

# *bit*defender



**ANTIVIRUS** 2008

*Navodila za uporabo*

## BitDefender Antivirus 2008

### Navodila za uporabo

Izdano 2008.05.07

Pravna zaščita© 2008 BitDefender

#### Pravni poduk

Vse pravice pridržane. Vse informacije, pisne in slikovne, vsebovane v teh navodilih, so v zakonsko dovoljenem okviru predmet avtorske zaščite ali druge oblike zaščite intelektualne lastnine. Dokumenti so lahko reproducirani le v nekomercialne namene, pri čemer morajo ohraniti vsa navedena opozorila o avtorskih ali drugih pravicah. Dokumentov se ne sme prepisovati, razmnoževati ali kako drugače razširjati v komercialne namene brez izrecnega pisnega dovoljenja podjetja SOFTWIN.

**Opozorilo.** Ta izdelek in njegova dokumentacija sta zaščiteni z avtorskimi pravicami. Informacije v teh dokumentih so podane "kot take" in zanje ne velja garancija. Kljub temu, da je bil pri pripravi dokumentov upoštevan vsak varnostni vidik, avtorji ne odgovarjajo za morebitno poškodbo ali izgubo podatkov na računalniku, ki je posledica neposrednih ali posrednih informacij, vsebovanih v tem delu.

Ta knjižica vsebuje povezave do spletnih strani drugih, ki niso pod nadzorom podjetja SOFTWIN in zato SOFTWIN ne more biti odgovoren za vsebino, ki se nahaja na teh straneh. Takšne strani obiskujete na lastno odgovornost. SOFTWIN te povezave podaja zgolj kot dodatek, kar seveda ne pomeni, da SOFTWIN stremi k vsebini teh spletnih strani.

**Blagovne znamke.** V tej knjižici se lahko pojavijo različne blagovne znamke. Vse registrirane in neregistrirane blagovne znamke v tem dokumentu so last njihovih lastnikov.



# Kazalo

<b>Licenca in Garancija</b> .....	<b>vii</b>
<b>Uvod</b> .....	<b>x</b>
1. Dogovori, uporabljeni v knjižici .....	x
1.1. Tipografski dogovori .....	x
1.2. Opozorila .....	xi
2. Struktura knjižice .....	xi
3. Komentarji .....	xii
<b>Namestitev</b> .....	<b>1</b>
<b>1. BitDefender Antivirus 2008 Namestitev</b> .....	<b>2</b>
1.1. Sistemske zahteve .....	2
1.2. Namestitveni koraki .....	3
1.3. Namestitveni čarovnik .....	5
1.3.1. Korak 1/6 - Registracija BitDefender Antivirus 2008 .....	5
1.3.2. Korak 2/6 - Kreiranje BitDefender računa .....	6
1.3.3. Korak 3/6 - Več o RČPV .....	8
1.3.4. Korak 4/6 – Izbira opravil .....	9
1.3.5. Korak 5/6 - Čakanje na dokončanje opravil .....	10
1.3.6. Korak 6/6 - Povzetek .....	11
1.4. Nadgradnja .....	11
1.5. Odstranjevanje, popravilo ali spreminjanje BitDefenderja .....	12
<b>Osrednja administracija</b> .....	<b>14</b>
<b>2. Uvod</b> .....	<b>15</b>
2.1. BitDefender ikona v sistemskem kotičku .....	16
2.2. Vrstica aktivnosti skeniranja .....	17
2.3. BitDefender ročno skeniranje .....	17
2.4. Igričarski način .....	18
2.4.1. Uporaba igričarskega načina .....	18
2.4.2. Spreminjanje hitre tipk za igričarski način .....	19
<b>3. Stanje zaščite</b> .....	<b>20</b>
3.1. Gumb stanja Antivirus .....	21
3.2. Gumb stanja Antiphishing .....	22
3.3. Gumb stanja nadzora zasebnosti .....	23
3.4. Gumb stanja Posodobitev .....	23
<b>4. Hitra opravila</b> .....	<b>25</b>
4.1. Zaščita .....	25
4.1.1. Posodabljanje BitDefenderja .....	25

4.1.2. Skeniranje z BitDefenderjem .....	27
<b>5. Zgodovina .....</b>	<b>32</b>
<b>6. Registracija .....</b>	<b>34</b>
6.1. Korak 1/3 - Registracija BitDefender Antivirus 2008 .....	34
6.2. Korak 2/3 - Kreiranje BitDefender računa .....	35
6.3. Korak 3/3 - Registracija BitDefender Antivirus 2008 .....	37
<b>Napredna varnostna administracija .....</b>	<b>38</b>
<b>7. Vmesnik nastavitvev .....</b>	<b>39</b>
7.1. Spreminjanje splošnih nastavitvev .....	40
7.1.1. Nastavitve poročil .....	40
7.1.2. Nastavitve virusnih poročil .....	42
7.1.3. Upravljanje z nastavitvami .....	42
<b>8. Protivirusna zaščita .....</b>	<b>43</b>
8.1. Skeniranje ob dostopu .....	43
8.1.1. Nastavitve stopnje zaščite .....	44
8.1.2. Zaščita po meri .....	45
8.1.3. Onemogočanje realnočasovne zaščite .....	49
8.2. Skeniranje na zahtevo .....	49
8.2.1. Opravila skeniranja .....	50
8.2.2. Uporaba hitrega seznama .....	52
8.2.3. Ustvarjanje opravil skeniranja .....	53
8.2.4. Nastavitve naloge skeniranja .....	53
8.2.5. Predmeti skeniranja .....	64
8.2.6. Ogljed prijav skeniranja .....	70
8.3. Predmeti izvzeti iz skeniranja .....	72
8.3.1. Izvzemanje poti iz skeniranja .....	74
8.3.2. Izvzemanje končnic iz skeniranja .....	76
8.4. Karantena .....	79
8.4.1. Upravljanje z datotekami v karanteni .....	79
8.4.2. Spreminjanje nastavitvev karantene .....	80
<b>9. Nadzor zasebnosti .....</b>	<b>82</b>
9.1. Stanje nadzora zasebnosti .....	82
9.1.1. Nadzor zasebnosti .....	83
9.1.2. Antiphishing zaščita .....	84
9.2. Napredne nastavitve-Nadzor identitete .....	85
9.2.1. Ustvarjanje pravil identitete .....	86
9.2.2. Določanje izjem .....	89
9.2.3. Upravljanje pravil .....	90
9.3. Napredne nastavitve-Nadzor registra .....	91
9.4. Napredne nastavitve-Nadzor piškotkov .....	93
9.4.1. Čarovnik za nastavitve .....	95

9.5. Napredne nastavitve-Nastavitve skripte .....	97
9.5.1. Čarovnik za nastavitve .....	98
9.6. Sistemske informacije .....	99
9.7. Orodna vrstica zaščite neželene pošte .....	101
<b>10. Posodobitev .....</b>	<b>103</b>
10.1. Samodejno posodabljanje .....	103
10.1.1. Zahteva posodobitev .....	105
10.1.2. Onemogočanje samodejnega posodabljanja .....	105
10.2. Posodobitvene nastavitve .....	106
10.2.1. Nastavitve lokacij posodobitev .....	107
10.2.2. Spreminjanje samodejnih posodobitev .....	107
10.2.3. Spreminjanje ročnih posodobitev .....	108
10.2.4. Spreminjanje naprednih nastavitvev .....	108
10.2.5. Upravljanje proxyjev .....	109
<b>BitDefenderjev obnovitveni CD .....</b>	<b>111</b>
<b>11. Pregled .....</b>	<b>112</b>
11.1. Sistemske zahteve .....	112
11.2. Vključena programska oprema .....	113
<b>12. BitDefenderjev reševalni CD Pomoč .....</b>	<b>116</b>
12.1. Zaženi BitDefender reševalni cd. ....	116
12.2. Zaustavitev BitDefender reševalnega cdja. ....	117
12.3. Kako izvedem proivirusno skeniranje? .....	118
12.4. Kako posodobim BitDefender preko proxy? .....	119
12.5. Kako dostopam do svojih podatkov? .....	119
<b>Pomoč .....</b>	<b>122</b>
<b>13. Podpora .....</b>	<b>123</b>
13.1. BitDefender baza znanja .....	123
13.2. Kako do pomoči .....	123
13.2.1. Pojdite na mrežno samopostrežno .....	123
13.2.2. Odpri kupon za podporo .....	124
13.3. Kontaktne informacije .....	124
13.3.1. Spletni naslovi .....	124
13.3.2. Franšizne pisarne .....	125
<b>Slovar izrazov .....</b>	<b>128</b>

## Licenca in Garancija

ČE SE NE STRINJATE S POGOJI, NE NAMESTITE PROGRAMA. Z IZBIRO ODGOVOROV "SPREJMEM", "V REDU", "NADALJUJ", "DA" ALI KAKRŠNOKOLI DRUGO UPORABO PROGRAMSKE OPREME SOGLAŠATE S POGOJI UPORABE LE-TE.

Ti pogoji se nanašajo na BitDefender rešitve, dokumentacijo in storitve, namenjene domačim uporabnikom. Z licenčno različico programa ste upravičeni do posodobitev in nadgradenj kot je to navedeno v dokumentaciji programa.

Ta licenčna pogodba je zakonita pogodba med vami in programsko hišo SOFTWIN in določa pogoje uporabe SOFTWIN programske opreme, ki vsebuje računalniško programsko opremo ter morebitno dodatno gradivo – medije, natisnjene materiale, spletno ali elektronsko dokumentacijo ("BitDefender"), ki je zaščitena z mednarodnimi zakoni o avtorskih pravicah. Z namestitvijo, kopiranjem ali drugim načinom uporabe BitDefender programske opreme, se strinjate z vsebino te licenčne pogodbe. Kakršnakoli zloraba je kazniva. V kolikor se ne strinjate s spodaj navedenimi pogoji, ne namestite ali uporabljajte programske opreme BitDefender. Programsko opremo je moč vrniti v osmih dneh od dneva nakupa, povrnjena vam bodo vsa sredstva. To storite na mestu, kjer ste programsko opremo kupili, potrebno bo dokazilo o nakupu.

Če se ne strinjate s pogoji uporabe, ne namestite programa BitDefender.

**BitDefender licenca.** Programska oprema BitDefender je zaščitena z mednarodnimi zakoni o avtorskih pravicah ter drugimi zakoni o intelektualni lastnini. BitDefender programska oprema je podvržena licenciranju, ne prodaji.

**LICENČNO DOVOLJENJE.** BITDEFENDER vam in zgolj vam na tem mestu dovoli uporabo programske opreme BitDefender.

**PROGRAMSKA OPREMA.** BitDefender lahko namestite na določeno število računalnikov, za katere imate veljavno licenco za uporabo programa. Upravičeni ste tudi do izdelave ene varnostne kopije.

**NAMIZNA LICENCA.** Ta licenca se nanaša na BitDefender izdelek, ki ga je moč namestiti na en sam računalnik in ne ponuja omrežnih storitev. Uporabnik lahko programsko opremo namesti na en računalnik in si izdelava eno varnostno kopijo. Število uporabnikov je omejeno s številom veljavnih licenc.

**POGOJI LICENCIRANJA.** Licenčno obdobje se prične z dnem namestitve programskega paketa BitDefender in traja do dne, označenega s potekom licenčnega ključa.

POTEK LICENCE. Ta izdelek bo prenehal pravilno delovati takoj po preteku veljavnosti licence.

NADGRADNJA. V primeru, da je BitDefender paket označen kot nadgradnja, preverite svojo licenco, če vam le-ta omogoča uporabo nadgradenj programskega paketa BitDefender. Nadgradnja običajno prinaša dodatne lastnosti in zmogljivosti obstoječi različici programskega paketa. Število nadgradenj ustreza številu licenc, ki jih za BitDefender izdelke posedujete. Pogoji te licence nadomeščajo in zamenjujejo vsa predhodna določila, ki obstajajo med vami in podjetjem SOFTWIN, glede originalnega izdelka in nadgrajenega izdelka.

AVTORSKE PRAVICE. Vse avtorske pravice, povezane s programsko opremo BitDefender (vključujoč slike, fotografije, logotipe, animacije, video ter avdio vsebino, tekst in druge lastnosti programa BitDefender) ter priloženimi dodatki v obliki tiskovin so last programske hiše SOFTWIN. Program BitDefender je zaščiten z avtorskimi pravicami, zato ga je potrebno jemati kot intelektualno lastnino. Dovoljena je izdelava ene varnostne kopije zgolj v varnostne namene. Kopiranje drugih BitDefender vsebin ter dodatkov je prepovedano. Za vse kopije programa BitDefender je potrebno imeti ustrezno licenčno pogodbo. Prepovedano je razmnoževanje, posojanje, podlicenciranje in druge oblike zlorab uporabniške licence. Prepovedan je povratni inženiring in vsi posegi ter modifikacije programske kode programa BitDefender.

OMEJENA GARANCIJA. Programska hiša BITDEFENDER jamči za dobo 30 dni, da je medij, na katerem se nahaja programski paket BitDefender, brezhiben in brez napak. V primeru, da je medij poškodovan, vam bo poslan drug medij (potrebno je dostaviti poškodovan medij), ali povrnjena kupnina. Programska hiša SOFTWIN ne jamči, da je programski paket BitDefender brez napak oziroma da bodo morebitne napake odpravljene. Programska hiša SOFTWIN tudi ne jamči, da bo BitDefender izpolnil vaša pričakovanja.

PROGRAMSKA HIŠA BITDEFENDER NA TEM MESTU ZAVRÄČA VSE DRUGE GARANCIJSKE OBVEZNOSTI ZA PROGRAMSKI PAKET BITDEFENDER. ZGORAJ OPISANI GARANCIJSKI POGOJI VAM NUDIJO SPECIFIČNE ZAKONSKE PRAVICE DO UVELJAVLJANA GARANCIJE.

NAPAKE. Uporabniki, ki programsko opremo BitDefender preizkušajo ter ocenjujejo, nosijo tudi vse tveganje napak v delovanju te programske opreme. V nobenem primeru programska hiša BITDEFENDER ni odgovorna za napake in poškodbe, neposredne ter posredne, ki bi nastale pri uporabi navedene programske opreme. V NEKATERIH DRŽAVAH TAKŠNA OMEJITEV GARANCIJE NE VELJA. V NOBENEM PRIMERU PA ODGOVORNOST PROGRAMSKE HIŠE NE PRESEGA ZNESKA, KATEREGA JE ODŠTEL KUPEC ZA NJENE PROIZVODE OB NAKUPU. Omejitve in obvestila

podana zgoraj veljajo ne glede za običajne uporabnike, preizkuševalce ter vse druge vrste uporabe omenjene programske opreme.

**POMEMBNO OBVESTILO ZA UPORABNIKE.** TA PROGRAMSKI PAKET NI BREZ NAPAK IN KOT TAK NI NAMENJEN UPORABI V TVEGANIH OKOLJIH, KJER SE ZAHTEVA POPOLNO DELOVANJE, BREZ MOŽNOSTI NAPAK. TA PROGRAMSKA OPREMA NI NAMENJENA UPORABI NA SISTEMIH, KI KRMILIJO LETALSKO NAVIGACIJO, OBJEKTE Z NUKLEARNO ALI VOJAŠKO VSEBINO, KOMUNIKACIJSKE SISTEME TER DRUGE NEPOSREDNE ALI POSREDNE SISTEME, KJER ODPOVED DELOVANJA LAHKO POVZROČI SMRT, TEŽKE FIZIČNE POŠKODBE OSEB ALI LASTNINE.

SPLOŠNO. Ta pogodba je izdelana po zakonskih določilih, veljavnih v Romuniji. Spori v zvezi s to pogodbo se bodo zato reševali na sodiščih, lociranih v Romuniji.

Cene, stroški in provizije za uporabo BitDefender rešitev se lahko spremenijo brez vnaprejšnjega opozorila.

V primeru neveljavnosti določenega dela te pogodbe, se neveljavnost nanaša samo na tisti del, ne pa na ostale dele te pogodbe.

BitDefender in BitDefender logotip sta blagovni znamki podjetja BITDEFENDER. Vse ostale blagovne znamke, uporabljene v izdelku ali pripadajočih materialih so last njihovih zakonitih lastnikov.

Licenčna pogodba se brez opozorila prekine v trenutku, ko je ugotovljeno, da je uporabnik kršil katerega izmed pogojev uporabe. V tem primeru ni upravičen do polnega ali delnega nadomestila sredstev s strani BITDEFENDER.

BITDEFENDER lahko po potrebi spremeni licenčne pogoje distribucije programske opreme. Če bo sprememba spoznana za neustrezno, bo njena veljavnost nična.

V primeru sporov in neskladnosti (protislovij) med prevodi splošnih določil in pogojev pogodbe obvelja angleška različica pogojev, ki jih objavlja podjetje BITDEFENDER.

Kontakt: BITDEFENDER, West Gate Park, Building H2, 24 Preciziei Street Sector 6, Bucharest, Romania, ali na Tel No: +4021 300 12 55 ali Fax:40-212641799, e-poštni anslov: [office@bitdefender.com](mailto:office@bitdefender.com).

## Uvod

Hvala, da ste izbrali **BitDefender Antivirus 2008** za varovanje vašega računalniškega sistema. Informacije, predstavljene v tej knjižici, so primerne tako za poznavalce računalniške opreme, temveč tudi za vse uporabnike, ki so večji dela z operacijskimi sistemi Windows.

V knjižici boste našli opis programa **BitDefender Antivirus 2008**, podjetja in ekipe, ki ga je pripravila, navodila za namestitev ter konfiguracijo programa. Spoznali boste kako uporabljati **BitDefender Antivirus 2008**, kako ga nadgraditi, testirati in nastaviti po vaših željah. Naučili se boste, kako iz BitDefender izvleči najboljše.

Želimo vam prijetno in koristno "predavanje".

## 1. Dogovori, uporabljeni v knjižici

### 1.1. Tipografski dogovori

V knjižici je uporabljenih več različnih pisav, s katerimi je izboljšana preglednost. Njihova podoba in pomen sta predstavljena v spodnji tabeli.

Podoba	Opis
sample syntax	Primeri sintaks so natisnjeni z manjšo pisavo.
<a href="http://www.bitdefender.com">http://www.bitdefender.com</a>	Spletne povezave kažejo na zunanje lokacije, http ali ftp strežnike.
<a href="mailto:support@bitdefender.com">support@bitdefender.com</a>	E-poštna sporočila/naslovi so vnešena v tekst za hitrejši kontakt.
"Uvod" (p. x)	Gre za notranjo povezavo na lokacijo v dokumentu.
filename	Datoteke in direktoriji so natisnjeni z manjšo pisavo.
<b>option</b>	Vse možnosti so natisnjene s <b>krepro</b> pisavo.
<code>sample code listing</code>	Deli programske kode so natisnjeni z manjšo pisavo.

## 1.2. Opozorila

Opozorila in opombe najdete poleg teksta v okvirčkih. Grafično označena zahtevajo vašo pozornost in razkrivajo dodatne informacije o posamezni vsebini.



### **Opomba**

Gre le za krajšo pripombo. Čeprav jih lahko preskočite, pa takšne pripombe vsebujejo dragocene informacije o izdelku ali njegovi uporabi, včasih tudi povezavo na podobne vsebine/teme.



### **Pomembno**

Takšni okvirji potrebujejo vašo pozornost, zato ni priporočljivo, da jih preskočite. Običajno vsebujejo nekritične, a zelo pomembne podatke/informacije.



### **Pozor**

Gre za informacije kritičnega značaja, zato jih velja podrobno prebrati. Če boste sledili navodilom v opozorilih, bo program delal brez težav. Opozorila morate prebrati in razumeti, saj opisujejo postopke delovanja, ki vas ob nepravilni uporabi lahko pripeljejo do težav z delovanjem sistema.

## 2. Struktura knjižice

Knjižica vsebuje sedem delov, ki vsebujejo glavne teme. Na voljo je tudi slovar tehničnih izrazov.

**Namestitev.** Navodila vas po korakih vodijo skozi namestitev programa BitDefender na računalnik. Gre za izčrpen opis postopka namestitve programa **BitDefender Antivirus 2008**. Začenši s prednostnimi pogoji za uspešno namestitev, vas opis spremlja skozi posamezne korake namestitvenega procesa. Na koncu je opisan tudi postopek odstranitve programa v primeru, da bi želeli odstraniti program BitDefender z vašega računalnika.

**Osrednja administracija.** Opis osnovne administracije in vzdrževanja BitDefenderja

**Napredna varnostna administracija.** Podrobna predstavitev varnostnih zmogljivosti BitDefenderja. Poglavlje podrobno opisuje vse možnosti naprednih nastavitev konzole. Naučite se kako nastaviti in uporabljati BitDefenderjeve module za učinkovito zaščito pred vsemi oblikami zlonamernega programja (virusi, vohunski programi, rootkiti, itd.)

**BitDefenderjev obnovitveni CD.** Opis BitDefender obnovitvenega CD-ja. Pomaga vam razumeti in uporabljati možnosti, ki se nahajajo na tem zagonskem CD-ju.

**Pomoč.** Kam in na koga se obrniti, če pride do težav.

**Slovar izrazov.** Slovar izrazov razlaga nekatere tehnične in manj pogoste strokovne izraze, na katere boste naleteli v tej knjižici.

### 3. Komentarji

Tudi vi ste povabljeni k izpopolnjevanju te knjižice, saj vaše mnenje velja. Knjižico smo pripravili po naših najboljših močeh.

V kolikor v knjižici najdete kakšno napako ali pa imate predlog, kako vsebino lepše podati/izboljšati, nam prosim pišite na elektronski naslov [documentation@bitdefender.com](mailto:documentation@bitdefender.com).



#### **Pomembno**

Prosimo vas, da e-pošto povezano s temi dokumenti napišete čim bolj eksaktno. S tem boste pripomogli k učinkovitejšemu procesiranju vaše pošte.

# **Namestitev**

# 1. BitDefender Antivirus 2008 Namestitev

**BitDefender Antivirus 2008 Namestitev** poglavje hitrega vodiča obsega naslednje vsebine:

- **Sistemske zahteve**
- **Namestitveni koraki**
- **Čarovnik za nastavitev iniciacije**
- **Nadgradnja**
- **Odstranjanje, popravilo ali spreminjanje BitDefenderja**

## 1.1. Sistemske zahteve

Za zagotovitev pravilnega delovanja programa pred namestitvijo preverite, ali so izpolnjene spodnje sistemske zahteve:

- Podprti operacijski sistemi: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (ali višje)

### Windows 2000

- 800 MHz procesor ali zmogljivejši
- Vsaj 256 MB pomnilnika (priporočeno 512 MB)
- Vsaj 60 MB prostora na trdem disku

### Windows XP

- 800 MHz procesor ali zmogljivejši
- Vsaj 256 MB pomnilnika (priporočeno 1 GB)
- Vsaj 60 MB prostora na trdem disku

### Windows Vista

- 800 MHz procesor ali zmogljivejši
- Vsaj 512 MB pomnilnika (priporočeno 1 GB)
- Vsaj 60 MB prostora na trdem disku

**BitDefender Antivirus 2008** preizkusno različico lahko prenesete s strani <http://www.parametca.si>.

## 1.2. Namestitveni koraki

Poiščite namestitveno datoteko in jo dvokliknite. Zagnal se bo namestitveni čarovnik, ki vas bo vodil skozi proces namestitve.

Pred zagonom čarovnika za nastavitve bo BitDefender poiskal nove različice namestitvenega pakea. V kolikor je na voljo novejša različica, boste opozorjeni. Kliknite **DA** da namestite novejšo različico ali **NE** da nadaljujete z namestitvijo z različico, ki jo imate v namestitvenem paketu.



### Namestitveni koraki

Sledite tem korakom za namestitev BitDefender Antivirus 2008:

1. Kliknite **Naprej** za nadaljevanje ali **Nazaj** za vrnitev na prvi korak.
2. Kliknite **Naprej**.

BitDefender Antivirus 2008 vas opozori, če imate na vašem računalniku nameščene druge protivirusne programe. Kliknite **Odstrani** za odstranitev ostalih programov. V kolikor želite nadaljevati ne da bi odstranili ostale programe, kliknite **Naprej**.



### Pozor

Zelo priporočljivo je, da pred namestitvijo BitDefender zaščite odstranite vse druge protivirusne programe. Poganjanje dveh ali več protivirusnih programov istočasno namreč ponavadi popolnoma ohromi računalnik.

3. Prosimo preberite Licenčna pogodba (pogoje uporabe), izberite **Sprejem pogoje licenčne pogodbe** in kliknite **Naprej**. Če se ne strinjate s pogoji uporabe, kliknite **Prekliči**. Proces namestitve bo prekinjen.
4. Izbirate lahko tudi mapo, v katero želite namestiti program. Privzeta mapa je `C:\Program Files\Softwin\BitDefender 10`. Če želite izbrati drugo mapo, kliknite **Prebrskaj** in v oknu, ki se odpre, izberite mapo, kamor želite namestiti BitDefender Antivirus 2008. Kliknite **Naprej**.

Kliknite **Naprej**.

5. Izberite možnosti povezane z namestitvijo. Privzeto imate na voljo dve možnosti:
  - **Odpri datoteko BeriMe** - Odpre BeriMe (readme) datoteko po zaključku namestitve.
  - **Ustvari bližnico na namizju** - Ustvari bližnico do programa BitDefender Antivirus 2008 na namizju ob zaključku namestitve.
  - **Izvrži CD po končani namestitvi** - ob končani namestitvi vam izvrže CD medij, v kolikor imate program na mediju.
  - **Izklopi Windows Defender** - za izklop Windows Defender; ta možnost je na voljo le v Windows Visti.

Kliknite **Namesti** za začetek namestitve programa.



### Pomembno

Med namestitvijo se bo pojavil **čarovnik**. Čarovnik vam bo pomagal pri registraciji vašega **BitDefender Antivirus 2008**, kreiranju BitDefender računa in konfiguriranju BitDefender zaščite za opravljanje pomembnih varnostnih opravil.

Dokončajte delo s čarovnikom pred nadaljevanjem z naslednjim korakom.

6. Kliknite **Končaj**. Operacijski sistem lahko od vas zahteva, da ponovno zaženete računalnik za dokončanje namestitve. Priporočamo, da to storite čimprej.

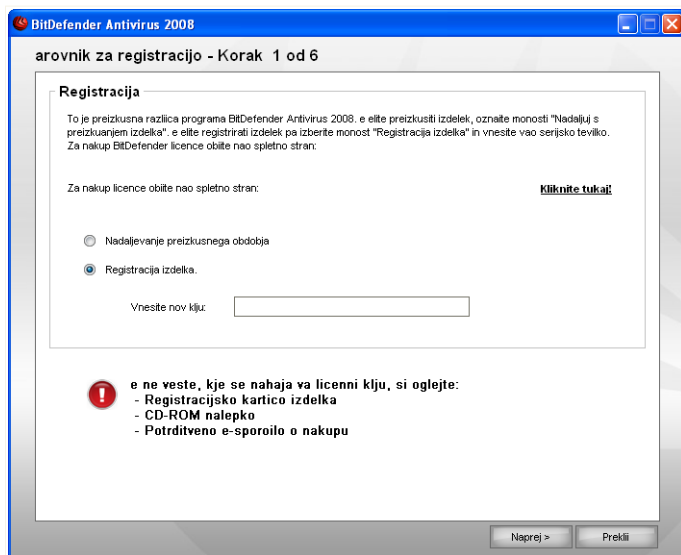
Če ste izbrali privzeto možnost za namestitveno mapo, potem je v mapi `Program Files` ustvarjena nova mapa, imenovana `BitDefender`. Le-ta pa vsebuje podmapo `BitDefender 2008`.

## 1.3. Namestitveni čarovnik

Med procesom namestitve se bo pojavil čarovnik, ki vam bo pomagal registrirati vaš **BitDefender Antivirus 2008**, kreirati BitDefender račun in konfigurirati BitDefender zaščito za opravljanje pomembnih varnostnih opravil.

Dokončanje tega čarovnika ni obvezno, kljub temu pa je priporočljivo, saj s tem prihranite čas in zagotovite zaščito vašega sistema še preden je BitDefender Antivirus 2008 nameščen.

### 1.3.1. Korak 1/6 - Registracija BitDefender Antivirus 2008



#### Registracija

Izberite možnost **Registriraj izdelek** za registracijo **BitDefender Antivirus 2008**. Vnesite licenčni ključ v polje **Vnesi nov ključ**.

Za nadaljevanje preizkušanja izberite **Nadaljuj s preizkušanjem izdelka**.

Kliknite **Naprej**.

## 1.3.2. Korak 2/6 - Kreiranje BitDefender računa

### Kreiranje računa

## Nimam še BitDefender računa

Za dostop do brezplačne BitDefender tehnične podpore in drugih storitev morate kreirati račun.



### Opomba

Če želite kasneje ustvariti račun, izberite pripadajočo možnost.

Za kreiranje BitDefender računa izberite možnost **Kreiraj nov BitDefender račun** in vnesite zahtevane podatke. Vnešeni podatki so zaupne narave.

- **E-pošta** - vnesite vaš e-poštni naslov.
- **Geslo** - vpišite geslo za vaš BitDefender račun.



### **Opomba**

Geslo mora biti dolgo vsaj štiri znake.

- **Ponoven vnos gesla** - ponovno vpišite geslo.
- **Ime** - vnesite vaše ime.
- **Priimek** - vnesite vaš priimek.
- **Država** - vnesite ime države, v kateri prebivate.



### **Opomba**

Uporabite vaš elektronski naslov in geslo za prijavo v vaš BitDefender račun na povezavi <http://myaccount.bitdefender.com>.

Za uspešno kreiranje vašega računa morate najprej aktivirati vaš elektronski naslov. Preverite vaš e-poštni naslov in sledite navodilom v e-sporočilu, poslanem od BitDefender registracijske službe.

Kliknite **Naprej**.

## **Že imam BitDefender račun**

BitDefender bo samodejno ugotovil, če imate že registriran BitDefender račun na vašem računalniku. V tem primeru le kliknite **Naprej**.

