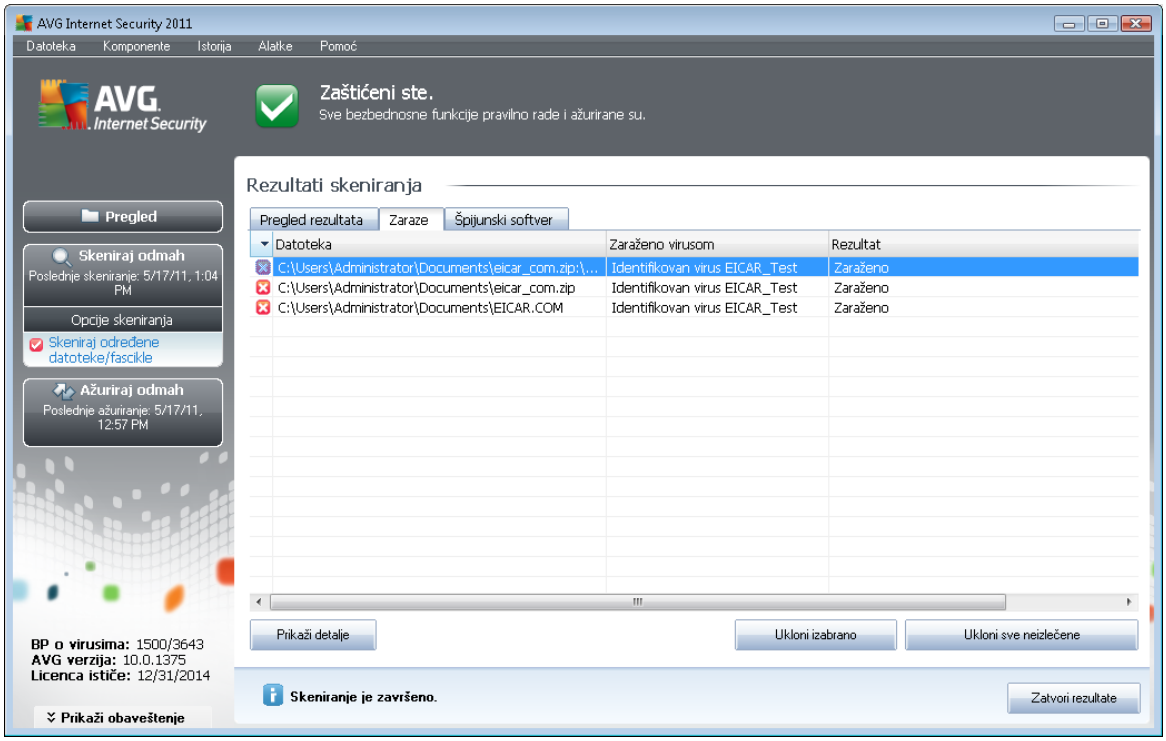
- detektovanim zarazama virusom / špijunskim softverom
- uklonjenim zarazama virusom / špijunskim softverom
- broju zaraza virusom / špijunskim softverom koji se ne mogu ukloniti ili oporaviti

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***.

11.7.2. 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*** - zaražđeni objekat je automatski izlečen i ostavljen je na originalnoj lokaciji
    - ***Premešteno u skladište virusa*** - zaraženi objekat je premešten u ***Skladište virusa***
    - ***Izbrisano*** - zaraženi objekat je izbrisan
    - ***Dodato u PUP izuzetke*** - pronađeni objekat je prepoznat kao izuzetak i dodat na listu Izuzeci 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

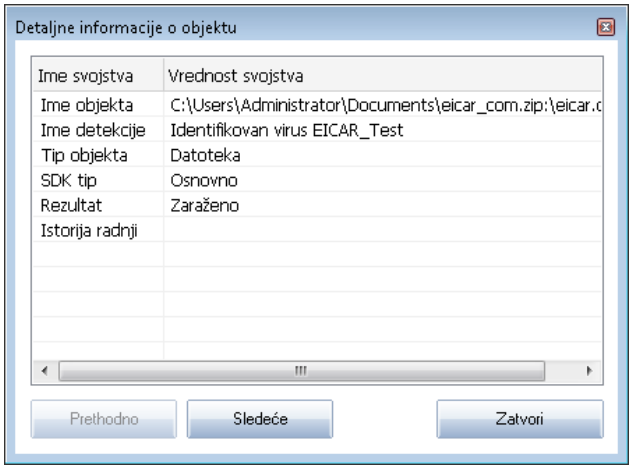
- **Potencijalno opasan objekat** - objekat je prepoznat kao potencijalno opasan, ali ne i zaražen (*npr. možda sadrži makroe*); ovu informaciju treba shvatiti samo kao upozorenje