Če že imate aktiven račun, vendar ga BitDefender ne odkrije, izberite **Vpis v obstoječ BitDefender račun** in vnesite e-poštni naslov ter geslo računa.



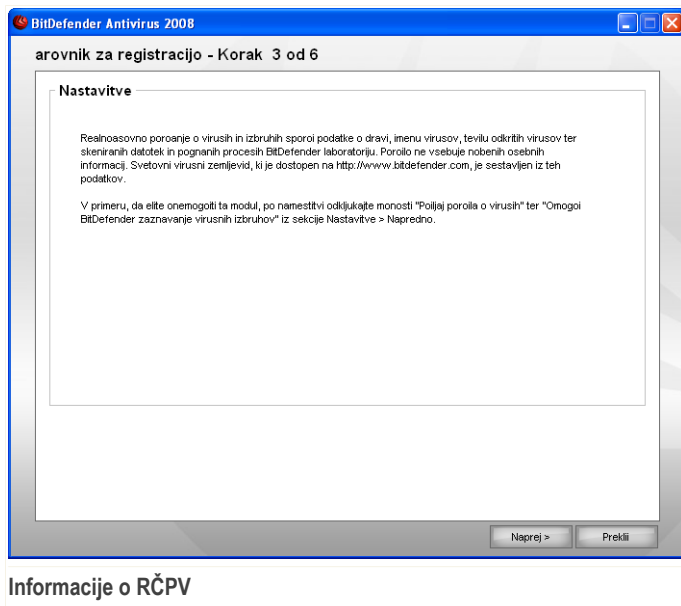
### **Opomba**

Če ste vpisali napačno geslo, bo sistem zahteval ponoven vpis, ko kliknete **Naprej**. Kliknite **V redu** za ponoven vpis ali **Prekliči** za izhod iz čarovnika.

Če ste pozabili geslo, kliknite **Ste pozabili geslo?** in sledite navodilom.

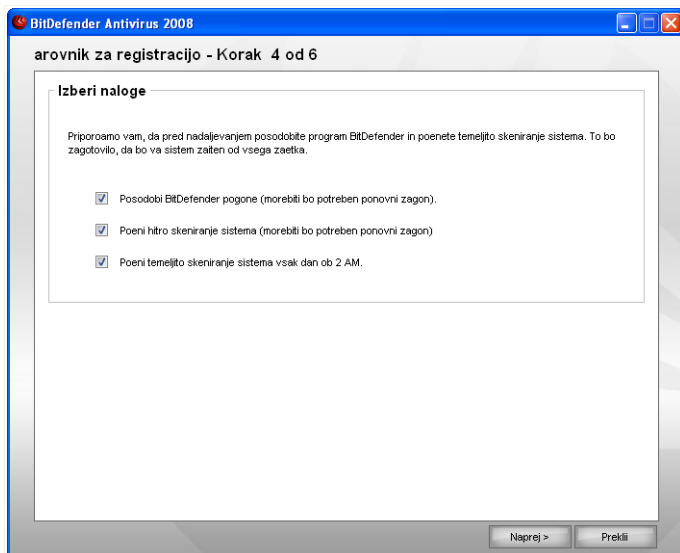
Kliknite **Naprej**.

### 1.3.3. Korak 3/6 - Več o RČPV



Kliknite **Naprej** za nadaljevanje ali **Prekliči** za izhod iz čarovnika.

## 1.3.4. Korak 4/6 – Izbira opravil



### Izbira opravila

Nastavite BitDefender Antivirus 2008 za opravljanje pomembnih nalog za varnost vašega sistema.

Možnosti so naslednje:

- **Posodobitev BitDefender pogonov (morebiti bo potreben ponoven zagon)** - med naslednjim korakom se bodo BitDefender pogoni posodobili in tako zaščitili vaš računalnik pred najnovejšimi grožnjami.
- **Poženi hitro skeniranje sistema (morebiti bo potreben ponoven zagon)** - med naslednjim korakom bo pognano hitro skeniranje sistema. Tako bo BitDefender preveril, ali vaše datoteke v mapah *Windows* in *Program Files* niso okužene.
- **Poženi polno skeniranje sistema vsak dan ob 2 AM** - požene polno skeniranje sistema vsak dan ob 2 AM.



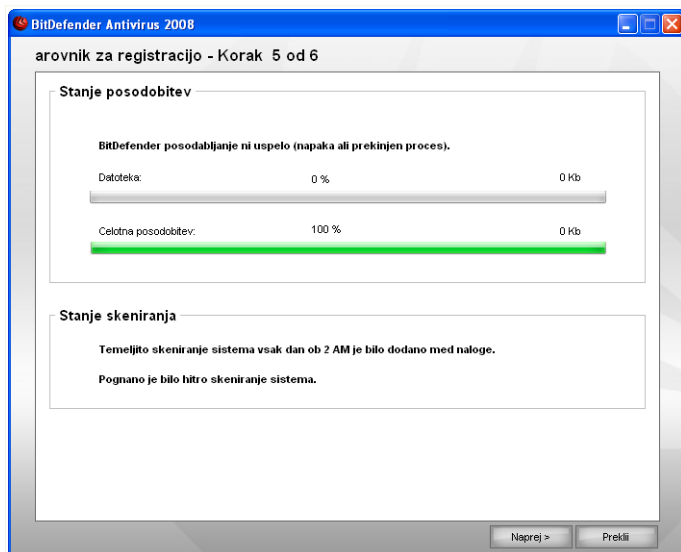
### **Pomembno**

Priporočamo vam, da omogočite naslednje možnosti pred nadaljevanjem na naslednji korak. S tem boste zagotovili visoko varnost vašega sistema.

Če izberete le zadnjo možnost ali nobene izmed možnosti, boste preskočili naslednji korak.

Kliknite **Naprej** za nadaljevanje ali **Prekliči** za izhod iz čarovnika.

### 1.3.5. Korak 5/6 - Čakanje na dokončanje opravil

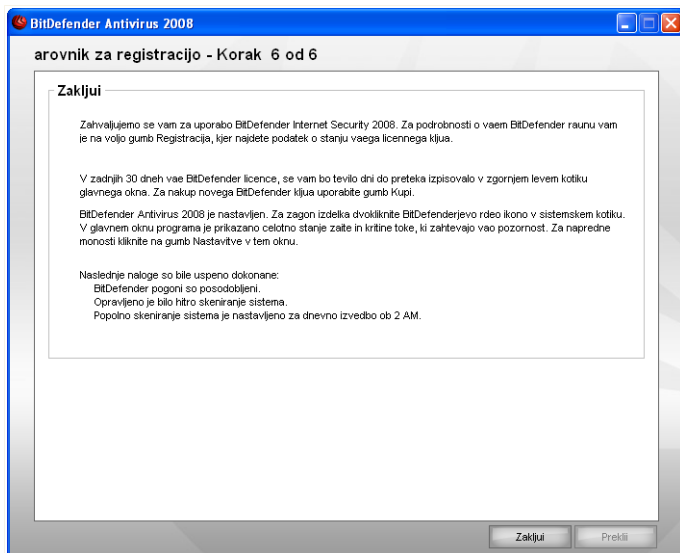


#### Stanje opravil

Počakajte, da se opravila dokončajo. Spremljate lahko stanje opravil, ki ste jih izbrali v prejšnjem koraku.

Kliknite **Naprej** za nadaljevanje ali **Prekliči** za izhod iz čarovnika.

## 1.3.6. Korak 6/6 - Povzetek



### Zaključni

To je zadnji korak namestitvenega čarovnika.

Kliknite **Končaj** za zaključek čarovnika in nadaljevanje namestitvenega procesa.

## 1.4. Nadgradnja

Za nadgradnjo BitDefenderja imate dvoje možnosti:

- **Namestitev brez odstranjevanja predhodne različice - za različice v8 ali novejše, Internet Security izvzet**

Dvokliknite namestitveno datoteko in sledite navodilom čarovnika, opis v delu "*Namestitveni koraki*" (p. 3).



### **Pomembno**

Med namestitvijo se lahko pojavi sporočilo o napaki, ki ga povzroči storitev Filespy. Kliknite **V redu** in nadaljujte z namestitvijo.

- **Odstranite prejšnjo različico in namestite novo - velja za vse BitDefender različice**

Najprej odstranite prejšnjo različico, ponovno zaženite računalnik in namestite novo, kot je opisano v razdelku "*Namestitveni koraki*" (p. 3).



#### **Pomembno**

Če nadgrajujete iz BitDefender v8 ali novejše različice, priporočamo, da shranite BitDefender nastavitve. Po nadgradnji jih boste znova naložili.

## 1.5. Odstranjevanje, popravilo ali spreminjanje BitDefenderja

Če želite spremeniti, popraviti ali izbrisati **BitDefender Antivirus 2008**, sledite poti iz Windows start menija: **Start** → **Programs** → **BitDefender 2008** → **Spremeni, popravi ali odstrani**.

Pozvani boste k potrditvi vaše izbire s klikom na gumb **Naprej**. Odprlo se bo novo okno, v katerem boste lahko izbrali:

- **Popravi** - ponovno namestite tiste komponente, ki ste jih namestili pri prejšnji namestitvi.

V kolikor izberete popravilo BitDefenderja, se pojavi novo okno. Kliknite **Popravi** za pričetek procesa samopopravila.

Ob opozorilu ponovno zaženite računalnik in nato kliknite **Namesti** za ponovno namestitev BitDefender Antivirus 2008.

Po končani namestitvi se bo pojavilo novo okno. Kliknite **Končaj**.

- **Odstrani** - izbrišete vse nameščene komponente.



#### **Opomba**

Za nemoteno ponovno namestitev predlagamo, da izberete **Odstrani**.

Če izberete to možnost, se bo pojavilo novo okno.



#### **Pomembno**

Z odstranitvijo BitDefender zaščite pred zlonamernim programjem, ne boste več zaščiteni pred zlonamernimi programskimi grožnjami, kot so virusi, vohunski programi, ipd.. V kolikor želite, da ostane Windows Defender omogočen, izberite ustrezno možnost. Ta možnost je na voljo samo za Windows Vista.

Kliknite **Odstrani** za pričetek odstranitve BitDefender Antivirus 2008 iz vašega računalnika.

Med odstranitvijo vam bomo dali možnost, da izrazite svoje mnenje o produktu, ki ga odstranjujete. Prosimo kliknite **V redu** za sodelovanje v raziskavi, ki je sestavljena iz petih kratkih vprašanj. V kolikor ne želite sodelovati v raziskavi kliknite **Prekliči**.

Ko je končan postopek namestitve, se pojavi novo okno. Kliknite **Končaj**.



#### **Opomba**

Priporočamo, da po končanem postopku odstranitve izbrišete tudi mapo BitDefender\Program Files.


### ***Pri odstranjevanju se je pojavila napaka.***

V kolikor je med postopkom odstranitve BitDefenderja prišlo do napake, se bo pojavilo novo okno. Kliknite **Zaženi orodje za odstranjevanje** za popolno odstranitev BitDefenderja iz vašega sistema. Orodje za odstranjevanje bo odstranilo vse datoteke in vnose v registru, ki niso bili odstranjeni med postopkom odstranjevanja.

# Osrednja administracija

## 2. Uvod

Po namestitvi BitDefenderja je vaš računalnik zaščiten. Odprete lahko BitDefender Security Center, kjer lahko preverite varnost sistema, določate preventivne ukrepe ali popoloma prenestavite izdelek.

Za dostop do BitDefender Security Center uporabite Windows Start meni in sledite poti **Start** → **Programs** → **BitDefender 2008** → **BitDefender Antivirus 2008** ali še hitreje, dvokliknite  **BitDefender ikono** v sistemskem kotičku.



### BitDefender Security Center

BitDefender Security Center je sestavljen iz dveh delov.

- **DelStanje** zajema podatke o ranljivostih in vam jih pomaga odpraviti. Tu tudi videti koliko zadev potrebuje vašo pozornost. S klikom na rdeč gumb **Odpravi vse težave** bodo odpravljene vse težave ali pa boste dobili navodila, kako preprosto rešiti težave. Na voljo so štiri gumbi stanja, ki se navezujejo na štiri varnostna področja. Zelen gumb stanja nakazuje, da ni nobenih težav, rumen in rdeč gumb, pa opozarjata na srednjo ali visoko nevarnost. Za odpravo težav enostavno kliknite

rumen/rdeč gumb in nato gumb **Popravi** posamezno ali gumb **Popravi vse** . Siva barva prikazuje komponente, ki niso nastavljene.

- **Hitra opravila** vam pomagajo ohraniti varnost sistema in omogočajo zaščito podatkov.

BitDefender Security Center vsebuje več uporabnih bližnjic.

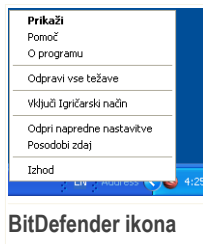
Povezave	Opis
<b>Kupi</b>	Odpre stran, kjer lahko kupite izdelek.
<b>Moj profil</b>	Odpre vaš BitDefender profil
<b>Prijava</b>	Odpre čarovnik za prijavo.
<b>Pomoč</b>	Odpre pomoč.
<b>Podpora</b>	Odpre stran za BitDefenderjevo podporo.
<b>Nastavitve</b>	Odpre vmesnik z naprednimi nastavitvami.
<b>Zgodovina</b>	Odpre okno z BitDefenderjevo zgodovino.

## 2.1. BitDefender ikona v sistemskem kotičku


Za hitrejše upravljanje z izdelkom, lahko uporabljate tudi ikono BitDefender v Sistemski vrstici.

Če dvokliknete to ikono, se bo odprl BitDefender Security Center . Desni klik odpre vsebinski meni, ki ponuja hitre upravljalne možnosti programa BitDefender:

- **Prikaži** - odpre BitDefender Security Center.
- **Pomoč** - odpre pomoč.
- **O Programu** - odpre vam spletno stran BitDefender.
- **Popravi vse težave** - pomaga pri odstranjevanju ranljivosti sistema.
- **Vključi/izključi Igričarski način** - vključi/izključi **Igričarski način**.
- **Napredne nastavitve** - omogočajo nastavitve protivirusnih možnosti.
- **Posodobi zdaj** - izvede takojšnjo posodobitev. Pojavi se novo okno, kjer lahko spremljate stanje posodobitev.
- **Izhod** - zapre aplikacijo.



Ob vključenem Igričarskem načinu se pojavi črka G nad  BitDefender ikono.

V primeru, da varnost vašega sistema ogroža kritična težava, se bo pojavil klicaj nad  BitDefender ikono. S premikom miškega kazalca nad ikono se vam prikaže število težav, ki vplivajo na varnost vašega sistema.

## 2.2. Vrstica aktivnosti skeniranja

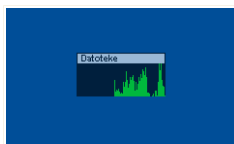
**Vrstica aktivnosti skeniranja** izrisuje grafični prikaz aktivnosti skeniranja na vašem sistemu.

Zeleni stolpci (**Datoteke**) prikazujejo število skeniranih datotek v sekundi, na lestvici od 0 do 50.



### Opomba

Vrstica aktivnosti skeniranja vas bo obvestila, kadar bo realnočasovna zaščita onemogočena, z rdečim križcem v delu **Datoteke**.



Vrstica aktivnosti

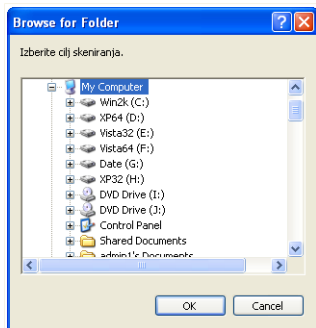
Odpravite se na razdelek **Pot skeniranja** in izberite stvari, ki jih želite skenirati. Oglejte si "**Povleci in izpusti skeniranje**" (p. 65) razdelek.

Ko ne želite več videti grafičnega prikaza, samo kliknite nanj z desnim miškinim gumbom in izberite možnost **Izhod**.

## 2.3. BitDefender ročno skeniranje

V kolikor želite hitro skenirati določeno mapo, lahko uporabite BitDefender ročno skeniranje.

Za dostop do ročnega skeniranja BitDefender uporabite Windows Start meni, **Start** → **Vsi programi** → **BitDefender 2008** → **BitDefender ročno skeniranje** Odprlo se bo novo okno:



BitDefender ročno skeniranje

Vse kar morate storiti je, da prebrskate mapo, izberete datoteko, ki jo želite skenirati in kliknete **V redu**. Pojavil se bo **Skener BitDefender**, ki vas bo vodil skozi postopek skeniranja.

## 2.4. Igričarski način

Nov ogričarski način začasno spremeni zaščitne nastavitve, kar minimalizira obremenitev računalnika in tako zagotovi varno in zabavno igričarsko izkušnjo. Igričarski način spremeni naslednje nastavitve:

- Prepreči vsa pojavna okna BitDefender.
- Stopnja realnočasovne zaščite je nastavljena na **Strpen**.

Ob vključenem Igričarskem načinu se pojavi črka **G** nad  BitDefender ikono.

### 2.4.1. Uporaba igričarskega načina

Za vključitev Igričarskega načina uporabimo eno izmed naslednjih metod:

- Desno kliknete BitDefenderjevo ikono v sistemskem kotičku in izberite možnost **Vključi Igričarski način**.
- Pritisnite **Alt+G** (prednastavljena hitra tipka).



#### **Pomembno**

Ne pozabite izključiti Igričarski način, ko končate. Uporabite iste metode, kot za vključitev.

## 2.4.2. Spreminjanje hitre tipk za igričarski način

Za spreminjanje hitre tipke sledite naslednjim korakom:

1. Kliknite **Nastavitve** - v BitDefender Varnostnem centru.



### **Opomba**

Desno kliknite BitDefenderjevo ikono v sistemskem kotičku in izberite **Napredne nastavitve**.

2. Kliknite **Napredno**.

3. V delu **Vključi Igričarski načines** izberite željeno hitro tipko:

- Izberite tipko, ki jo želite uporabiti in obkljukajte eno izmed naslednjih: Control (Ctrl), Shift (Shift) or Alternate(Alt).
- V polje za urejanje vpišite črko, ki jo želite uporabljati za hitro tipko.

Naprimera če želite uporabiti hitre tipke Ctrl+Alt+D morate izbrati Ctrl in Alt te vpisati D.



### **Opomba**

Za izključitev hitrih tipk odkljukajte **Omogoči hitro tipko za Igričarski način**

### 3. Stanje zaščite

Stanje zaščite prikazuje sistematično urejeno in lahko upravljano seznam varnostnih ranljivosti vašega računalnika. BitDefender Antivirus 2008 vas obvesti o vsaki težavi, ki lahko vpliva na varnost vašega računalnika.

Obstajajo štiri gumbi stanja zaščite:

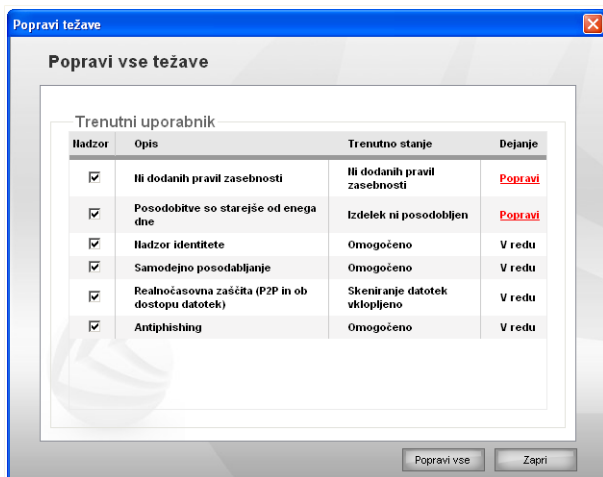
- **ANTIVIRUS**
- **ANTIPHISHING**
- **NADTOR ZASEBNOSTI**
- **POSODOBITVE**

Obenem lahko na levi vidite število težav, ki vplivajo na varnost vašega sistema in rdeč gumb **Popravi vse**

Štiri gumbi stanja so prikazani v zeleni, rumeni, rdeči ali sivi barvi, odvisno od trenutne stopnje zaščite.

- **Zelena** označuje nizko varnostno tveganje na vašem računalniku.
- **Rumena** označuje zmerno varnostno tveganje na vašem računalniku.
- **Rdeča** označuje visoko varnostno tveganje na vašem računalniku.
- **Siva** označuje neaktivne komponente.

Odprava vseh težav je možna že z enim klikom na gumb **Odpravi vse težave** Odprlo se bo novo okno



### Varnostne težave

Videli boste seznam varnostnih težav in kratek opis stanja teh težav.

Za odpravo individualnih težav kliknite na pripadajoč gumb **Popravi**. Težava bo odpravljena na mestu ali pa preko čarovnika. V kolikor se odločite, da odpravite vse težave hkrati kliknite gumb **Popravi vse** in sledite navodilom čarovnika.

Če potrebujete dodatno pomoč, kliknite na gumb **Več pomoči**, ki se nahaja na spodnjem delu okna. Prikaže se kontekstualna stran s pomočjo, ki postreže s podrobnimi podatki o težavah in navodili, kako jih odpraviti.



#### **Pomembno**

Za vsako težavo je na voljo možnost označevanja. V kolikor ne želite obravnavati določenih težav, odznačite pripadajoči predel. Prisomi, da uporabljate to možnost skrajno pazljivo, ker lahko hitro povečate varnostno tveganje, ki mu je izpostavljen vaš računalnik.

V kolikor želite težave odpraviti kasneje kliknite **Zapri**.

## 3.1. Gumb stanja Antivirus

V kolikor je gumb stanja Antivirus zelen, ni razlogov za skrbi. V kolikor pa je rumen, rdeč ali siv, pa obstaja zmerno ali visoko varnostno tveganje na vašem računalniku.

Barva gumbov stanja se lahko spreminja tudi kadar n eopravljate določenih pomembnih opravil- Naprimer, če je od zadnjega skeniranja sistema že poteklo dalj časa, se gumb obarva rumeno, v kolikor pa je poteklo preveč časa od zadnjega skeniranja pa bo gumb obarvan rdeče.

V spodnji tabeli so na voljo informacije o zajetih elementih pri ugotavljanju varnostnih tveganj.

<b>Težava</b>	<b>Barva</b>
Od zadnjega skeniranja sistema je preteklo že dalj časa.	Rumena
Od zadnjega skeniranja sistema je preteklo že zelo veliko časa.	Rdeča
Realnočasovna zaščita je onemogočena	Rdeča
Stanje protivirusne zaščite je nastavljeno na dovolji vse.	Rumena

Za odpravo težav sledite tem korakom:

1. Kliknite na gumb stanja Antivirus.
2. Kliknite gumb **Popravi** za odpravo posamezne težave ali pa kliknite gumb **Popravi vse** za odpravo vseh težav hkrati.
3. V kolikor težava ni odpravljena na mestu, sledite čarovniku za odpravo težav.

## 3.2. Gumb stanja Antiphishing

V kolikor je gumb stanja Antiphishing zelen, ni razloga za skrbi. Če je gumb rdeč ali siv obstaja visoko varnostno tveganje za vaš računalnik.

V spodnji tabeli so na voljo informacije o zajetih elementih pri ugotavljanju varnostnih tveganj.

<b>Težava</b>	<b>Barva</b>
Zaščita Antiphishing je omogočena	Zelana
Zaščita Antiphishing je onemogočena	Rdeča

Za odpravo težav sledite tem korakom:

1. Kliknite gumb stanja Antiphishing
2. Kliknite gumb **Popravi** za odpravo posamezne težave ali pa kliknite gumb **Popravi vse** za odpravo vseh težav hkrati.

3. V kolikor težava ni odpravljena na mestu, sledite čarovniku za odpravo težav.

### 3.3. Gumb stanja nadzora zasebnosti

V kolikor je Gumb stanja Zasebnost zelen, ni razlogov za skrbi. Če pa je gumb rdeč ali siv, pa je računalnik izpostavljen visokemu varnostnemu tveganju.

V spodnji tabeli so na voljo informacije o zajetih elementih pri ugotavljanju varnostnih tveganj.

Težava	Barva
Varovanje zasebnosti je pripravljeno in aktivno.	Zelana
Varovanje zasebnosti je pripravljeno in neaktivno.	Rdeča
Zaščita zasebnosti ni pripravljena.	Siva

Za odpravo težav sledite tem korakom:

1. Kliknite gumb stanja Nadzor zasebnosti
2. Kliknite gumb **Popravi** za odpravo posamezne težave ali pa kliknite gumb **Popravi vse** za odpravo vseh težav hkrati.
3. V kolikor težava ni odpravljena na mestu, sledite čarovniku za odpravo težav.

### 3.4. Gumb stanja Posodobitev

V kolikor je gumb stanja Posodobitev zelen ni razloga za skrbi. Če je gumb rdeč, je vaš računalnik izpostavljen visokemu varnostnemu tveganju.

V spodnji tabeli so na voljo informacije o zajetih elementih pri ugotavljanju varnostnih tveganj.

Težava	Barva
Samodejno posodabljanje je omogočeno	Zelana
Samodejno posodabljanje je onemogočeno	Rdeča
Zadnja posodobitev je stara en dan.	Rdeča

Za odpravo težav sledite tem korakom:

1. Kliknite gumb stanja Posodobitev.

- 
2. Kliknite gumb **Popravi** za odpravo posamezne težave ali pa kliknite gumb **Popravi vse** za odpravo vseh težav hkrati.
3. V kolikor težava ni odpravljena na mestu, sledite čarovniku za odpravo težav.

## 4. Hitra opravila

Pod štirimi gumbi stanja je del **Hitra opravila**

### 4.1. Zaščita

BitDefender zajema modul Zaščita, ki vam pomaga pri posodabljanju in zaščiti računalnika pred virusi.

Za vstop v modul Zaščita kliknite zavihek **Zaščita**.

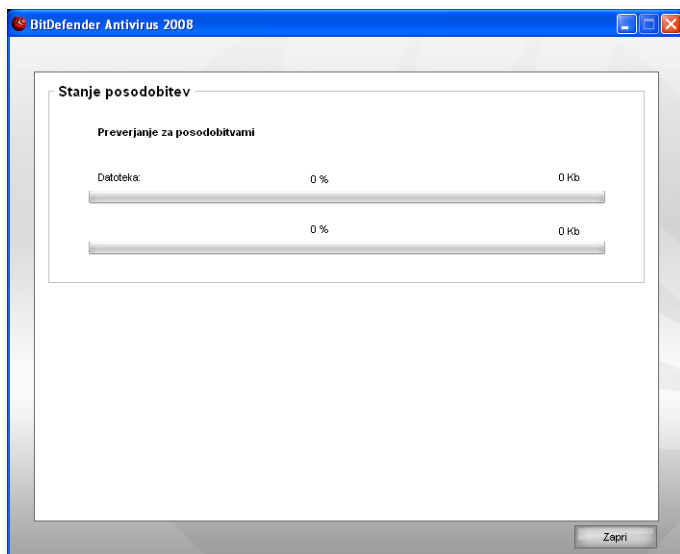
Na voljo so naslednji gumbi:

- **Posodobi zdaj** - izvede takojšnjo posodobitev.
- **Skeniraj Moje Dokumente** - hitro skeniranje mape Moji Dokumenti
- **Globoko sistemsko skeniranje**- popolno skeniranje sistema.
- **Popolno sistemsko skeniranje**- popolno skeniranje sistema.

#### 4.1.1. Posodabljanje BitDefenderja

Novi virusi so odkriti in prepoznani vsak dan. Zato je ključnega pomena, da je Bitdefender redno posodobljen z vsemi novimi definicijami virusov. Privzeti čas BitDefenderja za preverjanje novih posodobitev je uro.

Če ste povezani na internet preko širokopasovne povezave, oz. ADSLa, bo Bitdefender skrbel sam zase. Ko se boste povezali na internet, bo sam pregledal za posodobitev in vsake **ura** za tem. Sami lahko izvedete posodobitev s klikom na **Posodobi zdaj**. Prišel se bo postopek posodobitve. Pojavilo se bo naslednje okno:



### Posodabljanje BitDefenderja

V oknu lahko vidite stanje posodobitev.

Pri posodobitvah se datoteke nadomeščajo progresivno. Na ta način preprečimo napake v delovanju produkta in izključimo ranljivost zaradi posodabljanja programa.

Če želite zapreti okno kliknite **Zapri**. To ne bo prekinilo postopka posodobitve.



#### Opomba

Če ste na internet povezani preko klicne povezave, bi bilo primerno, da spremenite nastavitve tako, da boste sami pregledovali za posodobitve.

**Ponovno zaženite računalnik, če je to potrebno.** V primeru večjih posodobitev boste morali ponovno zagnati računalnik. V kolikor ne želite biti ponovno opomnjeni, da morate potrditi vašo izbiro med to sejo kliknite **Ne vprašaj več med to sejo**. Na ta način bo izdelek vedno počakal na ponovni zagon.

Kliknite **Ponovno zaženi** za ponoven zagon računalnika.

V kolikor ne želite kasneje ponovno zagnati računalnik kliknite **V redu**. Priporočamo, da čimprej izvedete ponovni zagon računalnika.

## 4.1.2. Skeniranje z BitDefenderjem

Če želite izvesti skeniranje poženite posamzne naloge s klikom na pripadajoči gumb. Naslednja preglednica zajema razpoložljive naloge skeniranja in njihov kratek opis.

Naloga	Opis
<b>Skeniraj Moji Dokumenti</b>	To opravilo vam skenira pomembne mape: My Documents, Desktop in StartUp. Na ta način si zagotovite varnost vaših dokumentov in varno delovno mesto. Na ta način si zagotovite varnost vaših dokumentov in varno delovno mesto.
<b>Globoko skeniranje</b>	<b>systemsko</b> Skenira celoten sistem V prednastavljeni konfiguraciji skenira za vsemi oblikami zlonamerne programja, kot so virusi, wohunski programi, rootkiti, itd..
<b>Popolno sistema</b>	<b>skeniranje</b> Pregleda celoten sistem, razen arhivov. V prednastavljeni konfiguraciji skenira za vsemi oblikami zlonamerne programja, kot so virusi, wohunski programi, rootkiti, itd..



### Opomba

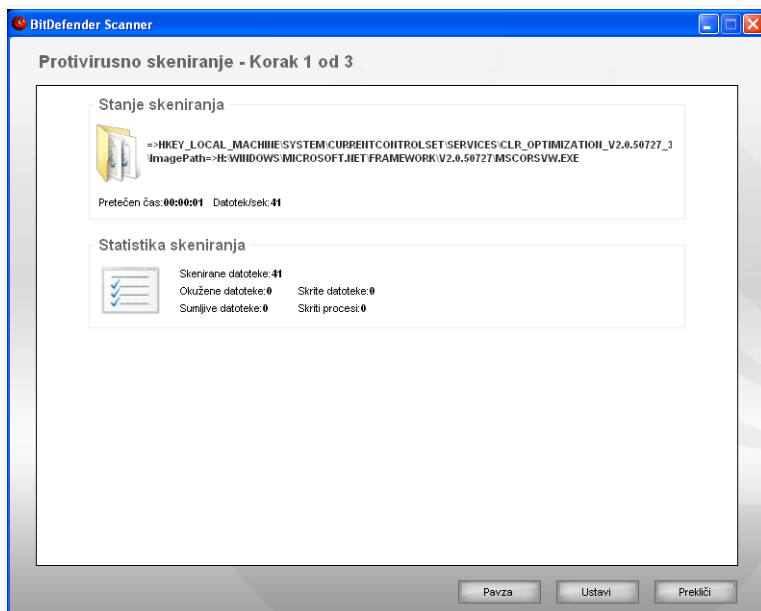
Ker opravili **Globoko skeniranje sistema** in **Popolno skeniranje sistema** pregledata celoten sistem, lahko traja nekaj časa, zato vam predlagamo, da izvajate skeniranje kadar ne uporabljate računalnika.

Ko poženete skeniranje na zahtevo, hitro ali celovito, se pojavi Skener BitDefender.

Sledite trem korakom vodenega postopka za zaključitev postopka skeniranja.

### Korak 1/3 – Skeniranje

BitDefender bo začel skenirati izbrane objekte.



## Skeniranje

Vidite lahko stanje skeniranja in statistiko (hitrost skeniranja, preostali čas, število skeniranih / okuženih/ sumljivih/ skritih predmetov in ostalo).



### Opomba

Proces bo lahko trajal kar nekaj minut, odvisno od obsega skeniranja.

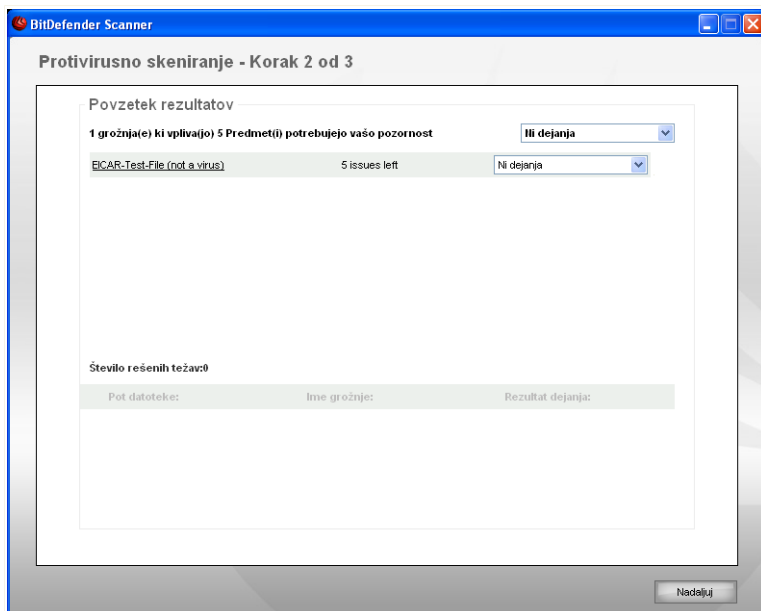
Za začasno prekinitvev postopka skeniranja kliknite **Pavza**. Za nadaljevanje skeniranja morate klikniti **Nadaljuj**

Skeniranje lahko ustavite kadarkoli s klikom na **Ustavi** & **Da**. Nadaljujete na zadnjem koraku čarovnika.

Počakajte, da BitDefender zaključi skeniranje.

## Korak 2/3 – Izberite dejanje

PO zaključku skeniranja se pojavi novo okno kjer lahko pregledate rezultate skeniranja.



## Dejanje

Razvidno je število težav, ki vplivajo na vaš sistem.

Okuženi predmeti so prikazani v skupini, glede na zlonamerni program, ki jih je okužil. Kliknite pripadajočo povezavo več informacij o okuženih predmetih.

Izbirate lahko med dejanji, ki vplivajo na vse skupine težav ali pa izberete posamezno dejanje za vsako težavo.

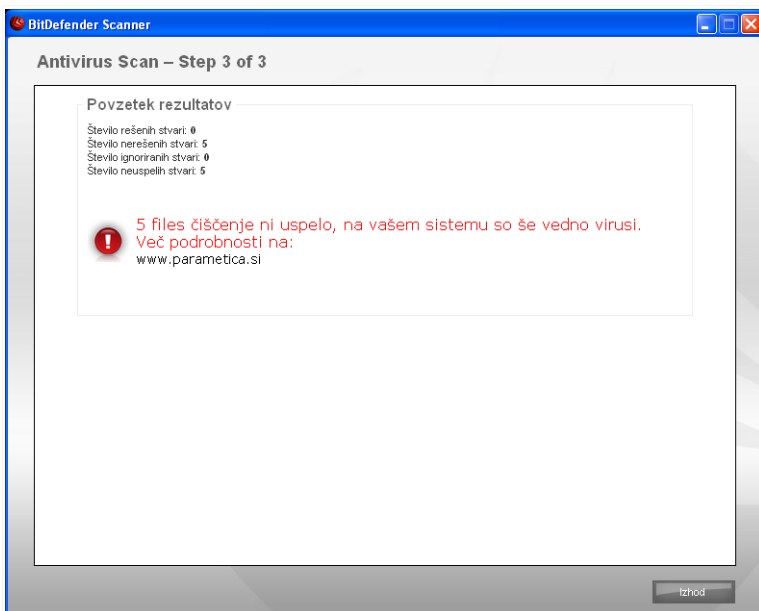
Možnosti so naslednje:

Dejanje	Opis
Ne ukrepaj	Nobeno dejanje ne bo uporabljeno pri okuženih datotekah.
Očisti	Očisti okužene datoteke.
Izbriši	Izbriše zoznane datoteke
Razkrij	Skriti predmeti postanejo vidni.

Kliknite **Nadaljuj** za izvedbo določenega dejanja.

### Korak 3/3 – Ogled rezultatov

Ko BitDefender popravi težave se pojavi novo okno z rezultati skeniranja.



#### Povzetek

Tu lahko vidite povzetek rezultatov. Dokument s poročilom o skeniranju je samodejno shranjen v odseku **Poročilo skeniranja** v delu **Lastnosti**.



#### **Pomembno**

Če je potrebno, ponovno zaženite računalnik za dokončanje procesa čiščenja.

Kliknite **Izhod** za zaprtje okna z rezultati.

### **BitDefender ni uspel odpraviti nekaterih težav**

V večini primerov BitDefender uspešno očisti odkrite okužene datoteke ali izolira okužbo. Vendar vseeno obstajajo težave, ki jih ni moč odpraviti.

V teh primerih vam priporočamo, da se obrnete na BitDefenderjevo podporo na [www.bitdefender.com](http://www.bitdefender.com). Naši strokovnjaki tehnične podpore vam bodo pomagali odpraviti težave, s katerimi se soočate.

### **BitDefender je izbrisal datoteke, zaščitene z geslom.**

Kategorija z geslom zaščitene datoteke vsebuje dve vrsti vnosov: arhivske in namestitvene datoteke. Te datoteke ne predstavljajo večje nevarnosti za sistem, razen v primeru, ko vsebujejo okužene datoteke in so pograne.

Prepričajte se, da so naslednje datoteke čiste:

- Če je datoteka, zaščitena z geslom, arhivska datoteka, ki ste jo zaščitili z geslom, odpakirajte vsebovane datoteke in jih skenirajte ločeno. Najenostavnejši način za skeniranje datotek je klik z desnim miškinim gumbom in izbira **BitDefender Antivirus 2008** iz menija.
- Če je z geslo zaščitena datoteka namestitveni program, se prepričajte, da je **realnočasovna zaščita** omogočena preden zaženete namestitveno datoteko. Če je namestitvena datoteka okužena, bo BitDefender izoliral okužbo.

Če ne želite, da BitDefender ponovno odkriva te datoteke, jih dodajte kot izjeme v proces skeniranja. Za dodajanje izjem skeniranja kliknite **Nastavitve** za odprtje konzole z nastavitvami in nato izberite **Antivirus > Izjeme**. Za dodatne informacije se obrnite na **Datoteke, izvzete iz skeniranja**.

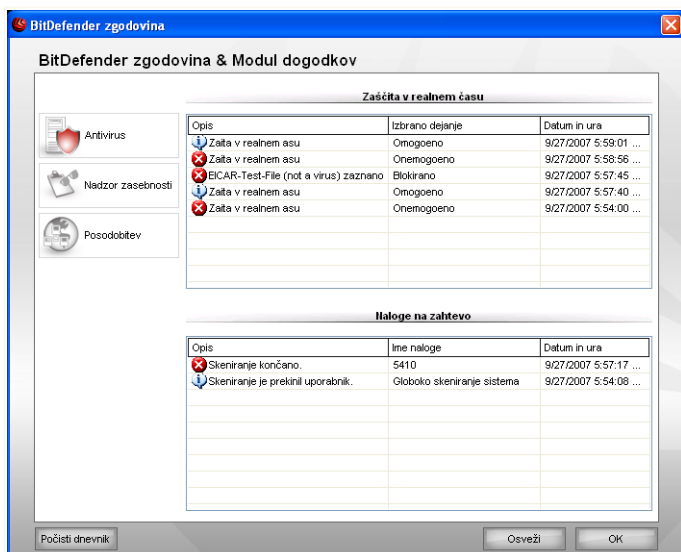
### **BitDefender je izbrisal sumljive datoteke**

Sumljive datoteke so zaznane s hevrističnim filtrom in lahko vsebujejo zlonamerno programje, za katerega protivirusni podpisi še niso na voljo.

Če skeniranje odkrije sumljive datoteke, vas bo pozvalo k pošiljanju le-teh v BitDefender Laboratorij. Kliknite **V redu** za pošiljanje teh datotek v nadaljnjo analizo v BitDefender Laboratorij.

## 5. Zgodovina

Povezava **Zgodovina** na dnu BitDefender Security Centra odpre novo okno z BitDefender zgodovino&dogodki. To okno vam omogoča pregled dogodkov povezanih z varnostjo. Preverite lahko potek posodobitev, najdeno zlonamerno programje, itd..



### Dogodki

Za lažje prečiščevanje BitDefender zgodovine&dogodki. so na levi navedene naslednje kategorije.

- **Antivirus**
- **Nadzor zasebnosti**
- **Posodobitve**

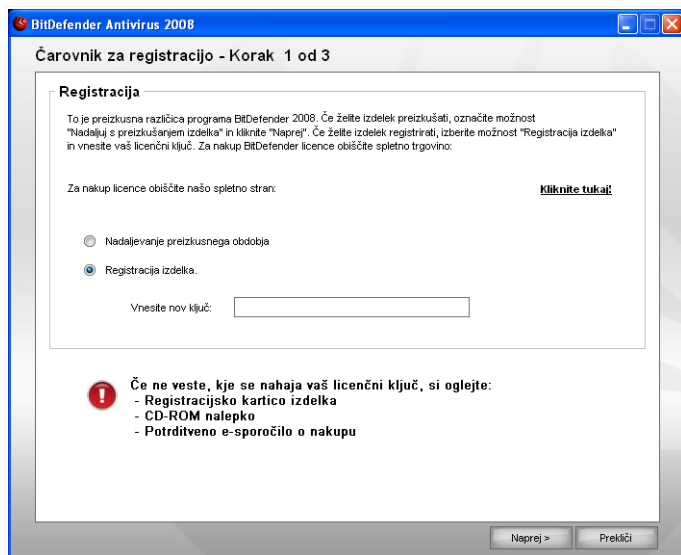
Seznam dogodkov je na voljo za vsako kategorijo. Vsak dogodek spremljajo naslednji podatki: kratek opis, dejanje, ki ga je izvedel BiDefender, ko se je dogodek pripetil ter datum in čas dogodka. Če želite več informacij o dogodku, dvokliknite na izbran dogodek na seznamu.

Kliknite **Počisti vnos** ali **Osveži**.

## 6. Registracija

BitDefender Antivirus 2008 je na voljo kot 30-dnevna preizkusna različica. Če želite registrirati BitDefender Antivirus 2008 ali spremeniti licenčni ključ oziroma kreirati BitDefender račun, kliknite na povezavo **Registracija**, ki se nahaja na vrhu okna BitDefender varnostnega središča. Pojavil se bo čarovnik za pomoč pri registraciji.

### 6.1. Korak 1/3 - Registracija BitDefender Antivirus 2008



#### Registracija

Če nimate BitDefender licence, kliknite na povezavo, ki vas bo vodila do BitDefender spletne trgovine za nakup licenčnega ključa.

Za registracijo BitDefender Antivirus 2008 izberite možnost **Registriraj izdelek** in vnesite licenčni ključ v polje **Vnesi nov ključ**.

Če preizkusno obdobje še ni poteklo, za nadaljevanje preizkušanja izberite možnost **Nadaljaj s preizkušanjem izdelka**.

Kliknite **Naprej**.

## 6.2. Korak 2/3 - Kreiranje BitDefender računa

**Čarovnik za registracijo - Korak 2 od 3**

**Registracija izdelka**

S kreiranjem BitDefender računa ali prijavo v obstoječ račun pridobite dostop do tehnične podpore, varne hrambe licenčnega ključa ter posebnih ponudb in promocij.

Prijava v obstoječ BitDefender račun

E-pošta:

Geslo:  [Ste pozabili geslo?](#)

Kreiranje novega BitDefender računa

E-pošta:

Geslo:

Ponovno vnesite geslo:

Ime:

Priimek:

Država:

Izdelaj račun kasneje

**Kreiranje računa**

### Nimam še BitDefender računa

Za dostop do brezplačne BitDefender tehnične podpore in drugih storitev morate kreirati račun.



#### Opomba

Če želite kasneje ustvariti račun, izberite pripadajočo možnost.

Za kreiranje BitDefender računa izberite možnost **Kreiraj nov BitDefender račun** in vnesite zahtevane podatke. Vnešeni podatki so zaupne narave.

- **E-pošta** - vnesite vaš e-poštni naslov.
- **Geslo** - vpišite geslo za vaš BitDefender račun.



**Opomba**

Geslo mora biti dolgo vsaj štiri znake.

- **Ponoven vnos gesla** - ponovno vpišite geslo.
- **Ime** - vnesite vaše ime.
- **Priimek** - vnesite vaš priimek.
- **Država** - vnesite ime države, v kateri prebivate.



**Opomba**

Uporabite vaš elektronski naslov in geslo za prijavo v vaš BitDefender račun na povezavi <http://myaccount.bitdefender.com>.

Za uspešno kreiranje vašega računa morate najprej aktivirati vaš elektronski naslov. Preverite vaš e-poštni naslov in sledite navodilom v e-sporočilu, poslanem od BitDefender registracijske službe.

Kliknite **Naprej**.

## Že imam BitDefender račun

BitDefender bo samodejno ugotovil, če imate že registriran BitDefender račun na vašem računalniku. V tem primeru le kliknite **Naprej**.

Če že imate aktiven račun, vendar ga BitDefender ne odkrije, izberite **Vpis v obstoječ BitDefender račun** in vnesite e-poštni naslov ter geslo računa.



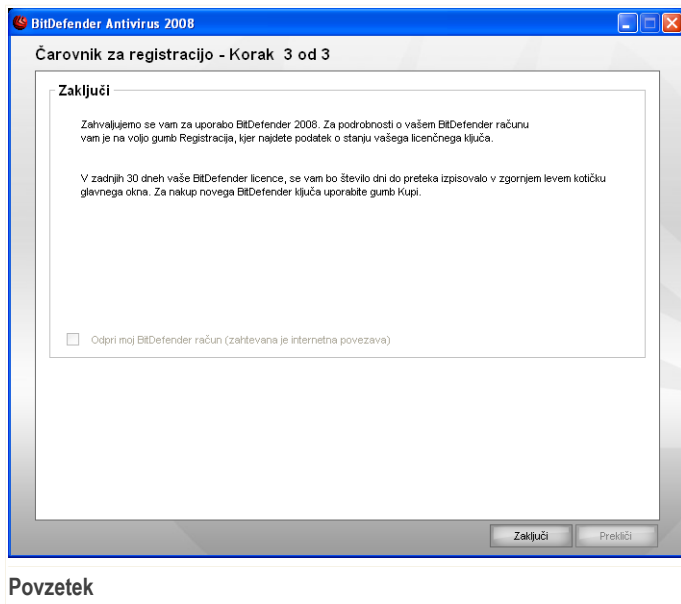
**Opomba**

Če ste vpisali napačno geslo, bo sistem zahteval ponoven vpis, ko kliknete **Naprej**. Kliknite **V redu** za ponoven vpis ali **Prekliči** za izhod iz čarovnika.

Če ste pozabili geslo, kliknite **Ste pozabili geslo?** in sledite navodilom.

Kliknite **Naprej**.

## 6.3. Korak 3/3 - Registracija BitDefender Antivirus 2008



Izberite **Odpri moj BitDefender račun** za dostop do vašega BitDefender računa. Potrebovali boste internetno povezavo.

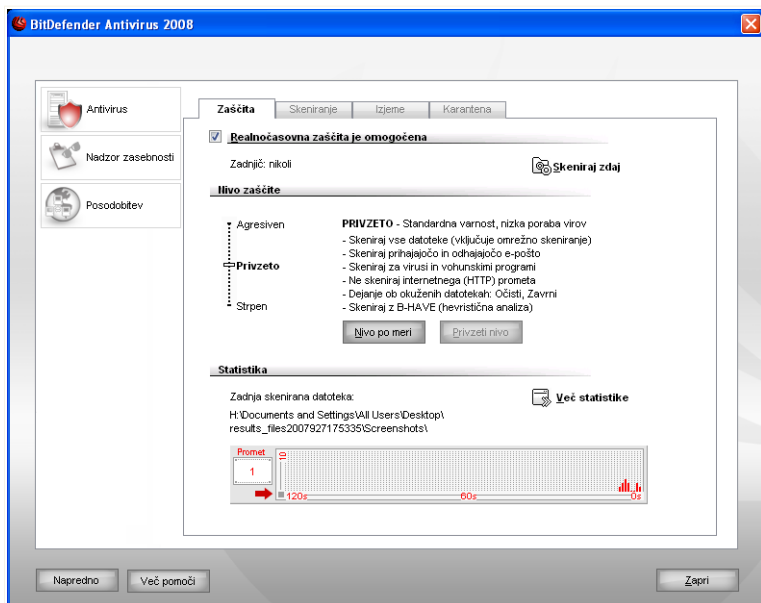
Kliknite **Zaključí** za zaprtje okna.

# **Napredna varnostna administracija**

## 7. Vmesnik nastavitvev

**BitDefender Antivirus 2008** vsebuje centralni vmesnik, od koder lahko uporabljate napredne nastavitve in administrirate BitDefender.

Za dostop do vmesnika za nastavitve kliknite **Nastavitve**.



Vmesnik nastavitvev

Na voljo so različni moduli: **Antivirus**, **Nadzor zasebnosti** in **Posodobitev**. To vam omogoča lažje upravljanje z BiDefenderjem osnovano na vrsti varnostnih težav.

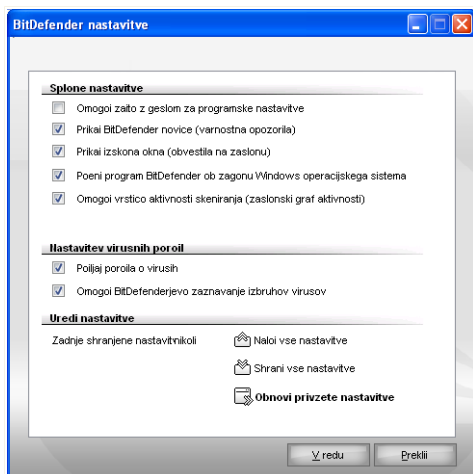
Na levi strani upravljaljske konzole se nahaja izbirnik modulov:

- **Antivirus** - v tem razdelku lahko nastavite modul **Antivirus**.
- **Nadzor zasebnosti** - v tem razdelku lahko nastavite modul **Nadzor zasebnosti**.
- **Posodobitev** - v tem razdelku lahko nastavite modul **Posodobitev**.

Če potrebujete dodatno pomoč, kliknite na gumb **Več pomoči**, ki se nahaja na spodnjem delu okna. Prikaže se kontekstualna stran s pomočjo in vam ponudi podrobne informacije o razdelku, v katerem se nahajate.

## 7.1. Spreminjanje splošnih nastavitev

Za spreminjanje splošnih nastavitev v BitDefender Antivirus 2008 in za upravljanje njegovih nastavitev kliknite **Napredno**. Odrplo se bo novo okno



### Nastavitve poročil

Tu lahko nastavljate splošno obnašanje programa BitDefender. Po privzetih nastavitvah se BitDefender samodejno zažene ob zagonu Windows-ov in se izvaja minimizirano v "sistemskem kotičku".

#### 7.1.1. Nastavitve poročil

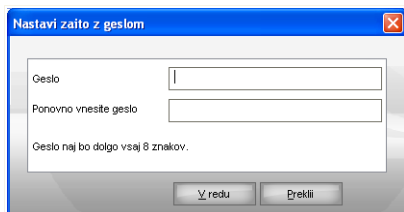
- **Omogoči zaščito z geslom** - omogoči zaščito BitDefender nastavitev z geslom.



#### Opomba

Če niste edini uporabnik računalnika, je priporočljivo, da si z geslom zaščitite svoje nastavitve programa BitDefender.

Če izberete to možnost, se bo pojavilo naslednje okno:



### Potrditev gesla

V polje **Geslo** vnesite geslo, potem pa ga še enkrat vtipkajte v polje **Ponovni vnos gesla** in kliknite **V redu**.

Če boste želeli spreminjati nastavitve zaščite z geslom, boste morali predhodno vpisati geslo. Geslo velja tudi za ostale administratorje sistema (če obstajajo).



### Pomembno

Če ste pozabili geslo, morate uporabiti funkcijo popravi, za ponovno pridobitev nadzora nad nastavitvami.

- **Sprejemanje varnostnih opozoril** - občasno iz BitDefenderjevih strežnikov prejmete varnostna opozorila o virusnih izbruhih.
- **Prikaži opombe** - prikaže izskočna (t.i. pop-up) okna o stanju programa.
- **Poženi program BitDefender ob zagonu Windows operacijskega sistema** - samodejno zažene BitDefender ob zagonu Windows-ov. Priporočamo, da ohranite to možnost izbrano.
- **Omogoči orodno vrstico dejavnosti skeniranja (prikaz aktivnosti skeniranja)** - prikaže orodno vrstico **Vrstica skeniranja** ob vsaki prijavi v Okna. Počistite to okno, če ne želite, da se orodna vrstica z aktivnostjo skeniranja prikazuje.



### Opomba

To možnost je moč nastaviti le za trenutno uporabljeni Windows uporabniški račun.

- **Omogoči hitro tipko za Igričarski način** - omogoča uporabo hitrih tipk za vklop in izklop Igričarskega načina. Prednastavljena hitra tipka je **Alt+G**.

Za spreminjanje hitre tipke naredite naslednje:

1. Obkljukajte željeno: Control (**Ctrl**), Shift (**Shift**) ali Alternate (**Alt**).
2. V polje za urejanje vpišite črko, ki jo želite uporabljati za hitro tipko.

## 7.1.2. Nastavitve virusnih poročil



- **Pošiljaj poročila o virusih** - pošlje poročilo o virusu v BitDefender laboratorije. Tako pomaga odkrivati izbruhe novih virusov.

Poročila ne vsebujejo nobenih zaupnih podatkov, kot so vaše ime, IP naslov, ipd. Poročila ne bodo uporabljena v komercialne namene. Poslane informacije vključujejo le ime virusa in so uporabljene izključno v statističnih poročilih.

- **Pošiljaj poročila o virusih** - pošlje poročilo o virusu v BitDefender laboratorije. Tako pomaga odkrivati izbruhe novih virusov.

Poročila ne vsebujejo nobenih zaupnih podatkov, kot so vaše ime, IP naslov, ipd. Poročila ne bodo uporabljena v komercialne namene. Poslane informacije vključujejo le ime virusa in so uporabljene izključno v statističnih poročilih.

## 7.1.3. Upravljalnje z nastavitvami

Uporabite gumba  **Shrani vse nastavitve** /  **Naloži vse nastavitve** za shranitev / nalaganje nastavitve programa BitDefender. Tako lahko ob ponovni namestitvi ali popravilu programa BitDefender hitro uporabite shranjene nastavitve.



### **Pomembno**

Samo uporabniki z administratorskimi pravicami lahko spreminjajo in shranjujejo nastavitve.

Za obnovo privzetih nastavitve kliknite na  **Obnova privzetih nastavitvev**.

## 8. Protivirusna zaščita

Bitdefender vas štiti pred vsemi oblikami zlonamernega programja ( virusi, trojanci, vohunski programi, rootkiti, itd.).

Uporabljeno bo metodično skeniranje datotek. Cilj tega skeniranja je odkriti še neznane viruse, glede na določene vzorce in algoritme. Možni so lažni alarmi. Ko je takšna datoteka odkrita, je označena kot sumljiva. V tem primeru, vam priporočamo, da datoteko pošljete v pregled v BitDefender laboratorije, kjer jo bodo strokovnjaki podrobno analizirali.

Zaščita pred virusi je razdeljena na dve metodi:

- **Skeniranje ob dostopu** - prepreči novim grožnjam, ki prihajajo na vaš sistem. To se imenuje tudi realnočasovna zaščita- datoteke so skenirane ob uporabi-ob dostopu Bitdefendr bo naprimer skeniral Word dokument ko ga odprete in e-pošto, ko jo prejmete.
- **Skeniranje na zahtevo** - omogoča zaznavo in odstranitev zlonamernega programja, ki je že na vašem sistemu. Gre za klasično skeniranje, ki ga sproži uporabnik, ki izbere kateri trdi disk, mapo ali datoteko želi skenirati. Opravila skeniranja vam omogoča kreiranje prilagojenih rutin skeniranja, ki jih lahko uredimo v urnik, tako da se redno izvajajo.

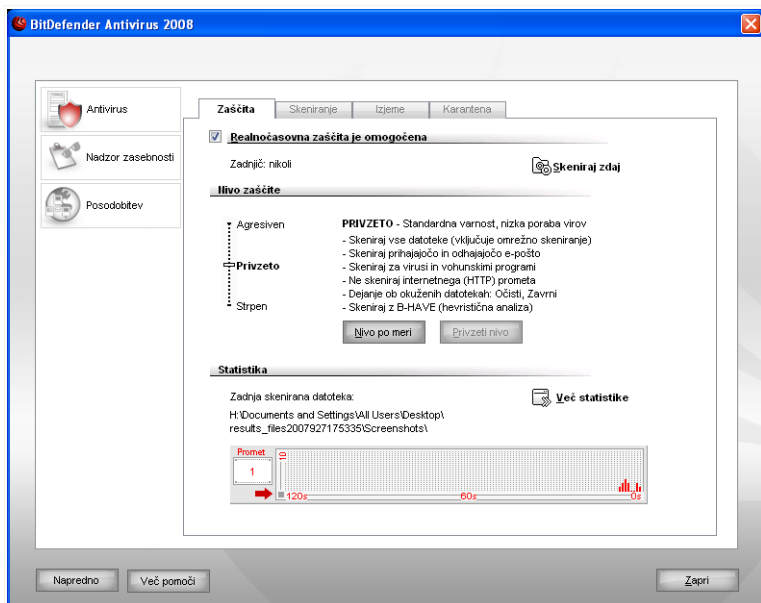
Poglavje **Protivirusna zaščita** vsebuje naslednje teme:

- Skeniranje ob dostopu
- Skeniranje na zahtevo
- Predmeti izvzeti iz skeniranja
- Karantena

### 8.1. Skeniranje ob dostopu

Skeniranje ob dostopu - za skeniranje odprtih datotek in komunikacij preko instantnih sporočil (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Izberite še vrsto skeniranih datotek.

Za uporabo privzetih nastavitvev realnočasovne zaščite kliknite na **Privzeta stopnja**. Odrplo se bo novo okno:



## Realnočasovna zaščita



### Pomembno

Za preprečitev okužbe z virusi pustite **Realnočasovno zaščito** vedno omogočeno.

V spodnjem delu odseka lahko vidite statistiko o **Realnočasovna zaščita** statistiko o skeniranih datotekah in e-pošti. Kliknite **Podrobnejša statistika**, če želite podrobnejši vpogled v statistiko realnočasovne zaščite.

Za začetek hitrega skeniranja sistema kliknite **Skeniraj zdaj**.

## 8.1.1. Nastavitev stopnje zaščite

Izbirate lahko med različnimi stopnjami zaščite, ki najboljše zadovoljujejo vaše potrebe po varnosti. Z drsnikom izberete zaželjeno stopnjo.