- **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***:



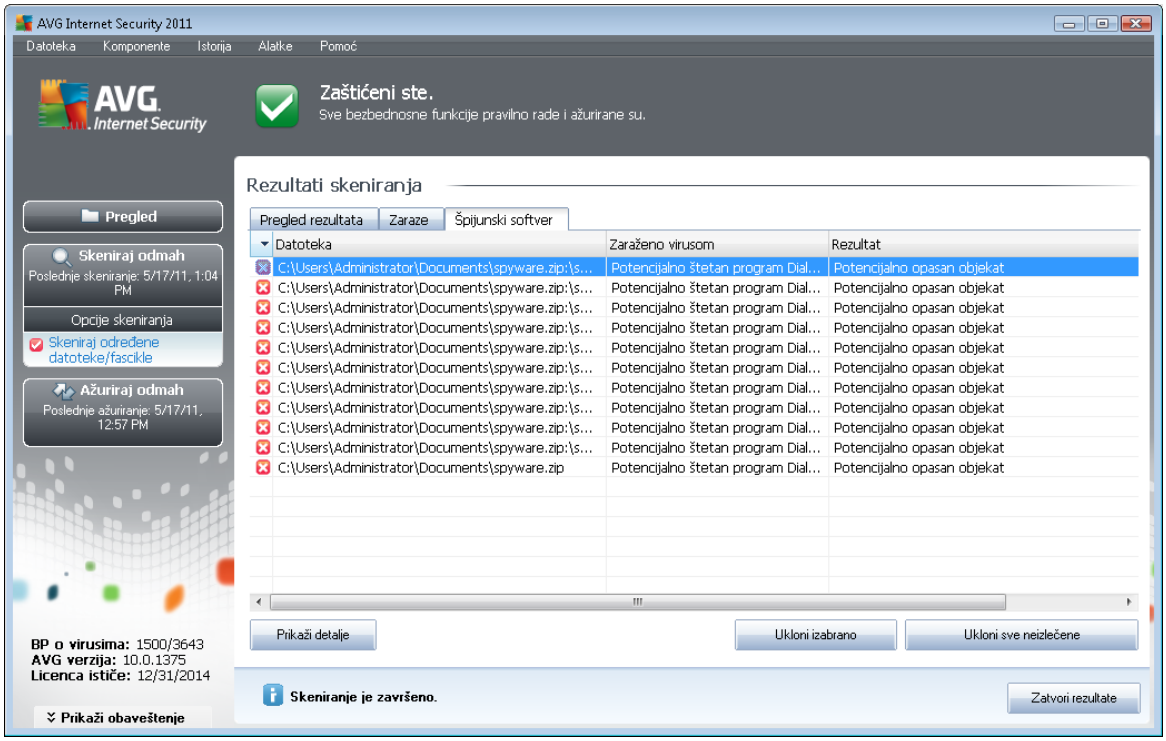
  U ovom dijalogu možete naći detaljne informacije o detektovanom zaraznom objektu (*npr. naziv i lokaciju zaraženog objekta, tip objekta, SDK tip, nalaz detekcije i istoriju radnji povezanih sa detektovanim objektom*). Pomoću dugmadi ***Prethodno*** / ***Sledeće*** možete prikazati informacije o željenim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

11.7.3. 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***
    - ***Izbrisano*** - 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

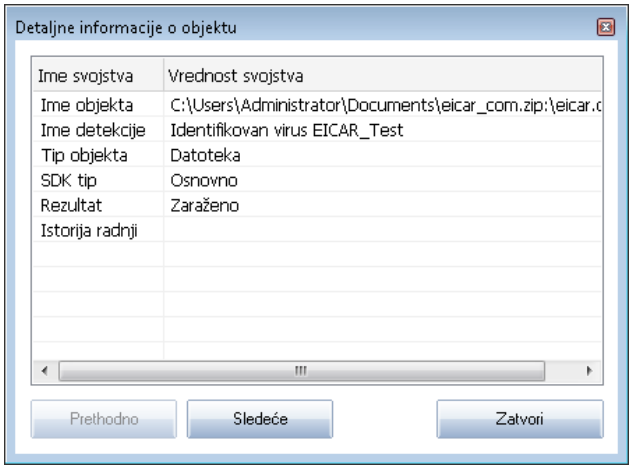
skenira

- o ***Potencijalno opasan objekat*** - objekat je označen kao potencijalno opasan, ali nije zaražen (na primer, možda sadrži makroe); ovo je samo upozorenje
- o ***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***

11.7.4. 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 adver ili špijunski softver. Ukoliko se AVG testom otkriju samo upozorenja, nije potrebno preduzeti nikakvu radnju.