Na voljo so 3 stopnje zaščite:

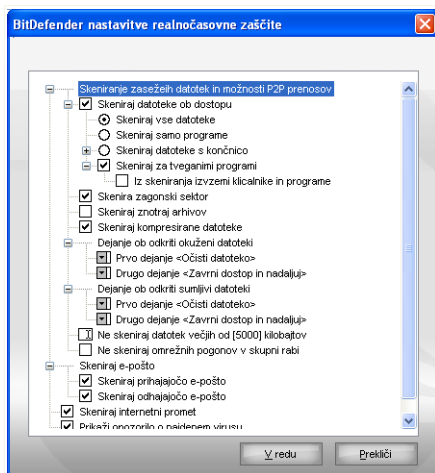
<b>Stopnja zaščite</b>	<b>Opis</b>
<b>Dovoli</b>	<p>Pokriva osnovne varnostne potrebe. Obremenitev sistema je zelo majhna.</p> <p>Programi in prihajajoča pošta so pregledani pred virusi. Poleg klasičnega skeniranja na podlagi podpisov virusov, se uporablja metodični analizator. Okužene datoteke se obravnava na način: očisti datoteko/zavrni dostop.</p>
<b>Privzeto</b>	<p>Standardna zaščita. Majhna obremenitev sistema.</p> <p>Vse datoteke in prihajajoča ter odhajajoča pošta so pregledane pred virusi in vohunskimi programi. Poleg klasičnega skeniranja na podlagi podpisov virusov, se uporablja metodični razčlenjevalec. Okužene datoteke se obravnava na način: očisti datoteko/zavrni dostop.</p>
<b>Agresivno</b>	<p>Višja zaščita. Srednja obremenitev sistema.</p> <p>Vse datoteke in prihajajoča ter odhajajoča pošta so pregledane pred virusi in vohunskimi programi. Poleg klasičnega skeniranja na podlagi podpisov virusov, se uporablja metodični razčlenjevalec. Okužene datoteke se obravnava na način: očisti datoteko/zavrni dostop.</p>

Za uporabo privzetih nastavitev realnočasovne zaščite kliknite na **Privzeta stopnja**.

## 8.1.2. Zaščita po meri

Napredni uporabniki si želijo prednosti nastavljanja nastavitev, ki jo ponuja BitDefender. Skeniranje je lahko nastavljeno tako, da preskoči datoteke z določenimi končnicami, določene mape in celo arhivske datoteke, za katere ste prepričani, da so popolnoma neškodljive. To pripomore k drastičnemu zmanjšanju časa za skeniranje.

Nastavite **Realnočasovna zaščita** s klikom na **Stopnja po meri**. Odprlo se bo sledeče okno:



### Nastavitve ščita

Možnosti skeniranja so organizirane kot razširljiv meni, podoben tistim v Windows okolju. Kliknite kvadrat s "+", da odprte možnosti in kvadrat s "-", da zaprete možnost.



#### Opomba

Opazite lahko, da nekaterih možnosti, klub temu da se pojavi znak "+", ne morete odpreti. Razlog tiči v dejstvu, da teh možnosti še niste izbrali. Ko jih boste omogočili, jih bo moč tudi odpreti.

- **Skeniranje odprtih datotek in možnosti P2P prenosov** - za skeniranje odprtih datotek in komunikacij preko instantnih sporočil (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Izberite še vrsto skeniranih datotek.

Možnost	Opis
<b>Skeniraj odprte datoteke</b>	Skenirane bodo vse odprte datoteke.
<b>Skeniraj vse datoteke</b>	Skenirane bodo vse datoteke.
<b>Skeniraj samo programe</b>	Skenirane bodo le programske datoteke. To so datoteke s končnico: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk;
<b>Skeniraj datoteke s končnico</b>	Skenirane bodo datoteke s končnicami, ki so določene v nastavitvah.
<b>Skeniraj za tveganimi programi</b>	Skenirane bodo datoteke, ki so določene v nastavitvah.
<b>Skeniraj zagonski sektor</b>	Skenirane bodo datoteke, ki so določene v nastavitvah.
<b>Skeniraj znotraj arhivov</b>	Skenirane bodo datoteke, ki so določene v nastavitvah.
<b>Skeniraj kompresirane datoteke</b>	Skenirane bodo datoteke, ki so določene v nastavitvah.
<b>Dejanje ob odkriti okuženi datoteki</b>	Dejanje ob odkriti okuženi datoteki.
<b>Dejanje ob odkriti sumljivi datoteki</b>	Dejanje ob odkriti sumljivi datoteki.
<b>Ne skeniraj datotek večjih od [5000] kilobajtov</b>	Ne skeniraj datotek večjih od [5000] kilobajtov.
<b>Ne skeniraj omejenih pogonov v skupini rabi</b>	Ne skeniraj omejenih pogonov v skupini rabi.
<b>Skeniraj e-pošto</b>	Skeniraj e-pošto.
<b>Skeniraj prihajajočo e-pošto</b>	Skeniraj prihajajočo e-pošto.
<b>Skeniraj odhajajočo e-pošto</b>	Skeniraj odhajajočo e-pošto.
<b>Skeniraj internetni promet</b>	Skeniraj internetni promet.
<b>Preklopi avtomatsko na nastavljen vir virusi</b>	Preklopi avtomatsko na nastavljen vir virusi.

Možnost	Opis
<p><b>Skeniraj datoteke z d e f i n i r a n o končnico</b></p> <p><b>Skeniraj za nevarnimi programi</b></p>	<p>.wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml in .nws.</p> <p>Skenirane bodo le datoteke s končnico, ki jo določi uporabnik. Končnice morajo biti ločene s podpičjem ";".</p> <p>Skenira datoteke. Skenira za nevarnimi programi. Te datoteke bodo obravnavane kot okužene. Programi, ki vsebujejo reklamno vsebino, bodo morebiti prenehali delovati, ko bo ta možnost omogočena.</p> <p>Izberite <b>Preskoči klicne dostope in aplikacije med skeniranjem</b>, če želite izvzeti takšne datoteke iz skeniranja.</p>
<b>Skeniraj zagonske sektorje</b>	Skenirani bodo zagonski sektorji.
<b>Skeniraj znotraj arhivov</b>	Skenirane bodo tudi odprte arhivirane datoteke. Z omogočenjem teh možnosti boste upočasnili delovanje računalnika.
<b>Skeniraj kompresirane datoteke</b>	Skenirane bodo vse stisnjene datoteke.
<p><b>Prvo dejanje</b></p> <p><b>Onemogoči dostop in nadaljaj</b></p> <p><b>Očisti datoteko</b></p> <p><b>Izbriši datoteko</b></p> <p><b>Premakni datoteko v karanteno</b></p>	<p>Izberete lahko eno izmed naslednjih dejanj:</p> <p>V primeru okužene datoteke, je dostop do te datoteke onemogočen.</p> <p>Očisti okužene datoteke.</p> <p>Brez opozorila izbriše okužene datoteke.</p> <p>Premakne okužene datoteke v karanteno.</p>
<p><b>D r u g o dejanje</b></p> <p><b>Onemogoči dostop in nadaljaj</b></p>	<p>Izberite drugo dejanje, ki se bo izvajalo v primeru, da prvo dejanje ne bo učinkovito.</p> <p>V primeru okužene datoteke, je dostop do te datoteke onemogočen.</p>

<b>Možnost</b>	<b>Opis</b>
<b>Izbriši datoteko</b>	Brez opozorila izbriše okužene datoteke.
<b>Premakni datoteko v karanteno</b>	Premakne okužene datoteke v karanteno.
<b>Ne skeniraj datotek večjih od[x] Kb</b>	Vtipkajte največjo dovoljeno velikost datotek za skeniranje. Če je vnesena vrednost enaka 0 Kb, bodo skenirane vse datoteke.
<b>Ne skeniraj datotek večjih od[x] Kb</b>	V kolikor je ta možnost omogočena BitDefender ne bo skeniral datoteke v skupni uporabi, kar omogoči hitrejšo dostopanje do interneta.  Priporočamo vam, da omogočite to možnost samo, če je omrežje, katerega del ste, ustrezno zaščiteno.

- **Skeniraj e-poštni promet** - skenira e-poštni promet.

Možnosti so naslednje:

<b>Možnost</b>	<b>Opis</b>
<b>Skeniraj prihajajočo pošto</b>	Skenira vso prihajajočo pošto.
<b>Skeniraj odhajajočo pošto</b>	Skenira vso odhajajočo pošto.

- **Skenira http promet** - skenira http promet.
- **Prikaži opozorilo o najdenem virusu** - ko program odkrije virus v datoteki ali elektronski pošti, se pojavi izskočno okno z opozorilom.

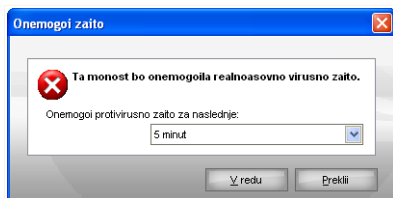
Opozorilo o okuženi datoteki vsebuje ime virusa, njegovo lokacijo, dejanje, ki ga je opravil BitDefender, ter povezavo na BitDefender stran z dodatnimi informacijami o virusu. Opozorilo o okuženi e-pošti pa bo vsebovalo še informacije o pošiljatelju in prejemniku sporočila.

Ob odkriti sumljivi datoteki je v opozorilnem oknu moč pognati tudi čarovnika, ki vam bo pomagal poslati datoteko v BitDefender Laboratorij na dodatno analizo. Če vpišete svoj elektronski naslov, boste prejeli tudi dodatne informacije o poročilu.

Kliknite **Potrdi** za shranitev sprememb.

### 8.1.3. Onemogočanje realnočasovne zaščite.

V kolikor boste onemogočili realnočasovno zaščito se bo pojavilo opozorilno okno.



onemogoči realnočasovno zaščito

Vašo izbitno morate potrditi preko manija, kako dolgo želite pustiti realnočasovno zaščito onemogočeno. Na voljo so možnosti 5,15, ali 30 minut, eno uro, stalno ali do naslednjega zagona sistema.



#### **Pozor**

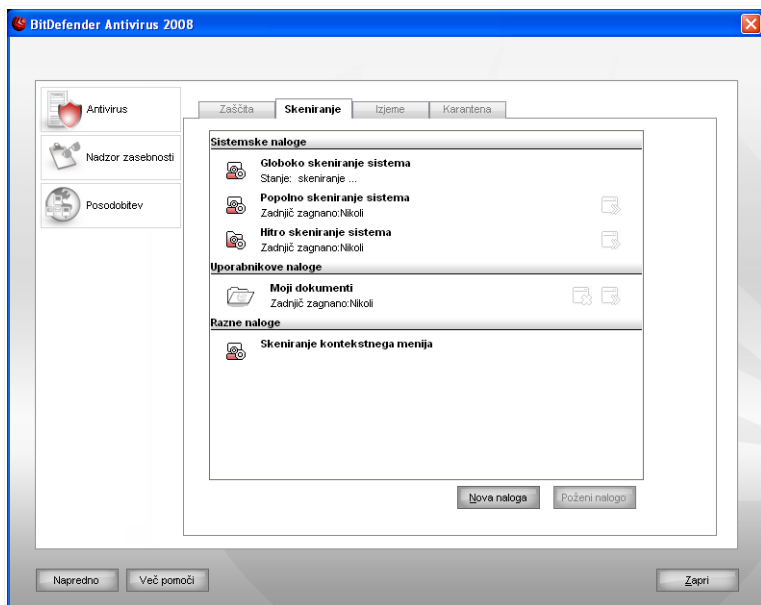
To je kritična varnostna težava. Priporočamo, da realnočasovno zaščito onemogočite kar se da redko in za čim manj časa. V kolikor realmpčasovna zaščita ni omogočena, je vaš računalnik izpostavljen zlonamernemu programju.

## 8.2. Skeniranje na zahtevo

Glavna BidDefender-jeva naloga je ohranjanje čistega in neokuženega računalniškega sistema. Glavni način za uspeh je preprečevanje vstopa novih virusov s skeniranjem elektronske pošte ter vseh datotek kopiranih ali prenesenih na vaš računalnik.

Obstaja tveganje, da je virus nastanjen v vašem sistemu, še preden namestite BitDefender. Zato vam svetujemo, da takoj po namestitvi izvršite skeniranje celotnega sistema. Priporočljivo je tudi občasno skeniranje celotnega sistema.

Za nastavitve in iniciacijo skeniranja na zahtevo kliknite **Antivirus>Skeniraj** v vmesniku z nastavitve. Odrplo se bo novo okno:



## Opravila skeniranja

Skeniranje na zahtevo bazira na opravljenih skeniranjih. Opravila skeniranja določijo možnosti skeniranja in predmete, ki bodo skenirani. Vaš računalnik lahko skenirate kadarkoli želite s pomočjo prednastavljenih opravil ali preko individualiziranih opravil skeniranja. Uredite jih lahko po urniku, da se izvaja redno ali pa, da se izvaja, ko vaš sistem miruje.

### 8.2.1. Opravila skeniranja

BitDefender vsebuje mnoga prednastavljena pravila, ki pokrivajo standardne varnostne težave. Sami pa lahko kreirate individualizirana pravila skeniranja.

Vsako pravilo vsebuje okence **Lastnosti**, ki vam omogoča nastavitve opravil in ogled rezultatov. Za več informacij se obrnite na "*Nastavitve naloge skeniranja*" (p. 53).

Obstajajo tri kategorije opravil skeniranja.

- **Sistemska opravila** - vsebuje seznam sistemskih opravil. Na voljo so naslednja opravila:

Prednastavljena opravila	Opis
<b>Globoko sistemsko skeniranje</b>	Skenira celoten sistem V prednastavljeni konfiguraciji skenira za vsemi oblikami zlonamernega programja, kot so virusi, wohunski programi, rootkiti, itd..
<b>Popolno skeniranje sistema</b>	Pregleda celoten sistem, razen arhivov. V prednastavljeni konfiguraciji skenira za vsemi oblikami zlonamernega programja, kot so virusi, wohunski programi, rootkiti, itd..
<b>Hitro skeniranje sistema</b>	Skenira mape Windows, Program Files in All Users V predstavljeni konfiguraciji skenira za vsemi oblikami zlonamernega programja, razen rootkitov, vendar ne skenira navideznega pomnilnika, registra in piškotkov.



### Opomba

Ker opravili **Globoko skeniranje sistema** in **Popolno skeniranje sistema** pregledata celoten sistem, lahko traja nekaj časa, zato vam predlagamo, da izvajate skeniranje kadar ne uporabljate računalnika.

- **Uporabnikova opravila** - vsebuje opravila, ki jih je definiral uporabnik.

Opravilo *My Documents* je zagotovljeno. To opravilo vam skenira pomembne mape: *My Documents*, *Desktop* and *StartUp*. Na ta način si zagotovite varnost vaših dokumentov in varno delovno mesto.

- **Ostala opravila** - vsebuje seznam ostalih opravil skeniranja. Ta opravila skeniranja se nanašajo na aternatine tipe skeniranja ki jih lahko poženete s tega okna. Spreminjate lahko samo njihove lastnosti ali pogled na poročilo skeniranja.

Na voljo so trije gumbi:

- **Načrtovana opravila** - pove, da je to opravilo načrtovano za kasneje. Kliknite ta gumb, da pridete v **Načrtovalec** iz **Lastnosti** kjer lahko spreminjate nastavitve.
- **Izbriši** - odstrani izbrano nalogo.



### Opomba

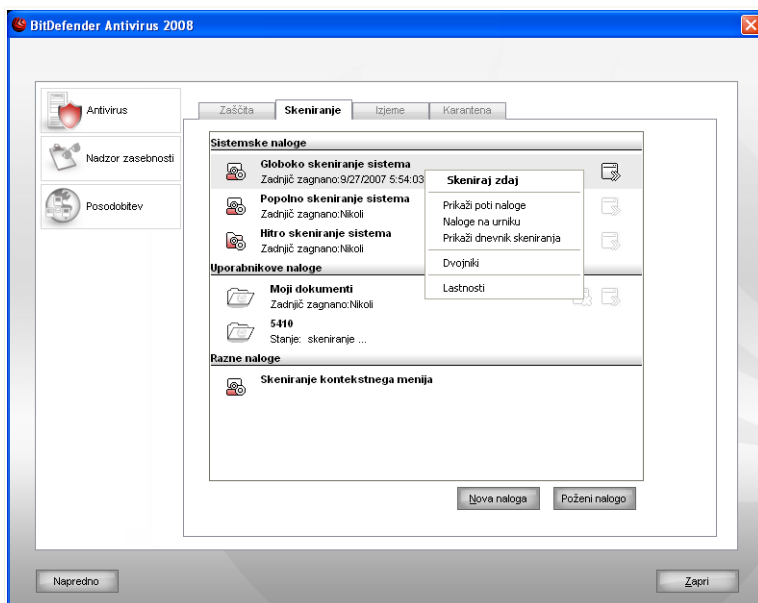
Ni na voljo za sistemska opravila. Ne morete odstraniti sistema opravila.

- **Skeniraj** - prične izvajati opravila in požene **takojsnje skeniranje**.

Na levi lahko vidite gumb **Properties**, ki vam omogoča spreminjanje opravil in pregled prijav skeniranja.

## 8.2.2. Uporaba hitrega seznama

Hitri seznam je na voljo za vsa opravila. Kliknite desni gumb miške in odprite opravilo. Možnosti so



### Hitri seznam

naslednje:

- **Skeniraj sedaj** - takoj izvede izbrano nalogo in prične s takojšnjim skeniranjem.
- **Spremeni mesta skeniranja** - odpre okno **Lastnosti Skeniraj poti**, kjer lahko spreminjate mesta skeniranja za izbrana opravila.



#### Opomba

V primeru sistemskih opravil, je ta možnost nadomeščena z **Prikaži poti opravil**, kjer lahko vidite samo predmet skeniranja.

- **Načrtuj opravila** - odpre okno **Lastnosti Načrtovalec**, kjer lahko načrtujete izbrana opravila.

- **Poglej prijave skeniranja** - odpre okno **Lastnosti Prijave skeniranja** kjer lahko vidite poročila narejena po izvršitvi izbranega opravila.
- **Podvoji** - podvoji izbrano nalogo.



**Opomba**

To je uporabno, ko ustvarjamo nova opravila. lahko pa spremenite nastavitve dvojnika opravil.

- **Izbriši** - izbriše izbrano nalogo.



**Opomba**

Ni na voljo za systemska opravila. Ne morete odstraniti systemskega opravila.

- **Lastnosti** - odpre okno **Lastnosti, Pregled** kjer lahko spreminjate nastavitve uzbranih opravil.



**Opomba**

Zaradi narave možnosti so **Lastnosti** in **Poglej prijave skeniranja** le te na voljo za opravila v kategoriji **Ostala opravila**.

### 8.2.3. Ustvarjanje opravil skeniranja

Za ustvarjanje opravila skeniranja uporabite eno izmed naslednjih metod

- **Podvoji** obstoječe pravilo, ga preimenujte in naredite potrebne spremembe v oknu **Lastnosti** window;
- Kliknite **Novo opravilo** da nastavite novo opravilo Nastavi.

### 8.2.4. Nastavitve naloge skeniranja

Vsako opravilo skeniranja ima svoje okno **Lastnosti**, kjer lahko spreminjate nastavitve skeniranja, določite tarče skeniranja, določite poteke opravil ali pogledate sporočila. Kliknite ali desnokliknite opravilo in nato kliknite **Odpri**.

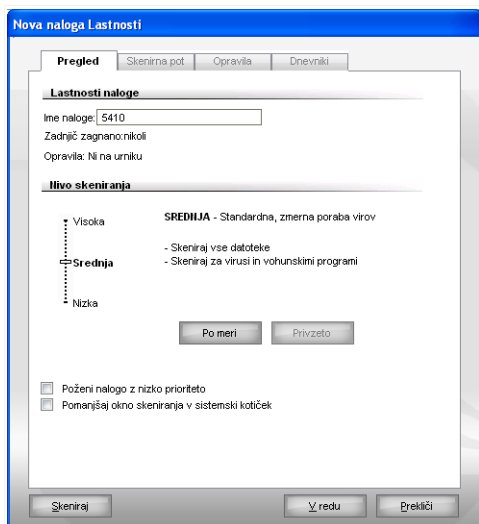


**Opomba**

Za več informacij o **Vnosi** si oglejte del o "**Ogled prijav skeniranja**" (p. 70).

### Spreminjanje nastavitvev skeniranja

Desnokliknite določeno opravilo in izberite **Lastnosti**. Odprlo se bo novo okno:



### Pregled

Tukaj lahko vidite podrobnosti o opravih (ime, zadnjič pognano in status naročenih opravil) in prilagodite nastavitve skeniranja.

### Izbira stopnje skeniranja

Povlecite drsnik po skali in izberite ustrezno stopnjo skeniranja.

Obstajajo 3 stopnje skeniranja:

Stopnja zaščite	Opis
<b>Nizka</b>	Zmerna učinkovitost detekcije. Majhna obremenitev sistema. Programi so pregledani pred virusi. Poleg skeniranja na osnovi podpisov virusov, uporablja program tudi metodični analizator.
<b>Srednja</b>	Dobra učinkovitost detekcije. Zmerna obremenitev sistema. Vse datoteke so pregledani pred virusi in vohunskimi programi. Poleg skeniranja na osnovi podpisov virusov, uporablja program tudi metodični analizator.
<b>Visoka</b>	Visoka učinkovitost detekcije. Velika obremenitev sistema.

Stopnja zaščite	Opis
	Vse datoteke in arhivi so pregledani pred virusi in vohunskimi programi. Polek skeniranja na osnovi podpisov virusov, uporablja program tudi metodični analizator.

Na voljo je tudi več splošnih možnosti skeniranja:

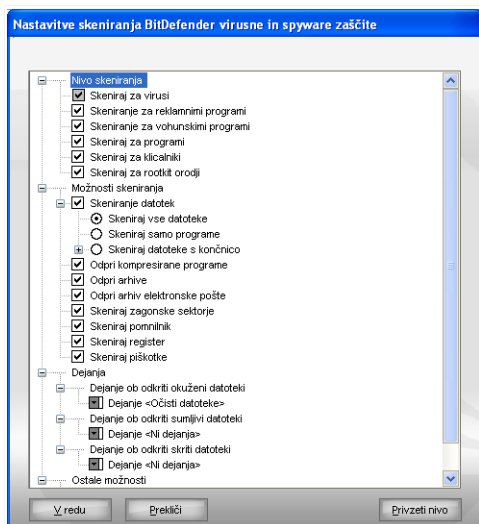
Možnost	Opis
<b>Poženi skeniranje z nizko prioriteto</b>	Zmanjša prioriteto procesu skeniranja. To bo omogočilo hitrejšo delo drugih programov in podaljšalo čas skeniranja.
<b>Minimiraj okno skeniranja v sistemski kotichek</b>	Minimira okno skeniranja v <b>sistemski kotichek</b> . Dvokliknite ikono BitDefender za ponovni prikaz.

Kliknite **V redu** za shranitev sprememb. Če kliknete na gumb **Skeniraj** poženete opravilo.

### Prilagajanje stopnje skeniranja

Napredni uporabniki si želijo prednosti nastavljanja nastavitev, ki jo ponuja BitDefender. Skeniranje je lahko nastavljeno tako, da preskoči datoteke z določenimi končnicami, določene mape in celo arhivske datoteke, za katere ste prepričani, da so popolnoma neškodljive. To pripomore k drastičnemu zmanjšanju časa za skeniranje.

Kliknite **Po meri** za nastavitve skeniranja. Odprlo se bo novo okno.



## Nastavitve skeniranja

Možnosti skeniranja so organizirane kot razširljiv meni, podoben tistim v Windows okolju. Kliknite kvadrat s "+" za odprtje možnosti in kvadrat z "-", da zaprete možnost.

Skenirne možnosti so razdeljene v štiri kategorije:

- **Stopnja skeniranja**
  - **Možnosti skeniranja za virusi**
  - **Možnosti dejanja**
  - **Ostale možnosti**
- Določite vrsto zlonamernega programja, ki ga želite skenirati z izbiro ustrezne **Stopnja skeniranja**.

Možnosti so naslednje:

<i>Možnost</i>	<i>Opis</i>
<b>Skeniraj pred virusi</b>	Skeniraj za poznanimi grožnjami

Možnost	Opis
	BitDefender zaznava tudi nepopolne virusne oblike ter tako odstrani vse potencialne grožnje, ki vplivajo na varnost vašega sistema.
<b>Skeniraj za oglaševalnimi programi</b>	Skenira za nevarnimi programi. Te datoteke bodo obravnavane kot okužene. Programi, ki vsebujejo reklamno vsebino, bodo morebiti prenehali delovati, ko bo ta možnost omogočena.
<b>Skeniraj za vohunskimi programi</b>	Skenira za znanimi vohunskimi programi. Te datoteke bodo obravnavane kot okužene.
<b>Skeniraj za programi</b>	Skenira datoteke programov (.exe in .dll).
<b>Skeniraj za klicalniki</b>	Skenira za klicalniki. Te datoteke bodo obravnavane kot okužene. Programi, ki vsebujejo klicalnike, bodo morebiti prenehali delovati, ko bo ta možnost omogočena.
<b>Skeniraj pred rootkiti</b>	Skenira datoteke in procese pred skritimi objekti-rootkiti.

- Določite vrste objektov, ki jih želite skenirati (arhivi, elektronska pošta itd.) in druge možnosti. Vse to poteka z izbiranjem določenih možnosti iz kategorije **Možnosti skeniranja za virusi**.

Možnosti so naslednje:

Možnost	Opis
<b>Skeniraj datoteke</b>	<b>vse</b> Skenirane bodo vse odprte datoteke.
<b>Skeniraj datoteke</b>	<b>Skeniraj le izvršilne datoteke</b> Skenirane bodo le programske datoteke. To so datoteke s končnico: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml in nws.

<b>Možnost</b>	<b>Opis</b>
<b>Skeniraj datoteke z definirano končnico</b>	Skenirane bodo le datoteke s končnico, ki jo določi uporabnik. Končnice morajo biti ločene s podpičjem ";".
<b>Odpri kompresirane programe</b>	Skenirane bodo stisnjene datoteke.
<b>Odpri arhive</b>	Skenirane bodo arhivske datoteke.
<b>Odpri arhive elektronske pošte</b>	Skeniran bo e-poštni arhiv.
<b>Skeniraj zagonske sektorje</b>	Skenirani bodo zagonski sektorji.
<b>Skeniraj pomnilnik</b>	Skenira pomnilnik pred virusi in ostalimi zlonamernimi programi.
<b>Skeniraj register</b>	Skenira vnose v register.
<b>Skeniraj piškotke</b>	Skenira datoteke piškotkov.

- Določite dejanje ob odkriti okuženi ali sumljivi datoteki. Odprite možnosti pod **Možnosti dejanja** za pregled vseh možnosti.
  - Izberete lahko eno izmed naslednjih dejanj: Možnosti so naslednje:

<b>Dejanje</b>	<b>Opis</b>
<b>Nič (vpis v poročilo)</b>	Nobeno dejanje ne bo uporabljeno pri okuženih datotekah. Datoteke bodo prikazane v poročilu.
<b>Očisti datoteke</b>	Očisti okužene datoteke.
<b>Izbriše datoteke</b>	Brez opozorila izbriše okužene datoteke.
<b>Premakni datoteke v karanteno</b>	Premakne okužene datoteke v karanteno.

- Izberete lahko eno izmed naslednjih dejanj: Možnosti so naslednje:

<b>Dejanje</b>	<b>Opis</b>
<b>Nič (vpis v poročilo)</b>	Nobeno dejanje ne bo uporabljeno pri okuženih datotekah. Datoteke bodo prikazane v poročilu.
<b>Izbriše datoteke</b>	Brez opozorila izbriše okužene datoteke.
<b>Premakni datoteke v karanteno</b>	Premakne okužene datoteke v karanteno.

**Opomba**

Če skeniranje odkrije sumljive datoteke, vas bo pozvalo k pošiljanju le-teh v BitDefender Laboratorij.

- Izberite dejanje, ki so bo izvedlo, ko bodo odkriti skriti predmeti (rootkiti). Možnosti so naslednje:

<b>Dejanje</b>	<b>Opis</b>
<b>Nič (vpis v poročilo)</b>	Nobeno dejanje ne bo uporabljeno pri okuženih datotekah. Datoteke bodo prikazane v poročilu.
<b>Premakni datoteke v karanteno</b>	Premakne skrite datoteke v karanteno.
<b>Omogoči ogled</b>	Omogoči ogled skritih datotek.

**Opomba**

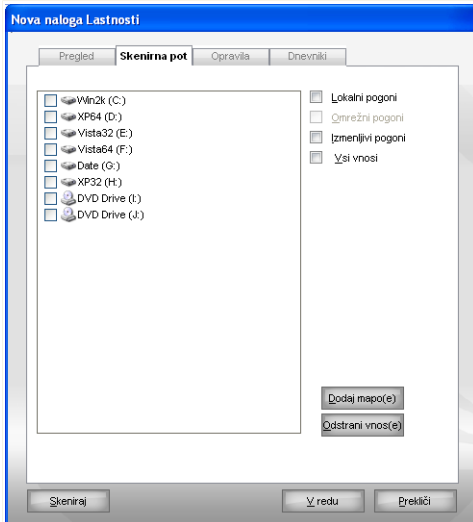
V kolikor se odločite prezreti zaznane datoteke ali, če bodo izbrana dejanja neuspešna, boste morali izbrati dejanje iz čarovnika za skeniranje.

- Obkljukajte **Pošlji sumljive datoteke v BitDefender Lab** v delu **Ostale možnosti**

Če kliknete **Privzeto**, boste naložili privzete nastavitve. Kliknite **Potrdi** za shranitev sprememb.

## Nastavite mesto skeniranja

Za nastavitve mest skeniranja za specifična opravila desnokliknite opravilo in izberite **Spremeni mesto skeniranja**. Odprlo se bo novo okno:



### Mesto skeniranja

Vidite lahko seznam lokalnih, mrežnih in izmenljivih pogonov ter datoteke in mape, ki so bile dodane. Vsi označeni predmeti bodo skenirani, ko se bo izvajalo opravilo.

Ta del vsebuje naslednje gumbе:

- **Dodaj datoteko(e)** - odpre brskalno okno, kjer lahko izberete datoteke, ki jih želite skenirati.



#### Opomba

Uporabite metodo povleci in izpusti za lažje dodajanje datotek/map.

- **Odstrani predmet(e)** - izbriše datoteke/mape, ki so bile prej dodane na seznam objektov za skeniranje.



#### Opomba

Zbrišete lahko le datoteke/mape, ki so bile dodane naknadno in ne tudi tistih, ki jih je BitDefendar zaznal samodejno.

Poleg zgoraj razloženih gumbov obstaja še nekaj možnosti kako hitro izbrati lokacije za skeniranje.

- **Lokalni pogoni** - skeniranje lokalnih pogonov.
- **Omrežni pogoni** - skeniranje omrežnih pogonov.
- **Izmenljivi pogoni** - skeniranje vseh prenosljivih pogonov (CD-ROM, gibki disk).
- **Vsi vnosi** - skeniranje vseh pogonov.



**Opomba**

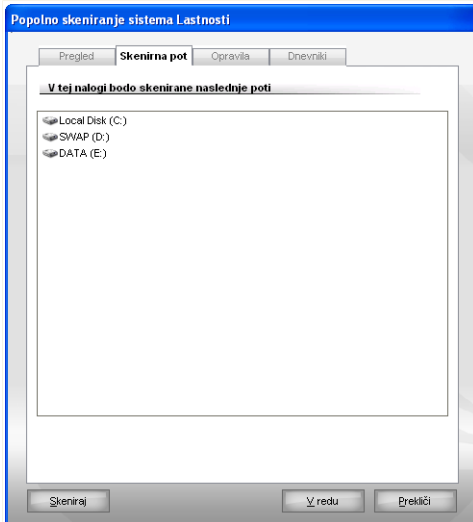
Če želite skenirati celoten sistem, preprosto izberite **Vsi vpisi**.

Kliknite **V redu** za shranitev sprememb. Če kliknete na gumb **Skeniraj** poženete opravilo.

**Ogled mest skeniranja v sistemskih nalogah.**

Spreminjate lahko mesta skeniranja sistemskih opravil v kategoriji **Sistemska opravila**. Vidite lahko samo njihova mesta skeniranja.

Za ogled mesta skeniranja posameznega opravila ali za spreminjanje le tega desno-kliknite opravilo in izberite **Pokaži poti opravil**. Kliknite **Popolno skeniranje**. Pojavi se naslednje okno:



### Mesto skeniranja za Popolno skeniranje sistema

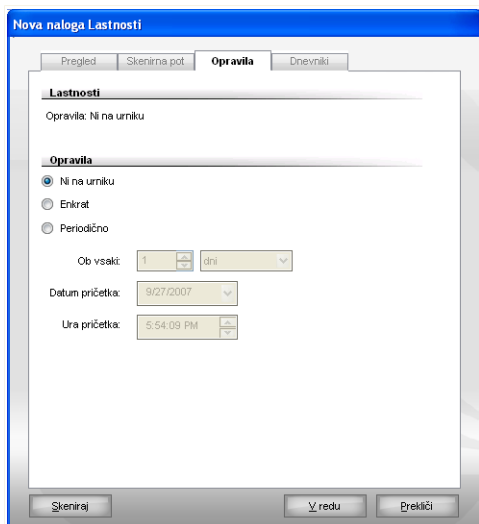
Mape **Polno s in Globoko skeniranje sistema** skenira vse lokalne pogone, medtem ko **Hitro skeniranje sistema** pregleda samo **Windows in Program Files**

Kliknite **V redu** da zaprete okno. izberite nalogo in kliknite **Skeniraj**.

### **Urnik opravil skeniranja**

Ker skeniranje vzame kar nekaj časa in je najbolj učinkovito, ko so zaprti vsi ostali programi, ja najpametneje nastaviti načrtovano skeniranje na tisti čas, ko vas ni za računalnikom, a je ta vseeno prižgan.

Za ogled urnika posameznega opravila ali za spreminjanje le tega desno-kliknite opravilo in izberite **Urnik opravil**. Odprlo se bo novo okno:



### Urnik

Tu lahko vidite urnik opravil.

Ko načrtujete opravilo morate izbrati med naslednjimi možnostmi:

- **Ni načrtovano** - požene skeniranje le na zahtevo.
- **Enkrat** - požene skeniranje le enkrat. Določite začetni datum in čas v **Začetni datum/čas**.
- **Periodično** - požene skeniranje v določenih intervalih (urah, dneh, tednih, mesecih, letih), začenši z določenim datumom.

Če želite, da se skeniranje ponavlja v določenih časovnih intervalih, obkljukajte izbiro **Periodično** ter vnesite v okno **Ob vsaki** število minut/ur/dni/tednov/mesecev/let, na katere naj se ta process ponavlja. Določiti morate tudi **Začetni Datum/Čas**

Kliknite **V redu** za shranitev sprememb. Če kliknete na gumb **Skeniraj** poženete opravilo.

## 8.2.5. Predmeti skeniranja

Preden pričnete skenirni postopek se prepričajte, da je BitDefender posodobljen. Skeniranje računalnika z zastarelimi bazami pvirusnih podpisov lahko preprečijo BitDefenderju detekcijo novih virusov, ki v starejših posodobitvah še eniso bili znani. Za najnovejš eposodobitve kliknite **Posodobi>Posodobi** v vmesniku za nastavitve.



### Opomba

Če želite izvesti popolno skeniranje morate zapreti vse odpre programe, še posebej to velja za e-poštni odjemalec (Outlook, Outlook Express ali Eudora).

## Načini skeniranja

BitDefender ponuja 4 načine skeniranja na uporabnikovo pobudo/zahtevo:

- **Takojšnje skeniranje** - požene opravila skeniranja in opravi sistemskih in uporabniških opravil.
- **Vsebinsko skeniranje** - desni klik na datoteko ali mapo in izberite BitDefender Antivirus 2008;
- **Povleci in izpusti skeniranje** - z načinom povleci in izpusti dodate datoteke ali mape v **Vrstica aktivnosti skeniranja**;
- **Ročno skeniranje** - pri BitDefender ročnem skeniranju neposredno izberete datoteke in mape, ki jih želite pregledati.

### Takojšnje skeniranje

Za skeniranje vašega računalnika ali dela le tega, lahko uporabite predstavljenih opravil skeniranja ali pa ustvarite svoja opravila. Obstajata dva načina kako ustvariti opravilo skeniranja: Takojšnje skeniranje

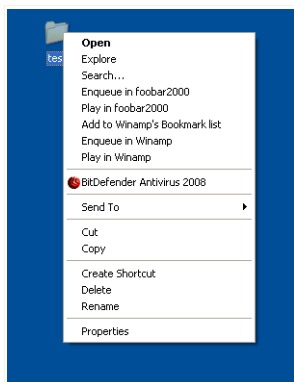
Izberete lahko eno izmed sledečih možnosti:

- iz seznama dvokliknite željeno opravilo skeniranja.
- Kliknite gumb **Skeniraj zdaj** za zagon opravila.
- izberite nalogo in kliknite **Poženi opravilo**.

Pojavi BitDefenderjev skener in prične se postopek skeniranja. Za več informacij si oglejte "**Skener BitDefender**" (p. 66).

### Vsebinsko skeniranje

Za skeniranje datotek in map, ne da bi ustvarili novo opravilo skeniranja, lahko uporabite vsebinski seznam. Vsebinsko skeniranje



Vsebinsko skeniranje

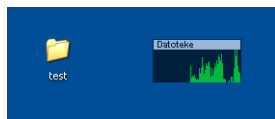
Na datoteko, ki jo želite skenirati, kliknite z desnim miškinim gumbom in izberite **BitDefender Antivirus 2008**.

Pojavi BitDefenderjev skener in prične se postopek skeniranja. Za več informacij si oglejte "*Skener BitDefender*" (p. 66).

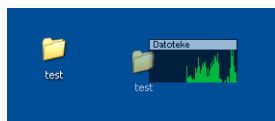
Spreminjate lahko možnosti skeniranja in pregleda poročil datotek z dostopom do okna Lastnosti v **Seznam vsebinskega skeniranja** task.

### Povleci in izpusti skeniranje

Primite datoteko, ki jo želite skenirati, in jo spustite na **Vrstica aktivnosti skeniranja**, kot je prikazano na spodnjih slikah.



Povleci datoteko



Spusti datoteko

Pojavi BitDefenderjev skener in prične se postopek skeniranja. Za več informacij si oglejte "*Skener BitDefender*" (p. 66).

## Ročno skeniranje

Pri ročnem skeniranju neposredno izberemo predmet skeniranja z možnostjo BitDefender ročno skeniranje iz mape BitDefender v seznamu Start.

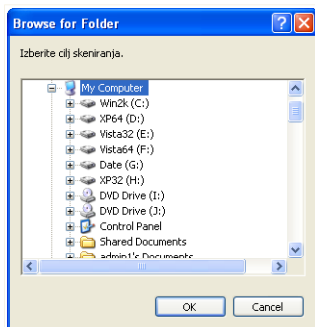


### Opomba

Ročno skeniranje je zelo uporabno, saj ga lahko uporabljate tudi kadar uporabljate varni način v WIN.

Za izbiro predmeta, ki ga želite skenirati z BitDefenderjem sledite poti **Start** → **Programi** → **BitDefender 2008** → **BitDefender Manual Scan**.

Odrplo se bo novo okno:



Ročno skeniranje

Izberite predmet skeniranja in kliknite **V redu**.

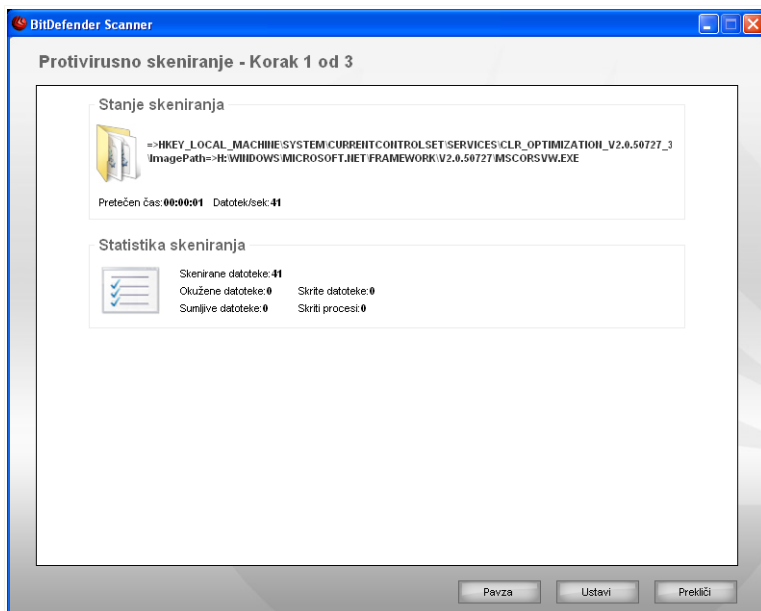
Pojavi BitDefenderjev skener in prične se postopek skeniranja. Za več informacij si oglejte "*Skener BitDefender*" (p. 66).

## Skener BitDefender

Kadar poženete skeniranje na zahtevo, se pojavi skener Bitdefender. Sledite trem korakom vodenega postopka za zaključitev postopka skeniranja.

### Korak 1/3 – Skeniranje

BitDefender bo začel skenirati izbrane objekte.



## Skeniranje

Vidite lahko stanje skeniranja in statistiko (hitrost skeniranja, preostali čas, število skeniranih / okuženih/ sumljivih/ skritih predmetov in ostalo).



### Opomba

Proces bo lahko trajal kar nekaj minut, odvisno od obsega skeniranja.

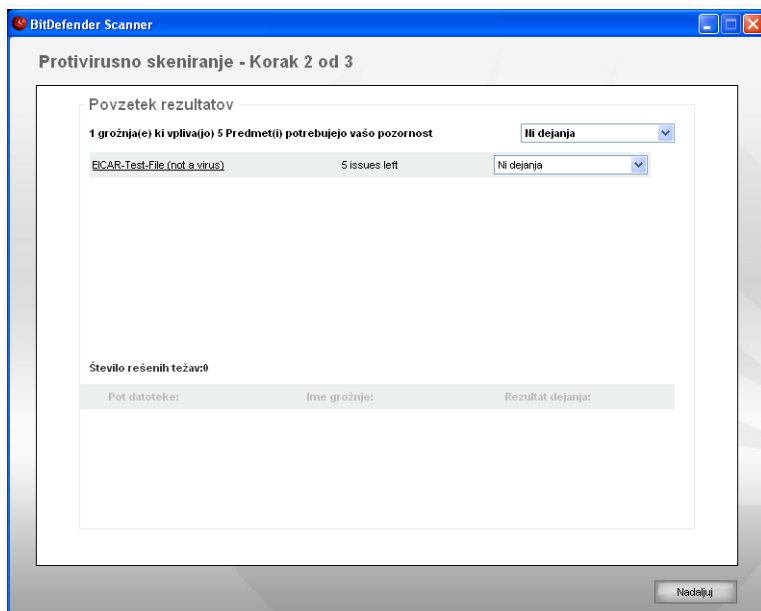
Za začasno prekinitvev postopka skeniranja kliknite **Pavza**. Za nadaljevanje skeniranja morate klikniti **Nadaljuj**

Skeniranje lahko ustavite kadarkoli s klikom na **Ustavi&Da**. Nadaljujete na zadnjem koraku čarovnika.

Počakajte, da BitDefender zaključi skeniranje.

## Korak 2/3 – Izberite dejanje

PO zaključku skeniranja se pojavi novo okno kjer lahko pregledate rezultate skeniranja.



## Dejanje

Razvidno je število težav, ki vplivajo na vaš sistem.

Okuženi predmeti so prikazani v skupini, glede na zlonamerni program, ki jih je okužil. Kliknite pripadajočo povezavo za več informacij o okuženih predmetih.

Izbirate lahko med dejanji, ki vplivajo na vse skupine težav ali pa izberete posamezno dejanje za vsako težavo.

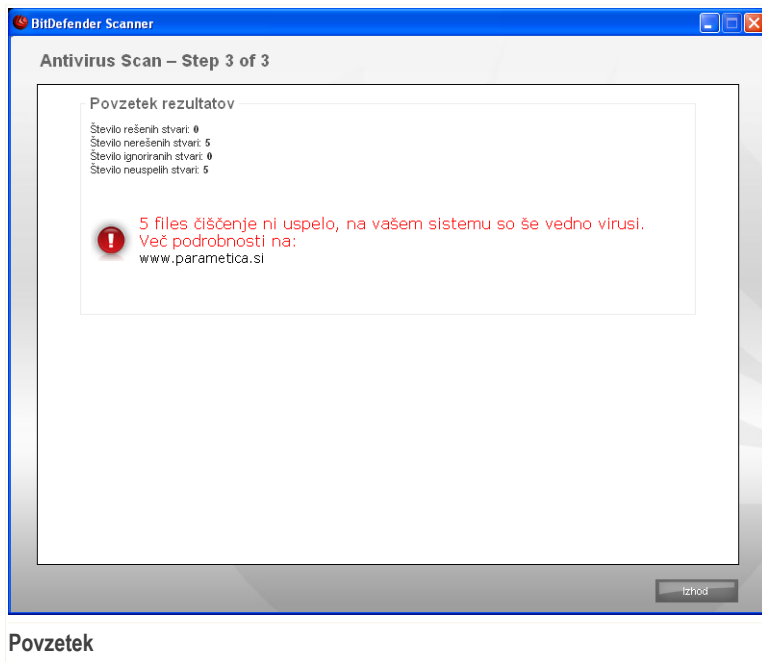
Možnosti so naslednje:

Dejanje	Opis
<b>Ne ukrepaj</b>	Nobeno dejanje ne bo uporabljeno pri okuženih datotekah.
<b>Očisti</b>	Očisti okužene datoteke.
<b>Izbriši</b>	Izbriše zoznane datoteke
<b>Razkrij</b>	Skriti predmeti postanejo vidni.

Kliknite **Nadaljuj** za izvedbo določenega dejanja.

### Korak 3/3 – Ogled rezultatov

Ko BitDefender popravi težave se pojavi novo okno z rezultati skeniranja.



Tu lahko vidite povzetek rezultatov. Dokument s poročilom o skeniranju je samodejno shranjen v odseku **Poročilo skeniranja** v delu **Lastnosti**.



#### **Pomembno**

Če je potrebno, ponovno zaženite računalnik za dokončanje procesa čiščenja.

Kliknite **Izhod** za zaprtje okna z rezultati.

#### **BitDefender ni uspel odpraviti nekaterih težav**

V večini primerov BitDefender uspešno očisti odkrite okužene datoteke ali izolira okužbo. Vendar vseeno obstajajo težave, ki jih ni moč odpraviti.

V teh primerih vam priporočamo, da se obrnete na BitDefenderjevo podporo na [www.bitdefender.com](http://www.bitdefender.com). Naši strokovnjaki tehnične podpore vam bodo pomagali odpraviti težave, s katerimi se soočate.

#### **BitDefender je izbrisal datoteke, zaščitene z geslom.**

Kategorija z geslom zaščitениh datotek vsebuje dve vrsti vnosov: arhivske in namestitvene datoteke. Te datoteke ne predstavljajo večje nevarnosti za sistem, razen v primeru, ko vsebujejo okužene datoteke in so pognane.

Prepričajte se, da so naslednje datoteke čiste:

- Če je datoteka, zaščitena z geslom, arhivska datoteka, ki ste jo zaščitili z geslom, odpakirajte vsebovane datoteke in jih skenirajte ločeno. Najenostavnejši način za skeniranje datotek je klik z desnim miškinim gumbom in izbira **BitDefender Antivirus 2008** iz menija.
- Če je z geslo zaščitena datoteka namestitveni program, se prepričajte, da je **realnočasovna zaščita** omogočena preden zaženete namestitveno datoteko. Če je namestitvena datoteka okužena, bo BitDefender izoliral okužbo.

Če ne želite, da BitDefender ponovno odkriva te datoteke, jih dodajte kot izjeme v proces skeniranja. Za dodajanje izjem skeniranja kliknite **Nastavitve** za odprtje konzole z nastavitvami in nato izberite **Antivirus > Izjeme**. Za dodatne informacije se obrnite na **Datoteke, izvzete iz skeniranja**.

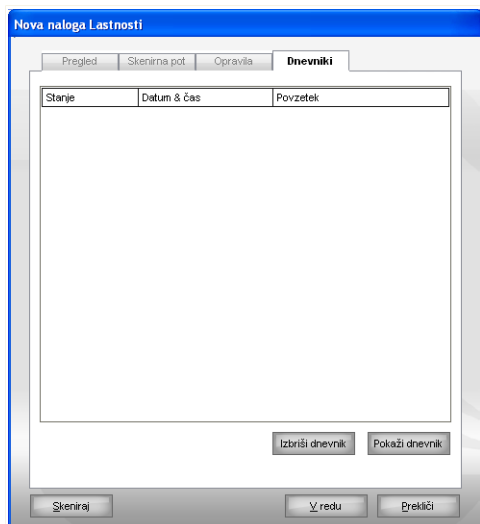
#### **BitDefender je izbrisal sumljive datoteke**

Sumljive datoteke so zaznane s hevrističnim filtrom in lahko vsebujejo zlonamerno programje, za katerega protivirusni podpisi še niso na voljo.

Če skeniranje odkrije sumljive datoteke, vas bo pozvalo k pošiljanju le-teh v BitDefender Laboratorij. Kliknite **V redu** za pošiljanje teh datotek v nadaljnjo analizo v BitDefender Laboratorij.

## **8.2.6. Ogled prijav skeniranja**

Za ogled rezultatov skeniranja, ko se izvede opravilo, desno-kliknite opravilo in izberite **Poglej prijave skeniranja**. Odprlo se bo novo okno:



### Prijave skeniranja

Tukaj lahko vidite poročilo o izvedenih nalogah.

Za vsako datoteko si lahko ogledate stanje skenirnega postopka, datum in čas skeniranja in povzetek rezultatov skeniranja.

Na voljo sta dva gumba:

- **Izbriši prijavo** - izbriše izbrano poročilo.
- **Prikaži prijavo** - odpre izbrano poročilo. Poročilo skeniranja se bo odprlo v spletnem brskalniku.



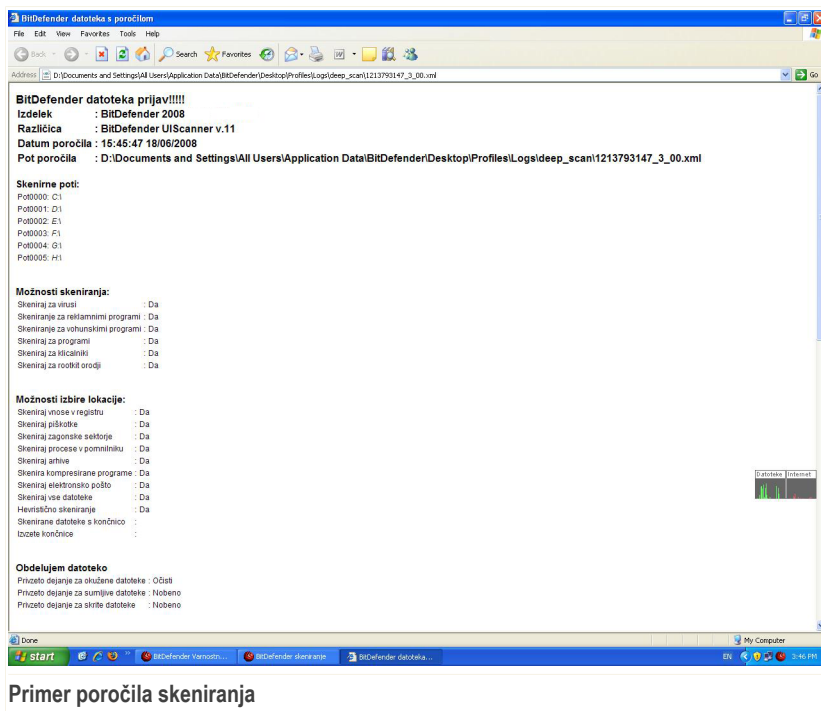
#### **Opomba**

Da pogledate ali izbrišete datotek, kliknite desni gumb miške in izberite med možnostmi iz hitrega seznama.

Kliknite **V redu** za shranitev sprememb. Če kliknete na gumb **Skeniraj** poženete opravilo.

### **Primer poročila skeniranja**

Naslednji primer ponazarja primer poročila skeniranja:



Poročila skeniranja vsebujejo podrobne informacije, kot so možnosti skeniranja, mesta skeniranja, najdene grožnje in dejanja, ki so se izvedla.

## 8.3. Predmeti izvzeti iz skeniranja

Včasih je potrebno določene datoteke izvzeti iz skeniranja. Naprimer, lahko bi želeli izvzeti EICAR preizkusno datoteko iz skeniranja ob dostopu ali datoteke .avi iz skeniranja na zahtevo.

Bitdefender dovoli, da izvzamete predmete iz skeniranja na zahtevo in skeniranja ob dostopu. Ta možnost je namenjena krajšanju časa skeniranja in nižja motnje vašega dela.

Izvamemo lahko dve vrsti predmetov.

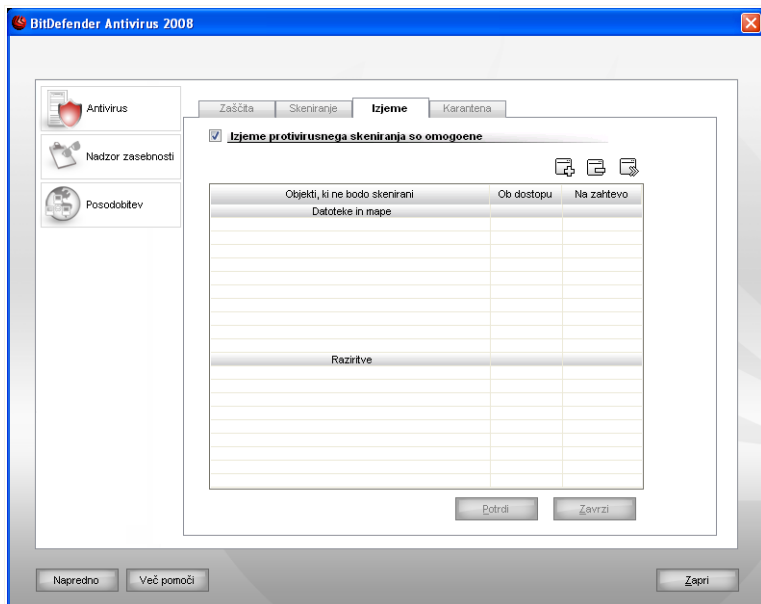
- **Poti**- datoteke in mape določene s specifično potjo bodo uzvzete iz skeniranja.
- **Uporabniško določene končnice** - vse datoteke z določenimi končnicami bod izvzete iz skeniranja.



### Opomba

Predmeti, ki so izvzeti iz skeniranja ob dostopu ne bodo skenirana ne glede na to ali do njih dostopate vi ali aplikacije.

Za ogled in upravljanje z izvzetimi predmeti kliknite **Antivirus>Izjeme** v vmesniku za nastavitve. Odprlo se bo novo okno:



### Izjeme


Izvzete predmete (datoteke, mape, končnice) lahko vidite. Za posamezen predmet lahko vidite ali je izvzet iz skeniranja ob dostopu, skeniranja na zahtevo, ali oboje.



### Opomba

Izjeme določene tukaj ne bodo veljale za vsebinsko skeniranje.

Za brisanje zapisa iz seznama, le-tega izberite in kliknite gumb  **Odstrani**.

Za urejanje vnosa v tabeli izberite vnos in kliknite gumb  **Uredi** Pojavilo se bo novo okno kjer lahko spremenite končnice ali poti, ki jih želite izvzeti in načine skeniranja iz katerih jih želite izvzeti. Spremenite potrebno in kliknite **V redu**.




#### Opomba

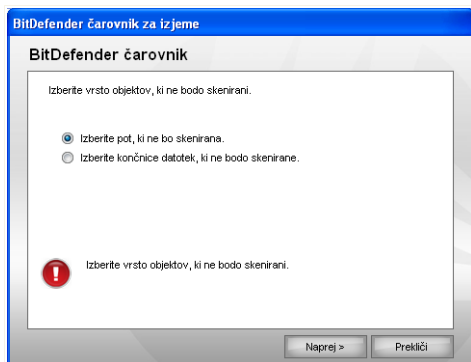
Prav tako lahko desno-kliknete predmet in uporabite možnosti na seznamu bližnjic za urejanje ali izbris.

Kliknite **Zavrzi** za preklic sprememb narejenih v seznam pravil, če jih niste shranili s klikom na **Uporabi**.

### 8.3.1. Izvzemanje poti iz skeniranja

Za izvzetje poti iz skeniranja kliknite gumb  **Dodaj** Čarovnik za nastavitve vas bo vodil skozi postopek izvzemanja poti.

#### Korak 1/3 – Izberite vrsto predmeta

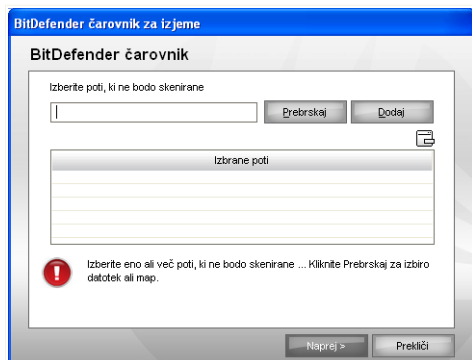


#### Vrsta predmeta

Izberite možnost izvzetja poti iz skeniranja.

Kliknite **Naprej**.

## Korak 2/3 – Določite izvzete poti



### Izvzete poti

Za določanje poti, ki jih želite izvzeti so na voljo naslednji načini:

- Kliknite **Prebrskaj**, izberite datoteko ali mapo, ki jo želite izvzeti in nato kliknite **Dodaj**.
- Vpišite pot, ki jo želite izvzeti in skeniranja, v polje za urejanje in kliknite **Dodaj**.



#### Opomba

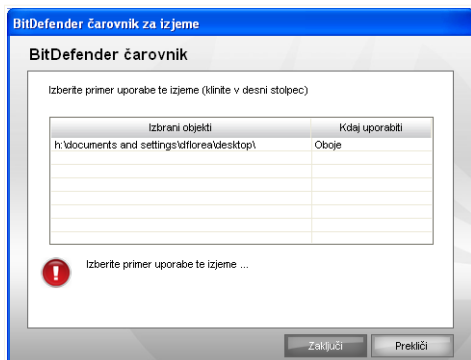
V kolikor vpisana pot ne obstaja se pojavi opozorilno okno. Kliknite **V r**edu in preglejte pravilnost vnosa.

Pot se bo pojavila v tabeli, ko jo dodate. Dodate lahko neomejeno število poti.

Za brisanje zapisa iz seznama, le-tega izberite in kliknite gumb  **Odstrani**.

Kliknite **Naprej**.

## Korak 3/3 - Izbira vrste skeniranja



### Vrsta skeniranja


Lahko vidite tabelo, ki vsebuje poti, ki bodo izvzete iz skeniranja in vrsto skeniranja iz katerega bodo izvzete.

V osnovi so izbrane poti izvzete iz skeniranja ob dostopu in skeniranja na zahtevo. Za spremembo vrste skeniranja, za katero veclja izjema, kliknite na desno vrstico in izberite željeno možnost iz seznama.

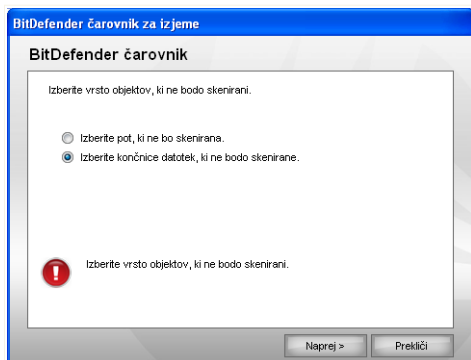
Kliknite **Končaj**.

Kliknite **Uporabi** za shranitev sprememb.