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 prijavi skrivenu datoteku za koju sumnjate da je zlonamerna, možete je premestiti u ***AVG 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.

11.7.5. Kartica Rootkit programi

Kartica***Rootkit programi*** prikazuje informaciju o rootkit programima koji su detektovani tokom skeniranja ukoliko ste pokrenuli ***Anti-Rootkit skeniranje***.

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***.

11.7.6. Kartica Informacije

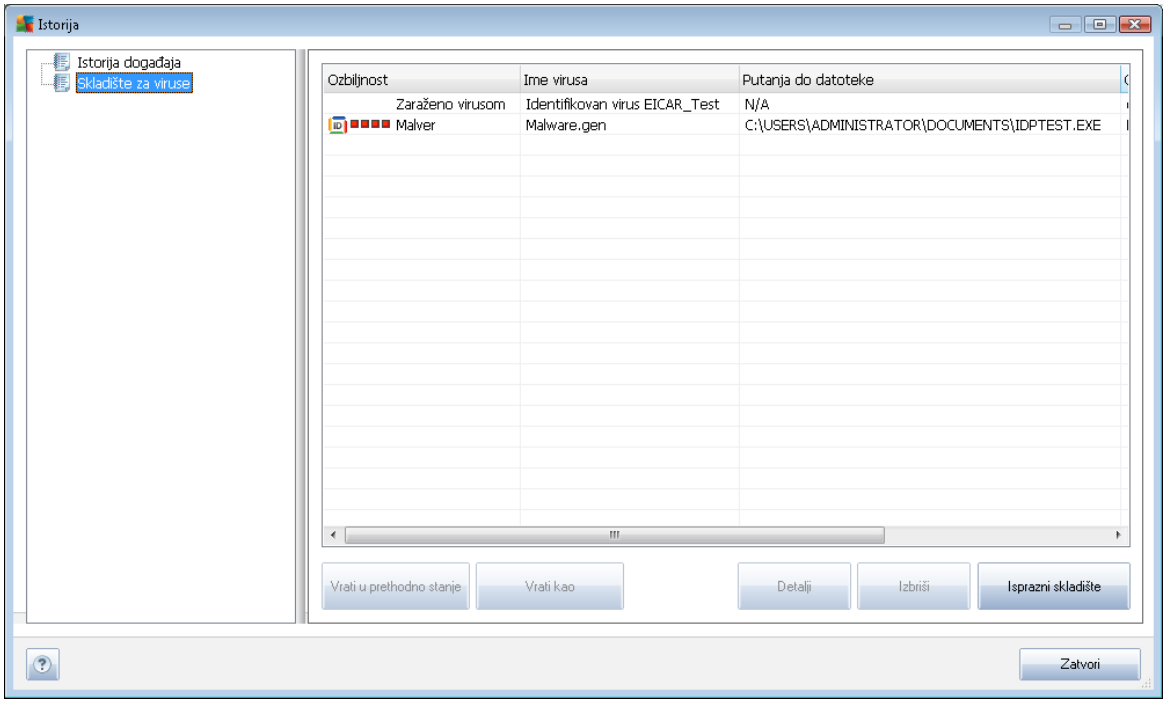
Na kartici ***Informacije*** nalaze se podaci o pronađenim objektima koji se ne mogu definisati kao zaraze virusom, špijunski softver itd. Ne mogu se obeležiti kao definitivno opasne, ali je potrebno da obratite pažnju na njih. AVG skeniranjem mogu da se otkriju datoteke koje nisu zaražene, ali su sumnjive. Za takve datoteke prikazuje se ***Upozorenje*** ili ***Informacija***.

Ozbiljnost na nivou ***Informacije*** prijavljuje se 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*** - AVG ne može da skenira datoteke zaštićene lozinkom (*kao ni 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 nije podrazumevano vidljiva u Windowsu, a AVG će vas obavestiti o ovakvim datotekama kako ih ne biste slučajno otvorili.
- ***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*), AVG će prijaviti to neslaganje. U nekim slučajevima, virusi koriste imena standardnih sistemskih procesa kako bi sakrili svoje prisustvo u sistemu.
- ***Zaključana datoteka*** - prijavljena datoteka je zaključana i AVG je ne može skenirati. To obično znači da neku datoteku neprekidno koristi sistem (*npr. datoteka virtuelne memorije*).