### 8.3.2. Izvzemanje končnic iz skeniranja

Za izvzetje končnic iz skeniranja kliknite gumb  **Dodaj** Čarovnik za nastavitve vas bo vodil skozi postopek izvzemanja končnic iz skeniranja.

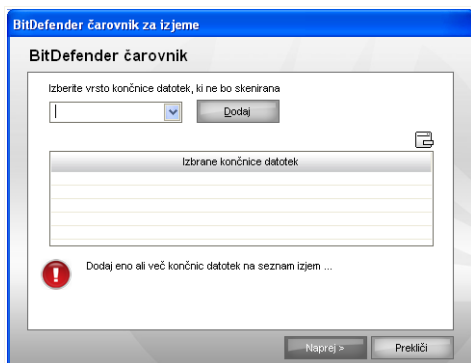
## Korak 1/3 – Izberite vrsto predmeta



### Vrsta predmeta

Izberite možnost izvzetja končnic iz skeniranja.  
Kliknite **Naprej**.

## Korak 2/3 – Določite izvzete končnice



### Izvzete končnice

Za določanje končnic, ki jih želite izvzeti uporabite enega izmed sledečih načinov.

- Iz seznama izberite končnico, ki jo želite izvzeti iz skeniranja, nato kliknite **Dodaj**.



### Opomba

Seznam vsebuje vse končnice, ki so na vašem računalniku. Ko izberete končnico, lahko vidite opis le te.

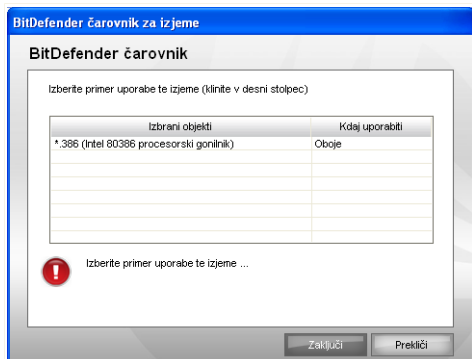
- Vpišite končnico, ki jo želite izvzeti iz skeniranja v polje za urejanje in kliknite **Dodaj**.

Končnice se bodo pojavile v razpredelnici, ko jih dodate. Dodate lahko neomejeno število končnic.

Za brisanje zapisa iz seznama, le-tega izberite in kliknite gumb **Odstrani**.

Kliknite **Naprej**.

## Korak 3/3 - Izbira vrste skeniranja



### Vrsta skeniranja

Vidite lahko razpredelnico s končnicami, ki bodo izvzete iz skeniranja in vrsto skeniranja iz katerega so izvzete,

V osnovi bodo izbrane končnice izvzete iz skeniranja na zahtevo in skeniranja ob dostopu. Za spremembo kliknite na desni stolpec in izberite ustrezno možnost iz seznama.

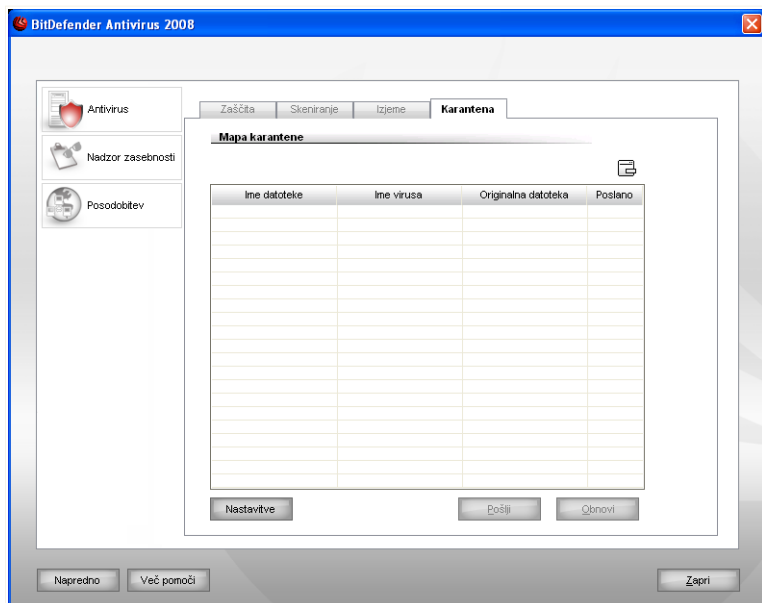
Kliknite **Končaj**.

Kliknite **Uporabi** za shranitev sprememb.

## 8.4. Karantena

BitDefender omogoča izoliranje okuženih in sumljivih datotek v zaščiteno območje, poimenovano karantena. Z izoliranjem teh datotek v karanteno se znebite tveganja, da bi vam virus še naprej škodil. Okužene datoteke lahko seveda pošljete v BitDefender-jeve laboratorije na podrobno analizo in s tem pripomorate k hitrejšemu odkrivanju novih virusov.

Za ogled in upravljanje z datotekami v karanteni kliknite **Antivirus>Karantena** v vmesniku za nastavitve.



Karantena

### 8.4.1. Upravljanje z datotekami v karanteni

Kot ste verjetno opazili vsebuje odsek **Karantena** seznam vseh do sedaj izoliranih datotek. Zraven vsake datoteke je zapisano njeno ime, velikost, datum izolacije in datum pošiljanja. Če želite videti še več podrobnosti, kliknite **Več podrobnosti**.

**Opomba**

Ko je virus v karanteni, je neškodljiv, ker ne more biti pogan ali prebran.

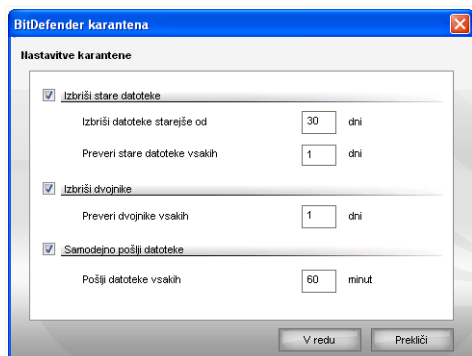
Za izbris izbrane datoteke kliknite **Odstrani**. Če želite obnoviti izbrano datoteko na izvorno lokacijo kliknite **Obnovi**.

Izbrane datoteke lahko pošljete iz karantene v BitDefenderjev laboratorij s pritiskom na **Pošlji**.

**Vsebinski meni.** S pomočjo vsebinskega menija lahko preprosto upravljate z datotekami v karanteni. Na voljo so enake možnosti kot so že bile omenjene. Za osvežitev karantene lahko izberete **Osveži**

## 8.4.2. Spreminjanje nastavitev karantene

Za spreminjanje nastavitev karantene kliknite **Nastavitve**. Odprlo se bo novo okno



### Nastavitve karantene

Z uporabo nastavitev karantene lahko BitDefender samodejno izvaja naslednja dejanja:

**Izbrisi stare datoteke.** Obkljukajte to možnost za samodejni izbris starih datotek iz karantene. Sami lahko določite kako dolgo naj BitDefender ohranja stare datoteke v karanteni in kako pogosto naj BitDefender pregleda stare datoteke.

**Opomba**

V osnovi bo BitDefender vsak dan poiskal stare datoteke in jih izbrisal vsake 10 dni.

**Briši dvojnike.** Za samodejn izbris podvojenih datotek v karanteni obkljukajte pripadajočo možnost. Določiti morate število dni med dvema zaporednima pregledoma za dvojniki.



**Opomba**

V osnovi bo BitDefender pregledal karanteno za dvojniki vsak dan.

**Samodejno pošlji datoteke.** Za samodejno pošiljanje datotek v karanteni obkljukajte pripadajočo možnost. Določiti morate pogostost pošiljanja datotek.



**Opomba**

V osnovi bo BitDefender samodejno pošiljal datoteke v karanteni na vsakih 60 min.

Kliknite **Potrdi** za shranitev sprememb.

## 9. Nadzor zasebnosti

Bitdefender nadzoruje več kot ducat vročih točk v vašem sistemu, kjer bi se lahko spyware aktiviral in prav tako preverja vsako spremembo, ki se zgodi vašemu sistemu in programski opremi. Poznane spyware grožnje se blokirajo v realnem času. Učinkovit je proti trojanskim konjem in ostalim orodjem, ki jih namestijo krekerji, ki skušajo ogroziti vašo zasebnost, ter se polastiti vaših podatkov, kot so številke bančnih računov in kreditnih kartic.

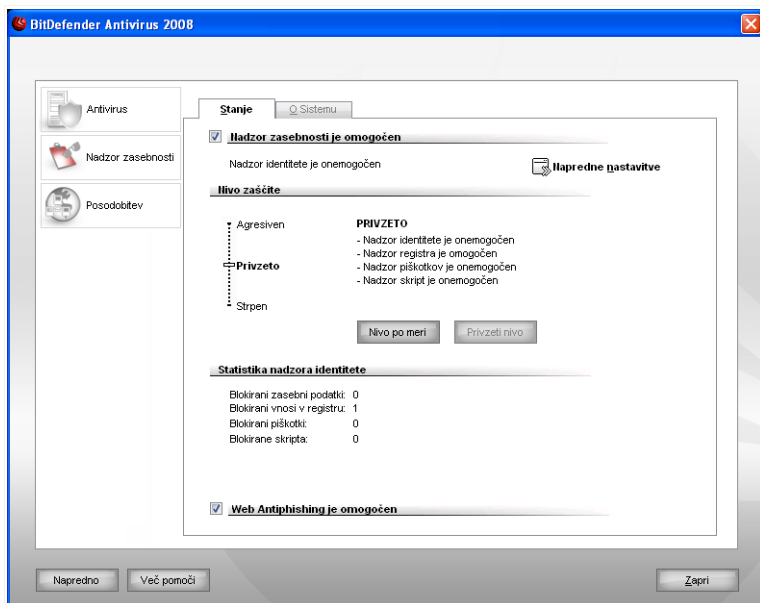
BitDefender skenira medmrežne strani, ki jih obiskujete in vas opozori pred nevarnostmi ribarjenja.

Poglavje **Nadzor zasebnosti** vsebuje naslednje teme:

- Stanje nadzornika zasebnosti
- Napredne nastavitve - Nadzor zasebnosti
- Napredne nastavitve-Nadzor registra
- Napredne nastavitve-Nadzor piškotkov
- Napredne nastavitve-Nadzor skript
- Sistemske informacije
- Orodna vsrtica Antiphishing

### 9.1. Stanje nadzora zasebnosti

Za spreminjanje nadzora zasebnosti in ogled informacij o aktivnostih le tega kliknite **Nadzor zasebnosti>Stanje** v vmesniku za nastavitve. Odprlo se bo novo okno:



Stanje nadzora zasebnosti

## 9.1.1. Nadzor zasebnosti



### Pomembno

Za preprečitev kraje podatkovimejte **Nadzor zasebnosti** vedno omogočen.

Nadzor zasebnosti ščiti vaš računalnik s pomočjo 5. pomembnih zaščitnih nadzornikov.

- **Nadzor zasebnosti** - ščiti vaše zasebne podatke s filtriranjem odhajajočega HTTP in SMTP prometa po pravilih, ki ste jih ustvarili na delu **Zasebnost**.



### Opomba

Na dnu lahko vidite statistiko **Statistika nadzora zasebnosti**.

- Modul **Nadzor registra** opazuje register, kar je zelo uporabno za odkrivanje trojanskih konjev. Opozoril vas bo vedno, ko bo kakšen program hotel spremeniti vsebino registra z namenom samodejnega zagona.
- Ko je **Nadzor piškotkov** aktiven, vas bo vedno, ko bo kakšna spletna stran želela ustvariti piškotek, prosil za potrditev.
- **Nadzor skript** boste vedno imeli v nadzoru spletne strani, ki jim zaupate in tiste, ki jim ne. Kadarkoli bo kakšna spletna stran želela pognati skripto, vas bo BitDefender prosil za potrditev / zavrnitev tega dejanja:

Za nastavitve nadzora kliknite  **Napredne nastavitve**.

## Nastavitev stopnje zaščite

Izbirate lahko med različnimi stopnjami zaščite, ki najbolj zadovoljujejo vaše potrebe po varnosti. Z drsnikom izberete zaželjeno stopnjo.

Na voljo so 3 stopnje zaščite:

Stopnja zaščite	Opis
<b>Dovoli</b>	Omogočen je samo <b>Nadzor registra</b>
<b>Privzeto</b>	Omogočena sta <b>Nadzor registra</b> in <b>Nadzor klicanja</b> .
<b>Agresivno</b>	Omogočeni so <b>Nadzor registra</b> , <b>Nadzor klicanja</b> in <b>Nadzor zasebnosti</b> .

Prilagodite stopnjo zaščito s klikom na **Stopnja po meri**. Odprlo se bo sledeče okno: Izberite željen nadzor in kliknite **V redu**.

Če kliknete **Privzeta stopnja**, boste naložili privzete nastavitve.

### 9.1.2. Antiphishing zaščita

Ribarjenje je kriminalna aktivnost na internetu, ki uporablja tehnike socialnega inženiringa za preslepitev ljudi, da izdajo zasebne informacije.

Večino phishing napadov se pojavi v obliki masovnih e-poštnih sporočil, ki lažno trdijo, da prihajajo od legalnega podjetja. Ta lažna sporočila so poslana v upanju, da bo vsaj peščica prejemnikov pripravljena razkriti zasebne informacije.

Sporočilo, ki vsebuje phishing navadno vsebuje vsebine povezane z vašimi medmrežnimi računi. Poskuša vas prepričati, da kliknete domnevno legitimno stran (v bistvu ponaredek), kjer zahtevajo zasebne informacije. Zahtevajo lahko naprimer

potrditev uporabniškega imena in gesla, bančni račun, številko police osebnega zavarovanja, ipd. Včasih ta sporočila, zaradi večje prepričljivosti, vsebujejo opozorilo, da je vaš račun ogrožen in bo odstranjen, če ne kliknete navedene povezave.

Ribarjenje uporablja tudi vohunske programe, ki omogočajo krajo zasebnih informacij neposredno iz vašega računalnika.

Glavne tarče so uporabniki internetnih plačilnih storitev, kot sta eBay ali PayPal, kot tudi uporabniki medmrežnih bančnih storitev. zadnje čase se pojavlja vse več poskusov ribarjenja s pomočjo strani za socialno mreženje, kjer poskušajo pridobiti podatke za osebno identifikacijo z namenom kraje identitete.

Za zaščito pred ribarskimi napadi, kadar brskate po internetu omogočite **Antiphishing**. BitDefender bo skeniral vsako stran preden vam dovoli dostop in vas opozoril, če obstaja možnost ribarskega napada. Nastavite lahko seznam dovoljenih internetnih strani, katere BitDefender ne bo skeniral.

Za lažje upravljanje zaščite pred ribarjenjem in seznama dovoljenih strani, uporabite BitDefenderjevo orodno vrstico Antiphishing. Za več informacij se obrnite na "*Orodna vrstica zaščite neželene pošte*" (p. 101).

## 9.2. Napredne nastavitve-Nadzor identitete.

Varovanje zasebnih podatkov je tema, ki nas vse obremenjuje. Kraje podatkov so ohranile stik z razvojem ITja in se stalno poslužujejo novih metod kako prevarati ljudi, da izdajo zaupne informacije.


**Nadzor identitete** pomaga ohranjati varnost vaših zasebnih podatkov. Skenira HTTP ali SMTP promet, ali oboje, in išče vrstice, ki ste jih vi definirali. Če najde odgovarjajoče dele, blokira internetno stran ali epšto.

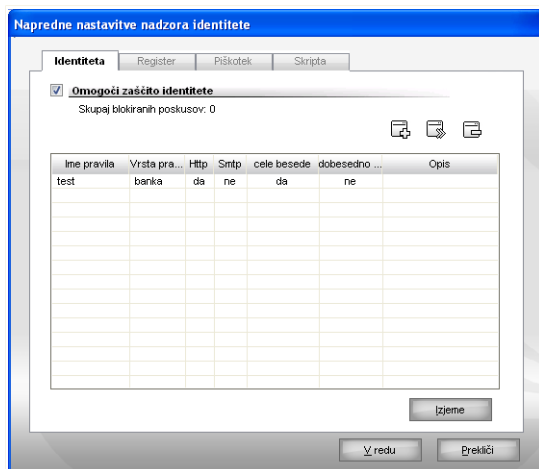
Večuporabniška podpora je zagotovljena tako, da ostali uporabniki ne morejo spreminjati pravil, ki ste jih dodali vi.

Pravila zasebnosti lahko spreminjate v delu **Identiteta** Za dostop do tega dela odprite okno **Napredne nastavitve nadzor zasebnosti** in kliknite zavihek **Identiteta**



### Opomba

**Napredne nastavitve nadzor zasebnosti** odprete s klikom na **Nadzor zasebnosti** > **Stanje** v vmesniku za nastavitve in kliknete  **Napredne nastavitve**.



Nadzor identitete

### 9.2.1. Ustvarjanje pravil identitete

Pravila morajo biti vnesena ročno (kliknite  **Dodaj** in izberite parametre za pravilo). Odpre se čarovnik za nastavitve.

Nastavitveni čarovnik ima 3 korake.

## Korak 1/3 - Določi vrste pravil in podatke

### Nastavite tipe pravil in podatke

Vpišite ime pravila v polje za urejanje.

Nastaviti morate naslednje parametre:

- **Vrsta pravila** - izberite vrsto pravila (naslov, ime, kreditna kartica, PIN, SSN itd.).
- **Podatki pravila** - Vnesite podatke o pravilu.



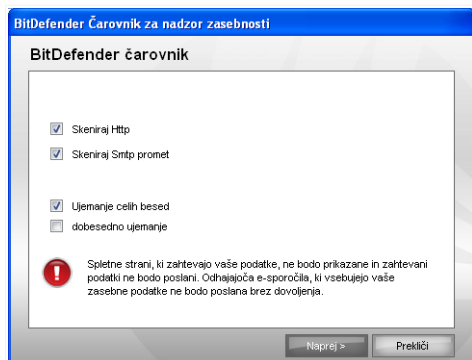
#### **Opomba**

V kolikor vpišete manj kot 3 znake, boste opozorjeni, da ponovno potrdite podatke. Priporočamo vam, da vpišete vsaj 3 znake v izogib preprečevanju napačnih strani in sporočil.

Podatki ki jih vnašate so kodirani. Za dodatno varnost ne vnašajte celotnih vrstic, ki jih želite zavarovati.

Kliknite **Naprej**.

## Korak 2/3 - Izbira prometa



### Izberite promet

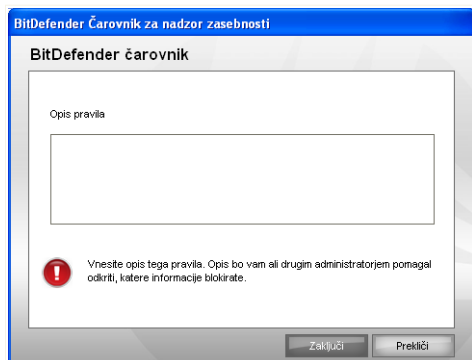
Izberite tip prometa, ki želite, da ga BitDefender skenira. Možnosti so naslednje:

- **Skeniraj HTTP** - skenira HTTP (mrežni) promet in prepreči odhajajoče podatke, ki ustrezajo pravilu.
- **Skeniraj SMTP** - skenira ves SMTP promet in prepreči vsa odposlana elektronska sporočila, ki vsebujejo pravilo.

Pravilo lahko uporabite le, če podatki pravila ustrezajo vsem besedam ali, če se podatki pravila in zaznani nizi besed enaki.

Kliknite **Naprej**.

## Korak 3/3 – Opis pravila



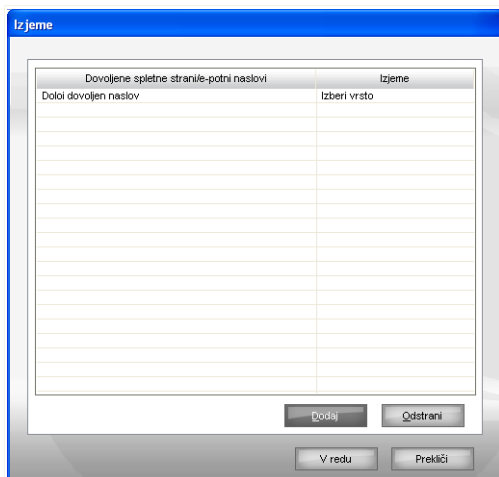
### Opiše pravilo

Vnesite kratek opis pravila v polje za urejevanje.  
Kliknite **Končaj**.

## 9.2.2. Določanje izjem

V nekaterih primerih morate določiti izjeme posameznim pravilom identitete. Vzemimo primer, ko ustvarite pravilo, ki preprečuje pošiljanje številke vaše kreditne kartice preko HTTP prometa. Kadarkoli je številka poslana na stran, je ta stran blokirana. Za strani, ki bi jih vseeno želeli uporabljati lahko ustvarite izjeme omenjenemu pravilu.

Za upravljanje z izjemami kliknite **Izjeme**.



### Izjeme

Za dodajanje izjem sledite tem korakom.


1. Za nov vnos v preglednico kliknite **Dodaj**
2. Dvokliknite **Doloi dovoljene naslove** in navedite naslove strani ali poštno naslove, ki jih želite dodati kot izjeme.
3. Dvokliknite **Izberite vrsto** in izberite iz seznama pripadajočo možnost vrsti naslova, ki ste ga vpisali.
  - V kolikor ste določili mrežni naslov izberite **HTTP**.
  - V kolikor ste določili poštni naslov izberite **SMTP**.


Izjemo odstranite iz seznama s klikom na **Odstrani**.

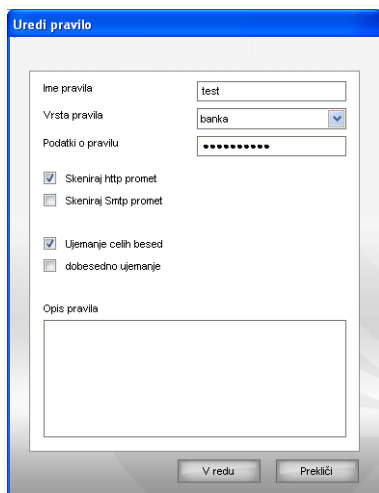
Kliknite **Potrdi** za shranitev sprememb.

## 9.2.3. Upravljanje pravil

Tu lahko vidite pravila razporejena v tabelo.

Za izbris pravila, ga izberite in kliknite  **Izbriši**. Za začasno ustavitev pravila, brez, da ga izbrisali označite okence pred pravilom.

Za urejanje pravila ga izberite in kliknite gumb  **Uredi** ali dvokliknite pravilo. Odprlo se bo novo okno.



Uredite pravilo

Tukaj lahko spremenite ime, opis in parametre dovoljenj(tip, podatki, promet). Kliknite **V redu**, da shranite spremembe.

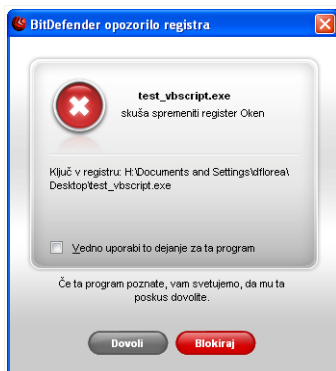
Kliknite **Potrdi** za shranitev sprememb.

### 9.3. Napredne nastavitve-Nadzor registra

Zelo pomembna komponenta Windows operacijskih sistemov je **Register** operacijski sistemi shranjujejo svoje nastavitve, nameščene programe, uporabnikove informacije itd.

**Register** je uporabljan tudi za določanje, kateri programi naj se zaženejo ob zagonu operacijskega sistema. Virusi velikokrat izkoriščajo to možnost, da si omogočijo zagon vedno, ko uporabnik zažene računalnik.

Modul **Nadzor registra** opazuje register, kar je zelo uporabno za odkrivanje trojanskih konjev. Opozoril vas bo vedno, ko bo kakšen program hotel spremeniti vsebino registra z namenom samodejnega zagona.



### Opozorilo registra

Spremembo lahko zavrnete s klikom na gumb **Ne** ali pa jo dovolite s klikom možnosti **Da**.

BitDefender si lahko zapomni vaše izbire; to omogočite z obkljukanjem kvadratika: **Zapomni si ta odgovor**. Pravilo bo ustvarjeno in isto dejanje se bo ponovilo kadarkoli ta program želi spremeniti vnos v registru, da bi se izvedel ob zagonu.




#### Opomba

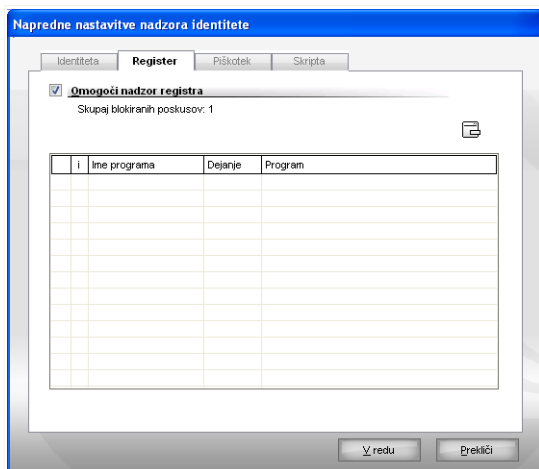
BitDefender običajno ob namestitvi novih programov, ki potrebujejo nov zagon po namestitvi, obvesti uporabnika o nevarnosti, a so taki programi večinoma neškodljivi.

Vsako pravilo, ki je bilo shranjeno lahko urejate v **Register**. Za dostop do tega dela odprite **Napredne nastavitve-Nadzor zasebnosti** in kliknite zavihek **Register**.




#### Opomba

**Napredne nastavitve nadzor zasebnosti** odprete s klikom na **Nadzor zasebnosti>Stanje** v vmesniku za nastavitve in kliknete  **Napredne nastavitve**.



#### Nadzor registra

Tu lahko vidite pravila razporejena v razpredelnico.

Za brisanje zapisa iz seznama, le-tega izberite in kliknite gumb  **Odstrani**. Za začasno onemogočanje pravila, ne da bi ga izbrisali, odkljukajte pripadajoč kvadratek.

Za spremembo dejanja pravila, dvokliknite polje dejanja in izberite ustrezno možnost iz seznama.

Kliknite **V redu** da zaprete okno.

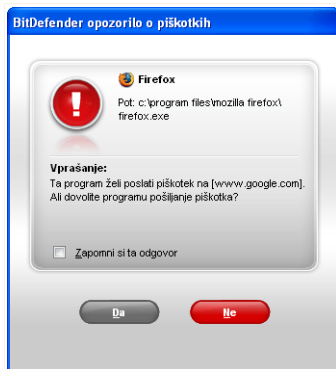
## 9.4. Napredne nastavitve-Nadzor piškotkov

**Piškotki** se redno pojavljajo na spletu. So majhne datoteke, shranjene na vašem računalniku. Piškotke ustvarijo spletne strani, da shranjujejo določene informacije o vas in dostopu do določene spletne strani.

Piškotki so v večini ustvarjeni, da vam olajšajo delo s spletnimi stranmi. Ponavadi shranjujejo vaše prijavnne podatke in nastavitve, tako da vam jih ni potrebno vnašati ponovno ob vsakem obisku teh spletnih strani.

Seveda pa so tudi piškotki lahko uporabljeni za zbiranje vaših osebnih informacij.

ln tu na pomoč priskoči **Nadzor piškotkov**. Ko je **Nadzor piškotkov** aktiven, vas bo vedno, ko bo kakšna spletna stran želela ustvariti piškotek, prosil za potrditev:



### Opozorilo o piškotku

Prikazano bo ime aplikacije, ki želi poslati piškotek.

Izberite **Zapomni si ta odgovor** in izberite **Da** ali **Ne** in ustvarjeno bo novo pravilo o (ne)dovoljenih povezavah tega programa. Ko bo ta spletna stran želela ponovno ustvariti piškotek, vas BitDefender ne bo več prosil za potrditev/zavrnitev, ker se bo ravnal po pravilih za to aplikacijo.

To vam omogoča lažje izbiranje, katerim stranem zaupate in katerim ne.




#### Opomba

Zaradi večjega števila piškotkov zna biti začetek z **Nadzor piškotkov** kar težaven. Na začetku vas bo namreč veliko spraševal o straneh, ki skušajo namestiti piškotke na vaš računalnik. Takoj ko boste dodali pogosto obiskovane strani na vaš seznam pa bo deskanje po spletu postalo bolj enostavno kot kdajkoli prej.

Vsako shranjeno pravilo je dostopno v odseku **Piškotki**. Za dostop do teh možnosti kliknite zavihek **Napredno** v modulu **Požarni zid**.

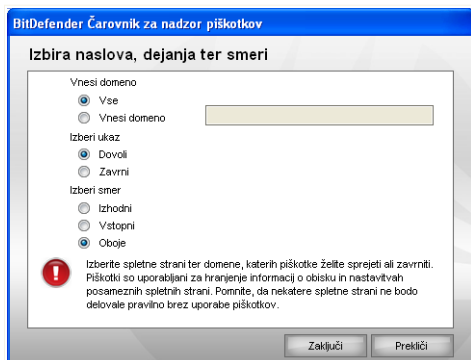


#### Opomba

**Napredne nastavitve nadzor zasebnosti** odprete s klikom na **Nadzor zasebnosti**>**Stanje** v vmesniku za nastavitve in kliknete  **Napredne nastavitve**.



## Korak 1/1 - Izberite naslov, dejanje in smer



### Izberite naslov, dejanje in smer

Nastavitve parametrov:

- **Naslov domene** - Vnesite naslov domene, za katero naj pravilo velja.
- **Dejanje** - Izberite katero dejanje naj pravilo izvrši.

<i>Dejanje</i>	<i>Opis</i>
<b>Dovoli</b>	Dovoli izvajanje piškotkov izbrane domene.
<b>Zavrni</b>	Zavrne izvajanje piškotkov izbrane domene.

- **Smer** - izberite smer prometa.

<i>Vrsta</i>	<i>Opis</i>
<b>Odhajajoči</b>	Pravilo bo veljalo za piškotke, ki so poslani nazaj na spletno stran.
<b>Prihajajoči</b>	Pravilo velja za piškotke, ki so poslani iz spletne strani.
<b>Oboje</b>	Pravilo velja za obe smeri.

Kliknite **Končaj**.

**Opomba**

Če želite, da bi piškotke le sprejemali, ne pa tudi pošiljali (vračali), izberite možnost **Zavrni** in smer prometa **Odhajajoči**.

Kliknite **Potrdi** za shranitev sprememb.

## 9.5. Napredne nastavitve-Nastavitve skripte

**Skripte** in podobni skupki kode kot so **ActiveX controls** in **Java applets**, ki se uporabljajo na interaktivnih spletnih straneh, so lahko preprogramirane, da povzročajo zelo nevarne učinke. ActiveX elementi tako lahko prevzamejo popoln nadzor nad vašimi podatki (to pomeni branje, spreminjanje in brisanje podatkov) medtem, ko ste povezani na internet. Tovrstne povezave izrecno dovolite samo stranem, ki jih dobro poznate in jim popolnoma zaupate.

BitDefender vam omogoča poganjanje teh elementov ali blokiranje njihovega izvajanja.

S **Nadzor skript** boste vedno imeli v nadzoru spletne strani, ki jim zaupate in tiste, ki jim ne. Kadarkoli bo kakšna spletna stran želela pognati skripto, vas bo BitDefender prosil za potrditev / zavrnitev tega dejanja:



**Opozorilo o skripti**

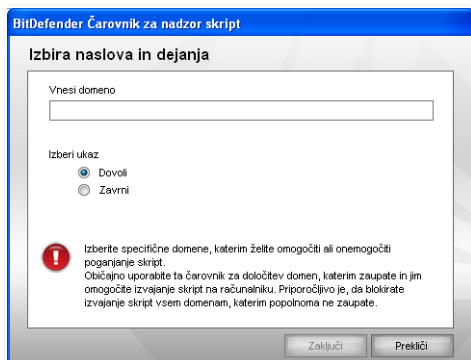
Tu lahko vidite ime vira.

Izberite **Zapomni si ta odgovor** in izberite **Da** ali **Ne** in ustvarjeno bo novo pravilo o (ne)dovoljenih povezavah tega programa. Ko bo ta spletna stran želela ponovno pognati skripto, vas BitDefender ne bo več prosil za potrditev/zavrnitev, ker se bo ravnal po pravilih za to aplikacijo.

Vsako shranjeno pravilo je dostopno v odseku **Skripta**. Za dostop do tega dela odprite **Napredne nastavitve-Nadzor zasebnosti** in kliknite zavihek **Skripta**.



## Korak 1/1 - Izbira naslova in dejanja



Izberite naslov in dejanje

Nastavitve parametrov:

- **Naslov domene** - Vnesite naslov domene, za katero naj pravilo velja.
- **Dejanje** - Izberite katero dejanje naj pravilo izvrši.

<i>Dejanje</i>	<i>Opis</i>
<b>Dovoli</b>	Skripte na tej domeni se bodo izvajale.
<b>Zavrni</b>	Skripte na tej domeni se ne bodo izvajale.

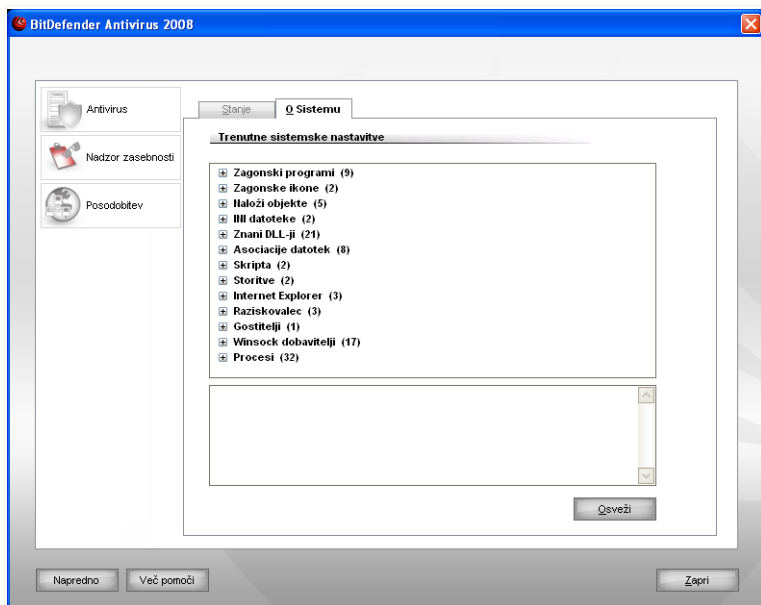
Kliknite **Končaj**.

Kliknite **Potrdi** za shranitev sprememb.

## 9.6. Sistemske informacije

BitDefender vam omogoča ogled vseh sistemskih nastavitvev in programov, ki se zaženejo ob zagonu računalnika. Na ta način lahko spremljate aktivnosti vašega sistema in programe, ki so naloženi ter možne okužbe sistema.

Za sistemske informacije kliknite **Nadzor zasebnosti > Sistemske informacije** v vmesiku za nastavitve. Odprlo se bo novo okno:



### Sistemske informacije

Seznam vsebuje vse datoteke, ki se naložijo ob zagonu sistema in ob zagonu določene aplikacije.

Na voljo so trije gumbi:

- **Odstrani** - izbriše izbrani element. Za potrditev izbire morate klikniti **Da**.



#### Opomba

V kolikor ne želite biti ponovno opomnjeni, da morate potrditi vašo izbiro med to sejo kliknite **Ne vprašaj več med to sejo**.

- **Pojdi** - odpre okno, kjer je izbrani element (npr. **Register**).
- **Osveži** - ponovno naloži **O sistemu**.




#### Opomba

Pojavi se eden ali oba gumba **Odstrani** ali **Pojdi**

## 9.7. Orodna vrstica zaščite neželene pošte

BitDefender vas varuje pred napadi ribarjenja medtem, ko brskate po internetu. Skenira dostopane internetne strani in vas opozori ob nevarnostih ribarjenja. Nastavite lahko seznam dovoljenih internetnih strani, katere BitDefender ne bo skeniral.

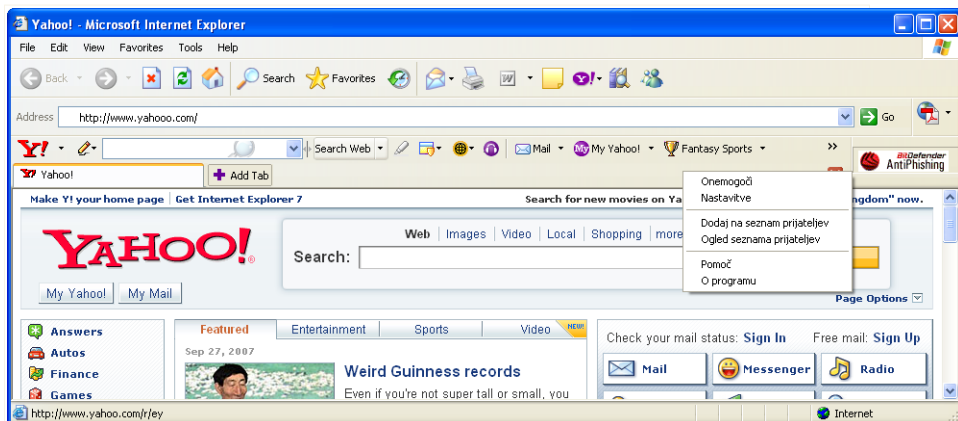
Preprost in učinkovit način za upravljanje z zaščito pred ribarjenjem in Seznamom prijateljev je BitDefender Antiphishing orodna vrstica, ki je integrirana v Internet Explorer.

Orodna vrstiva antiphishing, je prikazana z  **BitDefender ikono**, ki je locirana na zgornji strani Internet Explorerja. Za odprtje seznama orodne vrstice kliknite ikono BitDefender.



### Opomba

V kolikor ne vidite orodne vrstice odprite seznam **Pogled** poglejte **Orodne vrstice** In izberite **BitDefender orodna vrstica**.



### Orodna vrstica zaščite neželene pošte

Možnosti so naslednje:

- **Omogoči / Onemogoči** omogoči / onemogoči BitDefender Antiphishing orodno vrstico.



### Opomba

Če onemogočite orodno vrstico antiphishing, ne boste več zaščiteni pred napadi ribarjenja.

- **Nastavitve** - odpre okno, kjer lahko določite nastavitve orodne vrstice antiphishing.

Možnosti so naslednje:

- **Omogoči skeniranje** - omogoči antiphishing skeniranje
- **Vprašaj pred uvrstitvijo na Seznam prijateljev** - opozori preden doda stran v seznam prijateljev

- **Dodaj na seznam prijateljev** - doda trenutno stran na seznam prijateljev.



### Opomba

Dodajanje strani v Seznam prijateljev prepreči BitDefenderju skeniranje teh strani ob dostopu. Priporočamo, da dopdajate strani v seznam prijateljev le, če jim popolnoma zaupate.

- **Prikaži Seznam prijateljev** - odpre Seznam prijateljev.

Vidite lahko seznam vseh strani, ki jih BitDefenderjev antiphishing pogon ne kontrolira.

V kolikor želite odstraniti stran s Seznama prijateljev, da vas bo obveščalo o možnih nevarnostih ribarjenja, kliknite gumb **Odstrani**.

Na Seznam prijateljev lahko dodate strani, ki jim popolnoma zaupate in ne želite, da jih pregleda BitDefenderjev antiphishing pogon. Za dodajanje strani v Seznam prijateljev, vpišite naslov v prostor za vnašanje in kliknite **Dodaj**.

- **Pomoč** - odpre pomoč.
- **O programu** - odpre se okno, kjer lahko vidite informacije o BitDefenderju in pomoči.

## 10. Posodobitev

Novi virusi so odkriti in prepoznani vsak dan. Zato je ključnega pomena, da je Bitdefender redno posodobljen z vsemi novimi definicijami virusov. Privzeti čas BitDefenderja za preverjanje novih posodobitev je uro.

Če ste povezani na internet preko širokopasovne povezave, oz. ADSLa, bo Bitdefender skrbel sam zase. Ko se boste povezali na internet, bo sam pregledal za posodobitve in vsake **ura** za tem.

Če je zaznana nova posodobitev, odvisno od nastavitve **Možnost samodejnega posodabljanja**, vas bo program, če ga želite posodobiti ali pa se bo posodobitev izvedla samodejno.

Pri posodobitvah se datoteke nadomeščajo progresivno. Na ta način preprečimo napake v delovanju produkta in izključimo ranljivost zaradi posodabljanja programa.

Posodobitve prihajajo na naslednje načine:

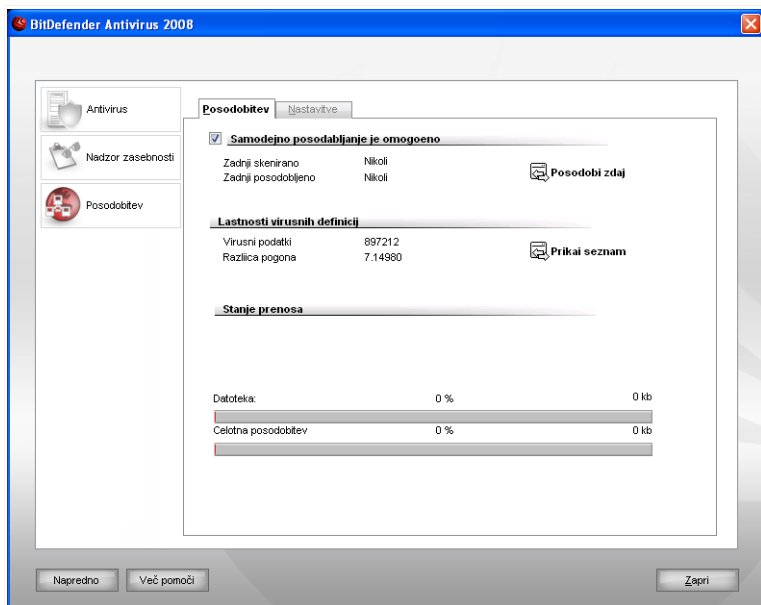
- **Posodobitve za antivirusne module** - ob pojavi novih groženj, morajo biti datoteke, ki vsebujejo podpise virusov, posodobljene, za zagotovitev stalne zaščite pred le-timi. Te posodobitve so znane tudi kot **Posodobitev virusnih definicij**.
- **Posodobitve pogona za odkrivanje vohunskih programov** - nove posodobitve bodo dodane v bazo. Te posodobitve so znane tudi kot **Posodobitev protivohunske zaščite**.
- **Programske posodobitve** - ko je izdana nova verzija programa, pridejo na trg nove prednosti programa in nove tehnike skeniranja, ki izboljšajo učinek programa. Te posodobitve so znane tudi kot **Posodobitev programa**.

Poglavje **Posodobitev** vsebuje naslednje teme:

- **Samodejno posodabljenje**
- **Nastavitve posodobitev**



### 10.1. Samodejno posodabljanje

Za ogled informacij v zvezi s posodobitvami in izvedbo samodejnih posodobitev kliknite **Posodobi>Posodobi** v vmesniku za nastavitve. Odprlo se bo novo okno:



### Samodejno posodabljanje

Tu si lahko ogledate zadnje posodobitve in pridobite informacije o uspešnosti izvedbe zadnje posodobitve. na voljo so tudi informacije o različici in številu podpisov.

Podpise zlonamernih programov vašega BitDefenderja lahko dobite tukaj s klikom  **Prikaži seznam**. HTML datoteka, ki vsebuje vse podpise, ki so na voljo, bo kreirana. Ponovno kliknite  **Prikaži seznam**, da si ogledate seznam. Pregledujete lahko podatkovne baze in iščete specifične zlonamerne podpise ali kliknite **BitDefenderjev seznam virusov** da dostopite do BitDefenderjeve baze podpisov.


Če odprete ta del med posodabljanjem, si lahko ogledate stanje dolpotega.



#### **Pomembno**

Za zaščito pred najnovejšimi grožnjami pustite **Samodejno posodabljanje** omogočeno.

## 10.1.1. Zahteva posodobitev

Samodejno posodabljanje je moč izvesti kadarkoli s klikom na možnost  **Posodobi zdaj**. Takšno posodabljanje se imenuje tudi **Posodobitev na zahtevo uporabnika**.

Modul **Posodobitev** se bo povezal z BitDefender posodobitvenim strežnikom in preveril za morebitnimi posodobitvami. Če zazna novo posodobitev, odvisno od nastavitve **Nastavitve ročnega posodabljanja**, vas bo program, če ga želite posodobiti ali pa se bo posodobitev izvedla samodejno.



### **Pomembno**

Lahko se zgodi da boste morali ponovno zagnati računalnik, ko bo BitDefender končal z namestitvijo posodobitev. Priporočeno je, da to storite takoj, ko bo to mogoče.

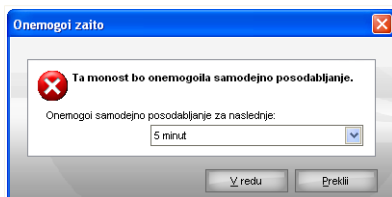


### **Opomba**

Če ste na internet povezani preko klicne povezave, bi bilo primerno, da spremenite nastavitve tako, da boste sami pregledovali za posodobitve.

## 10.1.2. Onemogočanje samodejnega posodabljanja

Če želite onemogočiti samodejno posodabljanje, se bo pojavilo opozorilno okno.



### **Onemogoči samodejno posodabljanje**

Svojo izbiro morate potrditi z določanjem časa onemogočanja samodejnega posodabljanja. Samodejno posodabljanje lahko omogočate za 5, 15 ali 30 minut, eno uro, neomejeno ali do ponovnega zagona sistema.



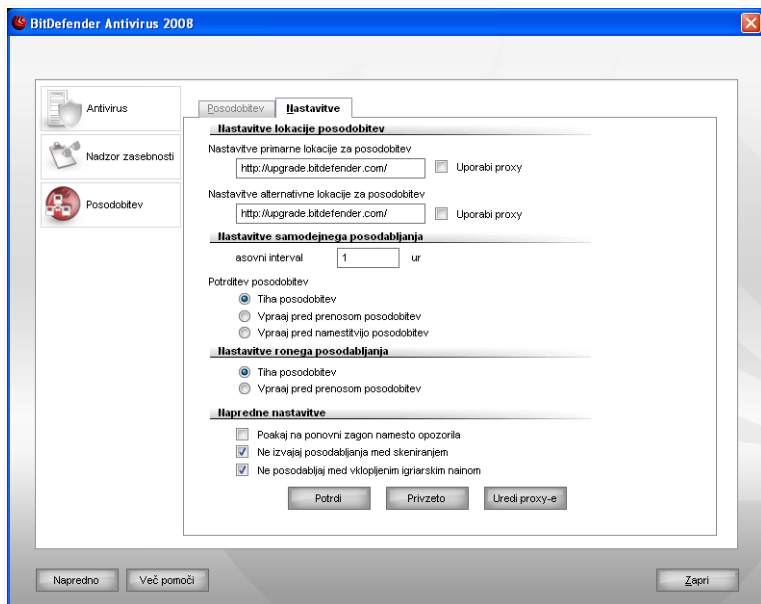
### **Pozor**

To je pomemben del varovanja. Priporočamo vam, da onemogočate samodejno posodabljanje kar se da redko. Če BitDefender ni redno posodabljan, zaščita ne bo delovala pravilno, saj ne boste, zaščiteni pred najnovejšimi grožnjami.

## 10.2. Posodobitvene nastavitve

Posodobitve se lahko izvedejo preko lokalnega omrežja, preko interneta, direktno ali preko proxy strežnika. V osnovi bo BitDefender posodabljan vsako uro. Namestitve bodo nameščene brez predhodnega opozorila.

Za določanje nastavitve posodabljanja in upravljanje s proxiji kliknite **Posodobitve>Nastavitve** vmesniku za nastavitve. Odrplo se bo novo okno:



### Posodobitvene nastavitve

Okno z nastavitvami posodabljanja vsebuje 4 kategorije nastavitvev (**Nastavitve lokacije posodobitev**, **Možnosti samodejnega posodabljanja**, **Nastavitve ročnega posodabljanja** in **Napredne nastavitve**), ki so nameščene v razširitvene menije, podobno kot v Windows.

## 10.2.1. Nastavitve lokacij posodobitev

Za nastavitve lokacij posodabljanja uporabite možnosti iz kategorije **Nastavitve lokacij posodobitev**.



### Opomba

Te nastavitve spreminjajte le, kadar ste povezani v lokalno omrežje, ki lokalno hrani BitDefenderjeve podpise ali, če ste povezani preko proxy strežnika.

Za bolj zanesljive in hitrejše prenose, lahko konfigurirate dve posodobitveni lokaciji: **Nastavitve primarne lokacije za posodobitve** in **Nastavitve alternativne lokacije za posodobitve**. Za obe morate konfigurirati naslednje možnosti:

Za spremembo lokacij posodabljanja vnesite URL lokalnega ogledala v pripadajočemu polju lokacije, ki jo želite spremeniti **URL**.



### Opomba

Priporočamo, da kot primarno lokacijo posodabljanja nastavite lokalno ogledalo, sekundarno lokacijo pa pustite nespremenjeno, saj v primeru težav na lokalnem ogledalu sekundarna lokacija vseeno omogoča posodabljanje.

V kolikor uporabljate proxy strežnik pregledajte **Uporabi proxy** in nato kliknite **Upravljaj s proxy strežniki** za spreminjanje nastavitve proxy strežnikov.



### Opomba

Za več informacij se obrnite na "[Upravljanje proxyjev](#)" (p. 109)

## 10.2.2. Spreminjanje samodejnih posodobitev

Za zaščito kritičnih podatkov lahko BitDefender izvaja samodejno posodabljanje. Za spreminjanje postopka posodabljanja, ki ga BitDefender izvaja samodejno uporabite možnosti v kategoriji **Nastavitve samodejnega posodabljanja**.

Določite lahko število ur med dvema zaporednima pregledoma za posodobitvami v polju **Časovni interval**. V osnovi je ta interval nastavljen na 1 uro.

Za določanje poteka postopka posodabljanja izberite eno izmed naslednjih možnosti.

- **Tiha posodobitev** - Bitdefender sam prenese in namesti posodobitve.
- **Vprašaj pred prenosom posodobitev** - vsakič, ko bodo posodobitve na voljo, vas bo program vprašal, pred prenosom.



**Opomba**

Opozorjeni boste pred posodabljanjem, tudi če zaprete Varnostni center

- **Vprašaj pred namestitvijo posodobitev** - vsakič, ko bo posodobitev prenesena, vas bo program vprašal pred namestitvijo.



**Opomba**

Opozorjeni boste pred posodabljanjem, tudi če zaprete Varnostni center

### 10.2.3. Spreminjanje ročnih posodobitev.

Za določanje poteka postopka ročnega posodabljanja izberite eno izmed naslednjih možnosti v kategoriji **Nastavitve ročnega posodabljanja**

- **Tiha posodobitev** - ročno posodabljanje se bo izvedlo avtomatično in v ozadju.
- **Vprašaj pred prenosom posodobitev** - vsakič, ko bodo posodobitve na voljo, vas bo program vprašal, pred prenosom.



**Opomba**

Opozorjeni boste pred posodabljanjem, tudi če zaprete Varnostni center

### 10.2.4. Spreminjanje naprednih nastavitev

V kolikor želite preprečiti BitDefenderju posodabljanje, medtem ko delate, spremenite nastavitve v kategoriji **apredne nastavitve**.

- **Počakaj na ponovni zagon namesto opozorila** - če posodobitev potrebuje ponovni zagon, bo izdelek deloval s starimi nastavitvami do ponovnega zagona sistema. Uporabnik ne bo pozvan za ponovni zagon, zato BitDefenderjevo posodabljanje ne bo motilo uporabnikovega dela.
- **Ne izvajaj posodabljanja med skeniranjem** - BitDefender se ne bo posodobil, če je aktiven proces skeniranja. Posodobitev BitDefenderja se ne vmešava v naloge skeniranja.



**Opomba**

Če boste BitDefender posodobili med skeniranjem, se bo proces skeniranja prekinil.

- **Ne izvajaj posodobljanja, ko je vklopljen igričarski način** - BitDefender se ne bo posodobil, če je vklopljen igričarski način. Na ta način lahko minimizirate vplive izdelka na delovanje sistema med igranjem.

## 10.2.5. Upravljanje proxyjev

V koikor uporabljate proxy strežnik za dostop do interneta, morae določiti nastavitve za proxy, da se BitDefender lahko posodobí. Drugače, bo uporabil nastavitve administratorja, ki je naložil produkt ali nastavitve trenutnega prízetega brskalnika.



### Opomba

Nastavitve za proxy lahko spreminja samo admionistrator sistema ali uporabniki, ki poznajo geslo za nastavitve.

Za upravljanje z nastavitvami za proxy kliknite **Upravljaj s proxyji**. Pojavilo se bo okno **Upravljalca za proxy**.

**Upravitelj proxy strežnikov**

**Nastavitve proxy strežnikov**

**Administratorjeve proxy nastavitve (zaznaj ob namestitvi)**

IP naslov :  Vrata :  Uporabnikovo ime :   
Geslo :

**Nastavitve proxy strežnika trenutnega uporabnika (iz prízetega brskalnika)**

IP naslov :  Vrata :  Uporabnikovo ime :   
Geslo :

**Doloi lastne nastavitve proxy strežnika**

IP naslov :  Vrata :  Uporabnikovo ime :   
Geslo :

### Upravljalca za proxy

Obstajajo tri kategorije opravil skeniranja.

- **Administratorjeve nastavitve za proxy (zaznane ob inštalaciji)** - proxy nastavitve zaznane na administratorjevemu profilu ob inštalaciji se lahko spreminjajo samo, če ste prijavljeni v ta profil. V kolikor proxy strežnik zahteva uporabniško ime in geslo, ju je potrebno določiti v pripadajočem polju.
- **Proxy nastavitve trenutnega uporabnika (privzetega brskalnika)**-proxy nastavitve trenutnega uporabnika v privzetem brskalniku. Če proxy strežnik zahteva uporabniško ime in geslo, ju morate določiti v pripadajočem polju.



#### **Opomba**

Podprti brskalniki so Internet Explorer, Mozilla Firefox in Opera. Če uporabljate drugačen privzeti brskalniki, BitDefender ne bo mogel prevzeti proxy nastavitve trenutnega uporabnika.

- **Vaš skupek proxy nastavitve.** - proxy nastavitve ki jih lahko spreminjate, če ste prijavljeni v administratorski profil.

Določene morajo biti naslednje nastavitve:

- **Naslov** - Vnesite IP-naslov proxy strežnika.
- **Vrata** - vpišite vrata, ki jih BitDefender uporablja za povezavo do proxy strežnika.
- **Uporabniško ime** - vpišite uporabniško ime, ki ga bo proxy strežnik prepoznal.
- **Geslo** - vpišite veljavno geslo za prej navedenega uporabnika.

Ko se povežete v Internet, se poskušajo izvesti posamezni skupki nastavitve, dokler se BitDefenderju ne uspe povezati.

Najprej bo uporabljen vaš skupek nastavitve za proxy, za povezavo v Internet. Če ne deluje, se uporabijo nastavitve zaznane pri inštalaciji. Če tudi ta pot ni uspešna, bodo uporabljene proxy nastavitve privzetega brskalnika za povezavo v Internet.

Kliknite **Potrdi** za shranitev sprememb.

Kliknite **Uporabi** za shranitev sprememb. Ob kliku na **Privzeto** se naložijo privzete nastavitve.

# **BitDefenderjev obnovitveni CD**

## 11. Pregled

**BitDefender Antivirus 2008** se distributira z zagonskim CDjem (BitDefenderjev reševalni CD, ki je osnovan na LinuxDefenderju), ki je sposoben skenirati in dezinficirati vse trde diske pred zagonom vašega operacijskega sistema.

Reševalni CD uporabite kadarkoli je obnašanje operacijskega sistema nestabilno zaradi virusne okužbe. To je rezultat neuporabe antivirusnega programa.

Posodobitev se izvede samodejno, vsakič, ko zaženete sistem z BitDefender reševalnim CDjem.

LinuxDefender je pre-programirana Knoppix distribucija, ki je vdela v trenutno BitDefenderjevo Linux varnostno rešitev na GNU/Linux Knoppix Live CD in ponuja takojšnjo SMTP antivirus/antispam zaščito ter namizni antivirusni program, ki je sposoben skeniranja in dezinfekcije obstoječih trdih diskov (vključujoč NFTS particije). Prav tako je ponujeno oddaljeno Samba/Windows deljenje za NFS točke. Vključena pa je tudi omrežno zasnovan nastavitveni vmesnik.



### Opomba

BitDefender obnovitveni CD je moč prenesti z naslednje povezave: [http://download.bitdefender.com/rescue\\_cd/](http://download.bitdefender.com/rescue_cd/)

## 11.1. Sistemske zahteve

Preden zaženete sistem z BitDefenderjevim zagonskim Cdjem, se prepričajte, če vaš sistem ustreza minimalnim zahtevam.

### Vrsta procesorja

x86 kompatibilen, najmanj 166 MHz, vendar s takim sistemom ne pričakujte hitrega odzivnega časa. Priporočen je vsaj procesor i686 generacije z delovno frekvenco 800 MHz.

### Pomnilnik

Vsaj 512 MB pomnilnika (priporočeno 1 GB)

### CD-ROM

LinuxDefender se zaganja s CDja, zato potrebujete CD-Rom in BIOS, ki ima opcijo zagon sistema s CD-ROMa.

### Internetna povezava

Čeprav je BitDefender Rescue CD sposoben delovati brez internetne povezave, bo proces posodabljanja potreboval aktivno http-povezavo, celo čez nekatere

proxy strežnike. Zato je torej internetna povezava za posodobljeno skeniranje sistema NUJNA.

### **Grafična resolucija**

Standardne SVGA-kompatibilne grafične kartice.

## **11.2. Vključena programska oprema**

BitDefenderjev reševalni Cd vsebuje naslednje programske pakete.

### **Xedit**

To je urejevalnik tekstovnih datotek.

### **Vim**

To je močno orodje za urejanje besedil, ki vključuje označevanje sintaks, GUI in mnogo več. Za več informacij se prosim obrnite na [Domača stran Vim](#).

### **Xcalc**

To je kalkulator.

### **RoxFiler**

Roxfiler je hitro in močno orodje za urejanje grafičnih datotek.

Za več informacij se obrnite na [Domača stran RoxFiler](#).

### **MidnightCommander**

GNU Midnight Commander (mc) je orodje za urejanje datotek v tekstovnem načinu.

Za več informacij se obrnite na [Domača stran MC](#).

### **Pstree**

Pstree prikaže delujoče procese.

### **Top**

Top prikaže Linuxova opravila.

### **Xkill**

Xkill konča kliente po njegovih X virih.

### **Partition Image**

Slika particije pomaga pri shranjevanju particije v sistemskih datotekah EXT2, Reiserfs, NTFS, HPFS, FAT16, in FAT32 na sliko datoteke. Ta program je uporaben za izdelavo varnostnih kopij.

Za več informacij se obrnite na [Domača stran Partimage](#) .

### **GtkRecover**

GtkRecover je GTK različica vmesnika programske obnovitve. Pomaga vam pri obnavljanju datotek.

Za več informacij se obrnite na [Domača stran GtkRecover](#) .

### **ChkRootKit**

ChkRootKit je orodje, ki vam pomaga pri skeniranju za rootkiti.

Za več informacij se obrnite na [Domača stran ChkRootKit](#).

### **Nessus Network Scanner**

Nessus je oddaljen varnostni skener za Linux, Solaris, FreeBSD, in Mac OS X.

Za več informacij se obrnite na [Domača stran Nessus](#).

### **lprtraf**

lprtraf je programski IP mrežni nadzornik.

Za več informacij se obrnite na [Domača stran lprtraf](#).

### **lftop**

lftop prikaže porabo pasovne širine na vmesniku.