11.8. 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 odsutstvo 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 ***Zaštita identiteta*** u okviru programa **AVG Internet Security 2011**, 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***

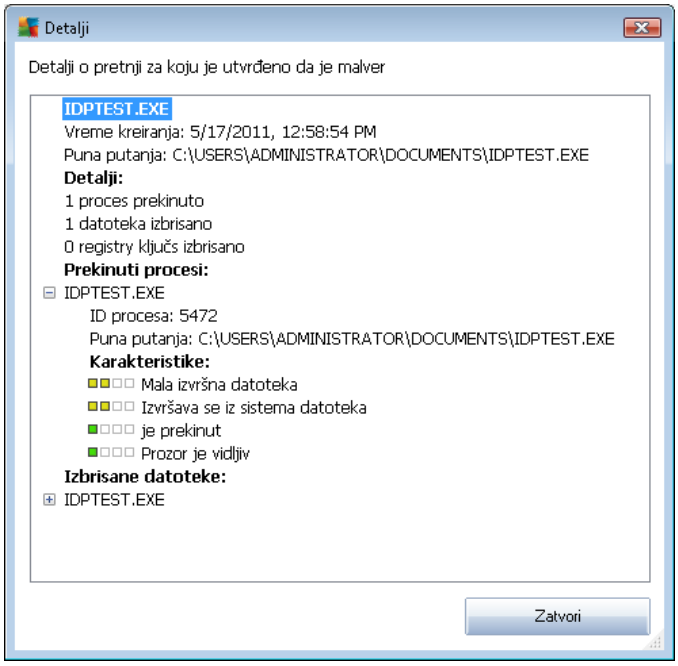
Kontrolna dugmad

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 ***Zaštita identiteta***. 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 „Zaštita identiteta“!



- ***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*).

12. Ažuriranje programa AVG

Ažuriranje programa AVG je izuzetno bitno kako bi novi virusi mogli da se otkriju što pre.

Pošto seažuriranje programa AVG ne izdaje prema određenom rasporedu, već pre kao reakcija na količinu i ozbiljnost novih pretnji, preporučljivo je da barem jednom dnevno ili čak i češće proveriti da li postoji novo ažuriranje. Samo na taj način možete biti sigurni da se ažuriranje vašeg **AVG Internet Security 2011** održava i tokom dana.

12.1. Nivoi ažuriranja

AVG nudi dva nivoa ispravki koje možete izabrati

- ***Ažurirane definicije*** sadrže promene neophodne za pouzdanu zaštitu od virusa. 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.

Kada pravite plan za ažuriranje, moguće je izabrati nivo prioriteta koji treba da bude preuzet i primenjen.

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

12.2. Tipovi ažuriranja

Razlikuju se dva tipa ažuriranja:

- ***Ažuriranje na zahtev*** je trenutno ažuriranje programa AVG koje se može izvršiti uvek kada postoji potreba za time.

- ***Planirano ažuriranje*** - u programu AVG možete i unapred podesiti plan ažuriranja. Planirano ažuriranje se zatim obavlja periodično u skladu sa konfiguracijom instalacije. Kada se na navedenoj lokaciji pojave nove datoteke ispravki, one se preuzimaju direktno sa Interneta ili iz mrežnog direktorijuma. Kada nema dostupnih novijih ispravki, ništa se ne dešava.