Za več informacij se obrnite na [Domača stran lftop](#).

### **MTR**

MTR je mrežno diagnostično orodje.

Za več informacij se obrnite na [Domača stran MTR](#) .

### **PPPStatus**

PPPStatus prikazuje statistiko o prihajajočem in odhajajočem TCP/IP prometu.

Za več informacij se obrnite na [Domača stran PPPStatus](#).

### **Wavemon**

Wavemon je program za spremljanje brezžičnih mrežnih naprav.

Za več informacij se obrnite na [Domača stran Wavemon](#) .

### **USBView**

USBView prikaže informacije o USB napravah.

Za več informacij se obrnite na [Domača stran USBView](#).

### **Pppconfig**

Pppconfig samodejno nastavi klicno ppp povezavo.

### **DSL/PPPoE**

DSL/PPPoE nastavi PPPoE (ADSL) povezavo.

### **I810rotate**

I810rotate zamenja video izhod na strojni opremi i810, z uporabo i810switch(1).

Za več informacij se obrnite na [Domača stran I810rotate](#) .

### **Mutt**

Mutt je močen MIME poštni klient osnovan na tekstu.

Za več informacij se obrnite na [Domača stran Mutt](#).

### **Mozilla Firefox**

Mozilla Firefox je dobro poznan spletni brskalnik

Za več informacij se obrnite na [Domača stran Mozilla Firefox](#).

### **Elinks**

Elinks je tekstovni spletni brskalnik.

Za več informacij se obrnite na [Domača stran Elinks](#).

## 12. BitDefenderjev reševalni CD Pomoč

To poglavje vsebuje informacije v zvezi s poganjanjem in ustavljanjem BitDefender reševalnega cdja, skeniranjem računalnika, reševanjem podatkov iz okuženega računalnika na odstranljivo napravo. Z uporabo tega programov, ki so na reševalnem cdju, lahko izvajate mnoga opravila, ki jih tukaj niti ne omenjamo.

### 12.1. Zaženi BitDefender reševalni cd.

Za zagon CDja, nastavite BIOS, da se bo sistem zagnal s CD-ROMa, vstavite Cd v pogon in ponovno zaženite računalnik. Prepričajte se, da se vaš sistem lahko zažene s CD-ROMa.

Počakajte, da se na zaslonu pokaže slika z zagonom in sledite navodilom za zagon LinuxDefenderja.



#### Zagonsko pozdravno okno

Posodobitev virusnih definicij se izvede samodejno vsakič, ko zaženete sistem z BitDefender reševalnim CDjem.

Ko se zagonski proces konča, boste zagledali namizje. Lahko začnete z uporabo LinuxDefenderja.



Namizje

## 12.2. Zaustavitev BitDefender reševalnega cdja.

Za pravilno zaustavitev Linuxdefenderja, je priporočeno da odklopite vse vklopljene particije, ki ste jih ustvarili, z uporabo **izvrži** ukaza iz menija, ki se odpre z desnim klikom na ikono diska na namizju in izberite **izvrži**. Nato lahko sistem varno zaustavite z izbiro **Izklopi** ukaza Iz LinuxDefender menija (odprete ga z desnim klikom miške), ali z izbiro **Ustavi** ukaza v terminalu.



Izberite »IZHOD«

Ko je Linuxdefender uspešno zaprl vse programe se bo na dnu prikazalo sporočilo, da Odstranite CD in pritisnite ENTER. Za ponovni zagon sistema z vašim operacijskim sistemom, odstranite CD in ponovno prižgite računalnik.

```

X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
(s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend)
(aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
(d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].

```

Počakaj na to sporočilo ob ugašanju

## 12.3. Kako izvedem proivirusno skeniranje?

Ob koncu boot procesa se pojavi čaropnik, ki vam omogoči popolno skeniranje sistema. Kliknite gumb **Začni**



### Opomba

Če resolucija vašega ekrana ni dovolj velika, boste vprašani za dovoljenje za skeniranje v besedilnem načinu.

Sledite trem korakom vodenege postopka za zaključitev postopka skeniranja.

1. Vidite lahko stanje skeniranja in statistiko (hitrost skeniranja, preostali čas, število skeniranih / okuženih/ sumljivih/ skritih predmetov in ostalo).



### Opomba

Proces bo lahko trajal kar nekaj minut, odvisno od obsega skeniranja.

2. Razvidno je število težav, ki vplivajo na vaš sistem.

Težave so prikazane v skupinah. Kliknite kvadrat s "+" za odprtje skupine in kvadrat z "-", da zaprete skupino.

Izberate lahko med dejanji, ki vplivajo na vse skupine težav ali pa izberete posamezno dejanje za vsako težavo.

3. Tu lahko vidite povzetek rezultatov.

Če želite skenirati samo določen direktorij, naredite sledeče:

Med raziskovanjem vaših trdih diskov, z desno tipko kliknite na datoteko, ali mapo in izberite **Pošlji** in nato izberite **BitDefender skener**.

Ali vpišite ukaz v Terminal. **BitDefenderjev proivirusni skener** bo uporabil izbrano mapo kot privzeto pot za skeniranje.

```
# bdscan /path/to/scan/
```

## 12.4. Kako posodobim BitDefender preko proxy?

Če uporabljate proxy strežnik, morate spremeniti določene nastavitve, z anemoteno posodabljanje.

Za posodabljanje preko proxy strežnika sledite korakom:

1. Desnokliknite Namizje. Pojavil se bo seznam BitDefender obnovitveni CD.
2. Izberite **Terminal (kot root)**.
3. Vnesite ukaz: **cd /ramdisk/BitDefender-scanner/etc**.
4. Vnesite ukaz **mcedit bdscan.conf** za urejanje te datoteke z uporabo GNU Midnight Commander (mc).
5. #HttpProxy = (izbrišiteznak # ) in navedite domeno, uporabniško ime, geslo in vrata proxy serverja. Naprimer:  

```
HttpProxy = myuser:mypassword@proxy.company.com:8080
```
6. Pritisnite **F2** za shranjevanje trenutne datoteke, potrdite shranjevanje in pritisnite **F10** za zaprtje.
7. Vnesite ukaz: **bdscan update**.

## 12.5. Kako dostopam do svojih podatkov?

Predpostavimo, da iz nenznanih vzrokov ne morete prižgati vašega računalnika, obenem pa nujno potrebujete podatke, ki so na njem. Na vrsti je BitDefenderjev reševalni cd.

Da shranite vaše podatke na prenosno napravo sledite naslednjim korakom:

1. Vstavite BitDefender reševalni cd v cd enoto, vstavite prenosno napravo in ponovno zaženite računalnik.

2. Počakajte, da BitDefender reševalni cd izvede zagon. Pojavi se naslednje okno:



Namizno okno

3. Dvokliknite particijo, na kateri so podatki, ki jih želite rešiti (e.g. [sda3]).

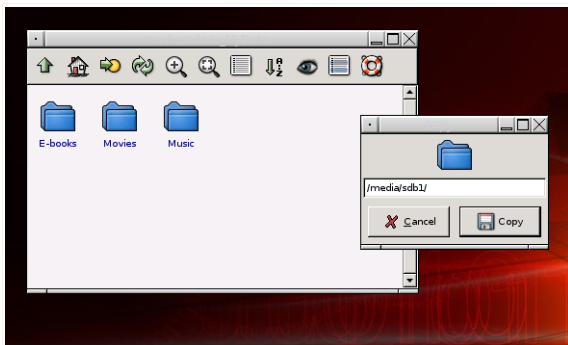


#### Opomba

Ob delu z BitDefender reševalnim cdjem boste imeli opravka z Linux poimenovanjem particij. Tako bo [sda1] verjetno pripadal (C:) Windows-type partition, [sda3] za (F:) in [sdb1] na prenosni napravi.

4. Prebrskajte vaše mape in odprite željen direktorij. Na primer MyData ki vsebuje poddirektorije Movies, Music in E-books

5. Desno-kliknite željen direktorij in izberite **Kopiraj**. Pojavi se naslednje okno.



### Shranjevanje podatkov

6. Vpišite `/media/sdb1/` v pripadajoč besedilni kvadratik in kliknite **Kopiraj**.

# Pomoč

## 13. Podpora

Kot resen ponudnik BitDefender stremi k popolni, hitri in natančni tehnični podpori za svoje izdelke. Center tehnične pomoči (ki ga lahko kontaktirate na spodnjem naslovu) premore vse informacije o novih virusih ter pozna odgovore na najpogosteje zastavljena vprašanja uporabnikov, tako da vam v primeru težav lahko hitro priskoči na pomoč.

Pri BitDefender-ju so vedno stremeli k cilju, da svojim strankam ponudijo najnaprednejše izdelke po poštenih cenah, s katerimi jim bodo omogočili prihranke časa in denarja. Še več, menijo, da je za dobro poslovanje nujna komunikacija med stranko in tehnično podporo.

V primeru težav se obrnite na našo tehnično pomoč na [podpora@parametica.si](mailto:podpora@parametica.si). Za hitrejši odziv vam priporočamo, da v elektronsko pošto dodate čimveč podrobnosti o programu BitDefender, vašem sistemu in karseda natančno opišete težavo.

### 13.1. BitDefender baza znanja

BitDefender baza znanja je spletna zbirka informacij o programih BitDefender. Hrani lahko dostopne informacije o stanju z BitDefender programsko opremo, tehnično podporo, dokumentacijo ter aktivnosti BitDefender razvojne ekipe. Tu najdete tudi več splošnih člankov glede virusnih nevarnosti in preventive, upravljanja s programom BitDefender ter druge podrobne razlage.

BitDefender baza znanja je javno dostopna. Ponuja bogato vsebino in informacije, po katerih klicatelji na BitDefender tehnično podporo najpogosteje povprašujejo.

BitDefender bazo znanja najdete na spletnem naslovu <http://kb.bitdefender.com>.

### 13.2. Kako do pomoči

#### 13.2.1. Pojdite na mrežno samopostrežno

Imate vprašanje? Naši varnostni strokovnjaki so vam na voljo 24/7 preko telefona, e-pošte ali brezplačne klepetalnice.

Sledite povezavam spodaj:

#### Angleško

<http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/>

## **Nemško**

<http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/>

## **Francosko**

<http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/>

## **Romunija**

<http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/>

## **Špansko**

<http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/>

### **13.2.2. Odpri kupon za podporo**

Če želite odpreti kupon za podporo in prejeti pomoč preko e-pošte, sledite enemu izmed teh korakov:

<http://www.parametica.si>

<http://www.parametica.si>

<http://www.parametica.si>

<http://www.parametica.si>

<http://www.parametica.si>

## **13.3. Kontaktne informacije**

Učinkovita komunikacija je ključ do uspeha. V zadnjih 10-ih letih je podjetje BITDEFENDER zgradilo uspešno sodelovanje s številnimi partnerji širom sveta. Tako lahko brez skrbi na nas naslovite sleherno vprašanje.

### **13.3.1. Spletni naslovi**

Prodaja: [prodaja@parametica.si](mailto:prodaja@parametica.si).

Tehnična podpora: [podpora@parametica.si](mailto:podpora@parametica.si)

Dokumentacija: [documentation@bitdefender.com](mailto:documentation@bitdefender.com)

Partnerji: [partners@bitdefender.com](mailto:partners@bitdefender.com)

Marketing: [prodaja@parametica.si](mailto:prodaja@parametica.si)

Odnosi z javnostmi: [info@parametica.si](mailto:info@parametica.si)  
Zaposlitvene priložnosti: [jobs@bitdefender.com](mailto:jobs@bitdefender.com)  
Poročila o virusih: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)  
Poročila o neželenih vsebinah: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)  
Poročila o zlorabah: [abuse@bitdefender.com](mailto:abuse@bitdefender.com)  
Spletna stran: <http://www.parametica.si>  
FTP strežnik: <ftp://ftp.bitdefender.com/pub>  
Lokalni distributerji: [http://www.bitdefender.com/partner\\_list](http://www.bitdefender.com/partner_list)  
BitDefender baza znanja: <http://kb.bitdefender.com>

### 13.3.2. Franšizne pisarne

BitDefender ima zastopstva v večih državah po svetu, kjer vam lahko predstavniki podjetja pomagajo pri iskanju odgovorov na vprašanja o splošnih ter komercialnih zadevah. Naslovi so navedeni spodaj.

#### U.S.A

**BitDefender, LLC**  
Dunajska 106  
1000 Ljubljana  
<http://www.parametica.si>  
Tehnična podpora:

- E-pošta: [podpora@parametica.si](mailto:podpora@parametica.si)
- Telefon:
  - 01 565 79 17
  - 01 565 79 18 (faks)

Podpora uporabnikom:

- E-pošta: [podpora@parametica.si](mailto:podpora@parametica.si)
- Telefon:
  - 01 565 79 17
  - 01 565 79 18 (faks)

#### Nemčija

**BitDefender GmbH**  
Predstavništvo za zahodno evropo

Karlsdorferstrasse 56  
88069 Tettngang  
Nemčija  
Telefon: 003861 565 79 17  
Fax: 07542/94 44 99  
E-pošta: [info@bitdefender.com](mailto:info@bitdefender.com)  
Prodaja: [prodaja@parametica.si](mailto:prodaja@parametica.si)  
<http://www.parametica.si>  
Tehnična podpora: [support@bitdefender.com](mailto:support@bitdefender.com)

## **Velika Britanija in Irska**

One Victoria Square  
Birmingham  
B1 1BD  
Telefon: +34 932189615  
Fax: +40 21 2330763  
E-pošta: [info@bitdefender.com](mailto:info@bitdefender.com)  
Prodaja: [prodaja@parametica.si](mailto:prodaja@parametica.si)  
Splet: <http://www.bitdefender.co.uk>  
Tehnična podpora: [podpora@parametica.si](mailto:podpora@parametica.si)

## **Španija**

**Constelación Negocial, S.L**  
C/ Balmes 195, 2ª planta, 08006  
Barcelona  
Tehnična podpora: [soporte@bitdefender-es.com](mailto:soporte@bitdefender-es.com)  
Prodaja: [comercial@bitdefender-es.com](mailto:comercial@bitdefender-es.com)  
Tel: +34 932189615  
Fax: +34 932179128  
Spletna stran produkta: <http://www.bitdefender-es.com>

## **Romania**

**BITDEFENDER**  
West Gate Park, Building H2, 24 Preciziei Street Sector 6  
Bucharest  
Tehnična podpora: [podpora@parametica.si](mailto:podpora@parametica.si)  
Prodaja: [prodaja@parametica.si](mailto:prodaja@parametica.si)  
Tel: +4021 300 12 55, 54

Fax: +4021 2641799

Spletna stran: <http://www.parametica.si>

## Slovar izrazov

### ActiveX

ActiveX tehnologija vsebuje komponente, ki spletnim brskalnikom kot je npr. Microsoft Internet Explorer omogočijo prikaz spletnih strani, da se le-te obnašajo kot računalniški programi in ne kot statična okna. S pomočjo ActiveX komponent uporabniki pritiskajo gumb in izvajajo razne kode na spletnih straneh. ActiveX komponente so pogosto napisane v programu Visual Basic.

Active X komponente so znane po svojih pomanjkljivih varnostnih mehanizmih, zato strokovnjaki njihovo uporabo na internetu odsvetujejo.

### Reklamni programi

Adware/reklamni programi so pogosto del druge aplikacije, ki je na voljo brezplačno, vse dokler se uporabnik strinja s prikazom reklam. Pogosto se reklamni programi namestijo po tem, ko se je uporabnik strinjal z licenčno pogodbo, zato ne kršijo pravic.

Kljub temu znajo biti izskočne reklame zelo nadležne in v nekaterih primerih tudi okrnijo delovanje sistema. Nekatere aplikacije tudi zbirajo podatke o uporabniku in njegovih navadah, česar pa se uporabniki, ki niso temeljito prebrali licenčne pogodbe ob namestitvi sploh ne zavedajo.

### Arhiv

Medij ali mapa, ki vsebuje shranjene datoteke.

Datoteka, ki vsebuje eno ali več datotek, v kompresiranem formatu.

### Stranska vrata

Gre za luknjo v sistem, ki so jo načrtno pustili načrtovalci ali vzdrževalci sistema. Takšne luknje niso nujno zlonamerne, saj jih imajo tudi nekateri operacijski sistemi, ki so že opremljeni s privilegiranimi računi za tehnično osebje ali vzdrževanje s strani programerjev.

### Zagonski sektor

Del razdelka na disku z informacijami o datotečnem sistemu diska in kratek program v strojnem jeziku, ki naloži operacijski sistem.

### Virus na zagonskem sektorju

Virusi na zagonskem sektorju diskete ali trdih diskov so bili med prvimi oblikami virusov. Širijo se s spremembami zagonskega sektorja, dela diskete ali trdega diska, v katerem je zapisan program, ki omogoča zagon računalnika in operacijskega sistema. Ko prižgemo računalnik, strojna oprema poišče program za zagon operacijskega sistema. Ta program se običajno nahaja na trdem disku,

seveda pa ga je moč najti tudi na disketah ter cedejih. Program se požene in naloži v pomnilnik računalnika. Virusi na zagonskem sektorju spremenijo program za zagon računalnika s svojo modificirano različico. Ob naslednjem zagonu sistema se uporabi okuženi zagonski sektor ter aktivira virus.

### **Brskalnik**

Krajše za spletni brskalnik. Je program za pregledovanje dokumentov HTML. Navadno jih prebere iz interneta. Z uporabo dodatnih programov skrbi za ustrezno predstavitev zvočnega in slikovnega gradiva, vstavljenega v dokument, pa tudi za sledenje povezavam do drugih dokumentov.

### **Ukazna vrstica**

Mesto na zaslonu, na katero uporabnik vnaša besedilne ukaze za upravljanje programa ali operacijskega sistema z znakovnim uporabniškim vmesnikom.

### **Piškotek**

Piškotek je datoteka, ki jo spletnemu brskalniku pošlje spletni strežnik. Brskalnik shrani sporočilo v besedilno datoteko. Sporočilo se nato pošlje nazaj strežniku, vsakokrat ko brskalnik zahteva stran s strežnika. Poglavitni namen piškotkov je identificiranje uporabnikov in priprava njim prilagojenih spletnih strani.

### **Diskovni pogon**

Gre za napravo, ki bere in zapisuje podatke.

Trdi disk bere in zapisuje podatke.

Disketni pogon služi branju in zapisovanju podatkov z/na diskete(o).

Diskovni pogoni so lahko vgradni (notranji) ali zunanji (ločena naprava, povezana z računalnikom).

### **Dolvleka**

Prenos podatkov iz osrednjega računalnika v terminal ali iz strežnika v odjemalec.

Gre za izmenjavo podatkov med dvema napravama, bodisi znotraj računalniškega sistema, bodisi med različnimi sistemi v omrežju.

### **E-pošta**

Elektronska pošta, sporočilo v elektronski obliki.

### **Dogodki**

Gre za spremembe v stanju operacijskega sistema, programa ali samo enega predmeta v programu.

### **Napačna diagnoza**

Napaka, ki se pojavi, povzroči, da protivirusni program označi brezhibno datoteko kot okuženo.

### **Razširitev imena datoteke**

Del imena datoteke, ki sledi njenemu zaključku. Ponavadi označuje vrsto podatkov, ki so shranjeni v datoteki.

Veliko operacijskih sistemov (primer Unix, VMS, MS-DOS) uporablja razširjena imena datotek. Oznake so ponavadi dolge med enim in tremi znaki. Primer: "c" pomeni izvorno kodo C, "ps" PostScript, "txt" pa označuje poljuben tekst.

### **Hevristično iskanje**

Iskanje podatkov na temelju zaporedja preskusov, ki dajejo približne rezultate. Če se zaporedje rezultatov dovolj hitro bliža končni vrednosti rezultata, je iskanje uspešno. Občasno so možne tudi "napačne diagnoze" sumljivih kod.

### **IP**

Kratica za Internet Protocol (internetni protokol). To je protokol za prenos podatkovnih paketov po internetu. IP nima dobrih mehanizmov za odpravljanje napak pri prenosu, zato je danes najpogosteje v rabi pri povezavi s protokolom TCP kot »polni« internetni protokol TCP/IP.

### **Javanski programček**

Gre za programček, ki je narejen zgolj za izvajanje na spletnih straneh. Ko obiščemo spletno stran, brskalnik s strežnika naloži ta program in ga zažene na uporabnikovem računalniku.

Zaradi strogih varnostnih politik pa ti programi lahko le tečejo na uporabnikovem računalniku, ne morejo pa brati ali zapisovati podatkov nanj. Dodatno so ti programi omejeni na branje in zapisovanje podatkov zgolj na domeno iz katere izhajajo.

### **Makro virus**

Gre za vrsto računalniškega virusa, ki se skriva v dokumentih z makro funkcijo (najbolj pogosto v Microsoft Word ter Excel dokumentih).

Ti programi ob odprtju dokumenta poženejo tudi morebiten makro.

### **Odjemalec elektronske pošte**

Odjemalec elektronske pošte je program, ki omogoča pošiljanje in sprejemanje elektronskih sporočil.

### **Pomnilnik**

Pomnilnik predstavlja sredstvo hranjenja za računalniške podatke. Navadno označuje elektronsko hranilno napravo brez gibljivih mehanskih delov, sestavljeno iz polprevodniških čipov (RAM, ROM, EPROM...). Glavni pomnilnik v računalniku ne more hraniti podatkov, ko izklopimo napajanje, zato moramo prej podatke iz pomnilnika shraniti v druga sredstva hranjenja.

### **Klasično skeniranje**

Metoda odkrivanja virusov s pomočjo virusnih definicij. Program, ki v skupku kode prepozna virusni vzorec, javi okužbo. Prednost te metode je, da ne pozna lažnih alarmov.

### **Stisnjeni programi**

Gre za datoteko v kompresiranem formatu. Številni operacijski sistemi in programi vsebujejo možnost kompresiranja datotek, tako da le-te zasedejo manj prostora. Primer: Imate tekstovno datoteko, ki vsebuje deset zaporednih presledkov. Navadno to zahteva deset bitov prostora.

Program, ki kompresira datoteke, bo presledke nadomestil s posebnimi oznakami. Tako bo deset presledkov zahtevalo le dva bita. To je le ena izmed kompresirnih tehnik - obstaja pa jih veliko.

### **Pot**

Splošen izraz za datotečno pot, lokacijo, kjer se datoteka v sistemu nahaja.

Katerakoli smer med katerimakoli vozliščema v omrežju. Pot lahko pelje čez niz vozlišč in obsega več vej.

### **Phishing**

Phising ali prevarantska elektronska pošta je izraz za sporočila, ki se uporabnikom predstavljajo kot legalne organizacije in od njega zahtevajo osebne podatke, s čimer se jim omogoči kraja podatkov/identitete. Takšna sporočila pogosto povabijo uporabnika na spletno stran, kjer ga pozovejo k posodobitvi osebnih podatkov kot so gesla, št. kreditne kartice, bančnega računa itd. Spletna stran je seveda lažna in narejena z namenom kraje informacij/podatkov.

### **Polimorfni virus**

Polimorfni virus mutira (spreminja svojo obliko) z vsako novo okužbo. Takšne viruse je zato zelo težko odkriti.

### **Vrata**

Točka za povezovanje, na katero povežemo naprave (modeme, tiskalnice, miške, tipkovnice...), ki posredujejo podatke v računalnik in iz njega.

Vrata TCP/IP predstavljajo logični kanal, ki ga uporablja protokol TCP/IP za razločevanje med različnimi hkratnimi dostopi v gostiteljski računalnik oziroma sistem. Vrata 80 so tako namenjena internetnemu, torej HTTP prometu.

### **Poročilo**

Izpis podatkov iz zbirke podatkov ali namenskega programa v vnaprej določeni obliki dokumenta, mnogokrat v obliki tabel. Poročilo si običajno ogledamo na zaslonu ter izpišemo s tiskalnikom. BitDifender poroča o vseh virusnih aktivnostih.

### **Rootkit**

Rootkit je del programskih orodij, ki ponuja administratorski dostop do sistema. Izraz je bil prvič uporabljen v UNIXovem operacijskem sistemu in se je nanašal na orodja, ki so omogočale vsiljivcem administratorske pravice in jim omogočal nevidno delovanje v sistemu.

Glavna naloga rootkitov je skrivanje procesov, datotek, prijav in povezav. Prestrezajo lahko tudi podatke iz terminalov, mrežnih povezav,...,če vsebujejo primerno programsko opremo.

Rootkiti so v osnovi zlonamerni. Sistem in celo nekatere aplikacije skrijejo kritične datoteke s pomočjo rootkitov, vendar so najpogosteje uporabljeni za skrivanje zlonamernih programov ali prikritje prisotnosti vsiljivcev v vašem sistemu. V kombinaciji z zlonamerno programsko opremo rootkiti predstavljajo veliko grožnjo integriteti in varnosti sistema. Spremljajo lahko promet, ustvarjajo skrite prehode v sistem, spreminjajo datoteke in se ostanejo nezaznani.

### **Skripta**

Vrsta programa, ki ga sestavlja množica ukazov ali makrov drugemu programu.

### **Neželjena pošta**

Odvečna elektronska pošta ali odvečna novičarska vsebina. Splošen izraz za vsakršno neželeno/neahtevano pošto.

### **Vohunski programi**

Spyware/vohunska programska oprema uporablja internetno povezavo brez uporabnikove vednosti, najpogosteje za reklamne namene. Vohunski programi so največkrat skrivoma priloženi brezplačnim programom, ki so na voljo za dolvleko s spleta; kljub temu pa velja omeniti, da večina plačljivih in zastonjskih programov ne vsebuje vohunskih dodatkov. Ko so enkrat nameščeni, vohunski programi merijo vse uporabnikove aktivnosti na računalniku in pošiljajo tovrstne informacije preko interneta avtorjem programov. Vohunski programi lahko zbirajo tudi podatke iz elektronske pošte, gesla in številke kreditnih kartic ter bančnih računov.

Vohunski programi so podobni trojanskim konjem, kjer uporabniki namestijo program z neželenimi dodatki. Zelo pogosto so vohunski programi pripeti datotekam, ki si jih uporabniki izmenjujejo preko spleta v t.i. P2P omrežjih za izmenjavo datotek.

Poleg etičnih in zasebnih vidikov pa vohunski programi škodijo uporabniku z odžiranjem sistemskih virov in spletne povezave, ki jo uporabljajo za pošiljanje informacij. Ker vohunski programi uporabljajo pomnilnik in druge sistemske vire, lahko njihovo delovanje vodi do sesutja sistema ali nestabilnega delovanja.

### **Zagonski programi**

Programi ali datoteke, ki se nahajajo v mapi Zagon (ang. Startup), se ob zagonu računalniškega sistema tudi poženejo. Veliko virusov svojo škodljivo kodo vstavi v to mapo.

### **Sistemski kotichek**

Sistemski kotichek je bil predstavljen v Windows 95 in se nahaja v orodni vrstici (običajno na dnu zaslona poleg ure). Premore majhne ikone za hiter dostop do sistemskih funkcij kot so faksi, tiskalniki, modemi, pogoni in drugo. Dvokliknite ali desno kliknite na ikono za pregled in dostop do podrobnosti ter nastavitev.

### **TCP/IP**

Kratica za Transmission Control Protocol/Internet Protocol. Predstavlja dejanski standard za protokol interneta (za krmiljenje prenosa podatkov po internetu).

### **Trojanski konji**

Trojanski konji so na videz neškodljivi programi, ki potem, ko dosežejo računalnik, izvedejo vrsto akcij, ne da bi uporabnik to opazil. Programi namreč izvajajo ukaze, ki niso navedeni v njihovih specifikacijah. Uporabnik tako požene domnevno običajen program, le-ta pa skrivno izvaja druge, največkrat škodljive operacije.

Izraz izhaja iz Homerjeve Iliade, v kateri so Grki svojim nasprotnikom, Trojancem, podarili lesenega konja v znak sprave. Ko so Trojanci konja pripeljali za svoje obzidje, so se iz njegovega trebuha pretihotapili Grški vojaki in odprli mestna vrata, s čimer so omogočili Grški vojski, da je zavzela Trojo.

### **Posodobitev**

Postopek za spreminjanje programske opreme zato, da bi le-ta pridobila nove zmožnosti, da bi odpravili znane napake v njenem delovanju in zagotovili učinkovitejše delo z njo.

BitDefender premore lasten posodobitveni modul, ki vam omogoča ročno preverjanje za posodobitvami, lahko pa se odločite za samodejno posodabljanje izdelka.

### **Virus**

Računalniški virus je računalniški program, ki ustvarja lastne kopije in se širi po drugih računalnikih in omrežjih, običajno brez uporabnikove vednosti. Virusi imajo lahko tudi škodljive stranske učinke. Slednji se pojavljajo v različnih oblikah – od nadležnih sporočil do brisanja vseh podatkov na računalniku. Virusi veljajo za samorazmnoževalne programe, ki lahko okužijo in uničujejo druge programe. Zanje je značilno, da se ob vsaki okužbi množijo. Danes se največ računalniških virusov širi preko elektronske pošte (v obliki priponk elektronskih sporočil) in

neposredno preko interneta. Slednja vrsta virusov ne potrebuje gostitelja, da bi se razširila iz enega na drug računalnik.

### **Virusne definicije**

So vzroci virusnih kod, ki jih protivirusni program uporablja pri svojem delu odkrivanja in odstranjevanja računalniških virusov.

### **Črv**

Računalniški črvi so podobni računalniškim virusom, od slednjih se razlikujejo le po tem, da za svoje širjenje ne potrebujejo prenašalca (kot je na primer datoteka, zagonski sektor diska ipd.). Črvi namreč naredijo svojo kopijo in za širjenje uporabljajo komunikacijsko povezavo med dvema računalnikoma, najpogosteje elektronsko pošto ter internet. Črv zaganja druge programe, ne spreminja pa datotek ali sektorjev na diskih. Za črve je značilno, da običajno ne napadajo drugih programov, vendar pa lahko zasedejo veliko količino računalniških virov in tako ohromijo računalniški sistem.