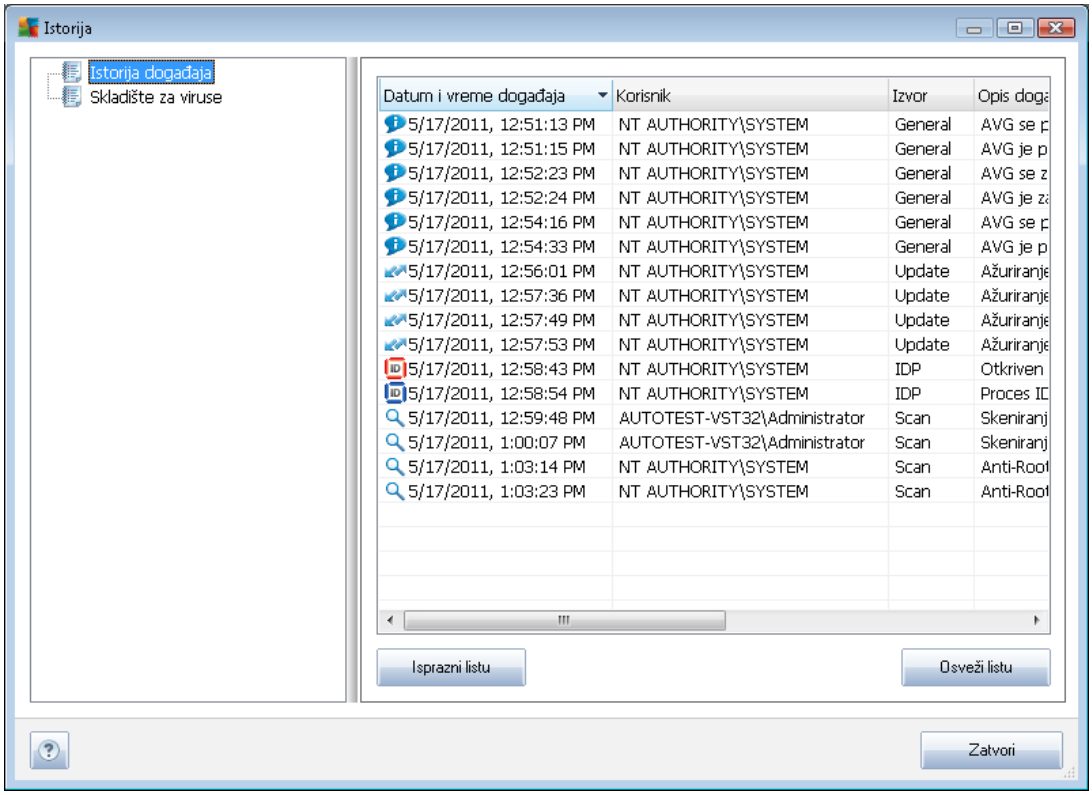
12.3. Proces ažuriranja

Proces ažuriranja moguće je pokrenuti odmah pomoću brze veze ***Ažuriraj odmah***. Ova veza dostupna je u svakom trenutku iz bilo kojeg dijaloga u AVG korisničkom interfejsu. Međutim, preporučuje sa da redovno obavljate ažuriranje, kao što je navedeno u planu ažuriranja koji je moguće urediti pomoću komponente Upravljanje ažuriranjem.

Kada pokrenete ažuriranje, AVG će prvo proveriti da li su dostupne nove datoteke za ažuriranje. Ako jesu, AVG će započeti njihovo preuzimanje 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 pokretanja ažuriranja programa AVG, kreira se tačka za vraćanje sistema u prethodno stanje. Ako proces ažuriranja ne uspe i dođe do pada operativnog sistema, možete ga uvek vratiti u stanje prvobitne konfiguracije. Toj opciji možete da pristupite ako kliknete na Start / Svi programi / Pribor / System tools / Oporavak sistema. Preporučuje se samo iskusnim korisnicima!*

13. 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 2011**. ***Istorija*** beleži sledeće tipove događaja:

- Informacije o ispravkama za AVG aplikaciju
- Početak, završetak ili zaustavljanje skeniranja(, *uključujući automatski izvršene testove*)
- Događaje koji su povezani sa otkrivanjem virusa (*pomoću komponente*Stalni štit *ili* skeniranjem,) uključujući lokaciju događaja
- Druge važne događaje

Za svaki događaj, navode se sledeće informacije:

- ***Datum i vreme događaja*** sadrži tačno vreme i datum događaja
- ***Korisnik***navodi ko je pokrenuo događaj
- ***Izvor*** sadrži izvornu komponentu ili neki drugi deo AVG sistema koji je pokrenuo događaj
- ***Opis događaja*** daje rezime događaja

Kontrolna dugmad

- ***Isprazni listu*** - brisanje svih stavki sa liste događaja
- ***Osveži listu*** - ažuriranje svih stavki sa liste događaja

14. Najčešća pitanja i tehnička podrška

Ukoliko imate poslovnih ili tehničkih problema sa programom AVG, pogledajte odeljak ***Najčešća pitanja*** na AVG Web lokaciji (http://www.avg.com/).

Ako na taj način ne uspete da pronađete odgovarajuću pomoć, obratite se odeljenju tehničke podrške e-poštom. Upotrebite obrazac za kontakt kojem možete pristupiti iz sistemskog menija izborom stavke ***Pomoć / Pomoć na mreži*** .