

bitdefender **ANTIVIRUS v10**



Navodila za uporabo



Protivirusna zaščita

Protivohunska zaščita

BitDefender Antivirus v10

Navodila za uporabo

BitDefender

Izdano 2007.02.13

Version 10.2

Pravna zaščita© 2007 SOFTWIN

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 škodo 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

Licenca in garancija	ix
Uvod	xiii
1. Dogovori, uporabljeni v knjižici	xiii
1.1. Tipografski dogovori	xiii
1.2. Opozorila	xiv
2. Struktura knjižice	xiv
3. Komentarji	xv
O BitDefenderju	1
1. Kaj je BitDefender?	3
1.1. Zakaj BitDefender?	3
1.2. O SOFTWINu	4
Namestitev	7
2. BitDefender Antivirus v10 Namestitev	9
2.1. Sistemske zahteve	9
2.2. Namestitveni koraki	9
2.3. Namestitveni čarovnik	12
2.3.1. Korak 1/8 - BitDefender namestitveni čarovnik	13
2.3.2. Korak 2/8 - Registracija BitDefender Antivirus v10	13
2.3.3. Korak 3/8 - Kreiranje BitDefender računa	14
2.3.4. Korak 4/8 - Vnos podatkov o računu	15
2.3.5. Korak 5/8 - Več o RČPV	16
2.3.6. Korak 6/8 - Izbira opravil	16
2.3.7. Korak 7/8 - Čakanje na dokončanje opravil	17
2.3.8. Korak 8/8 - Povzetek	18
2.4. Nadgradnja	18
2.5. Odstranjevanje, popravilo ali spreminjanje BitDefenderja	19
Opis in lastnosti	21
3. BitDefender Antivirus v10	23
3.1. Protivirusna zaščita	23
3.2. Protivohunska zaščita	24
3.3. Druge lastnosti	24
4. BitDefenderjevi moduli	27
4.1. Splošno modul	27
4.2. Modul Antivirus	27
4.3. Modul Antispyware	27

4.4. Posodobitveni modul	28
Upravljalna konzola	29
5. Pregled	31
5.1. Sistemski kotiček	32
5.2. Vrstica aktivnosti skeniranja	33
6. Splošno modul	35
6.1. Osrednja administracija	35
6.1.1. Hitra opravila	36
6.1.2. Stopnja varnosti	36
6.1.3. Registracija	37
6.2. Nastavitve glavnega okna	37
6.2.1. Nastavitve poročil	38
6.2.2. Nastavitve poročil	39
6.2.3. Nastavitve vmesnika	40
6.2.4. Upravljalne nastavitve	40
6.3. Dogodki	40
6.4. Registracija vaše kopije	42
6.4.1. Čarovnik za registracijo	42
6.5. O programu	46
7. Modul Antivirus	49
7.1. Skeniranje ob dostopu	49
7.1.1. Nivoji zaščite	50
7.2. Skeniranje na zahtevo	53
7.2.1. Opravila skeniranja	54
7.2.2. Nastavitve opravi skeniranja	55
7.2.3. Hitri seznam	66
7.2.4. Skeniranje na zahtevo	67
7.2.5. Skeniranje proti rootkitom	71
7.3. Karantena	71
8. Modul Antispyware	75
8.1. Status protivohunske zaščite	75
8.1.1. Nivoji zaščite	77
8.2. Napredne nastavitve-nadzor zasebnosti	77
8.2.1. Čarovnik za nastavitve	78
8.3. Napredne nastavitve-Nadzor registra	82
8.4. Napredne nastavitve-Nadzor klicanja	83
8.4.1. Čarovnik za nastavitve	85
8.5. Napredne nastavitve-Nadzor piškotkov	87
8.5.1. Čarovnik za nastavitve	88
8.6. Napredne nastavitve-Nastavitve skripte	90
8.6.1. Čarovnik za nastavitve	91
8.7. Sistemske informacije	92



9. Posodobitveni modul	95
9.1. Samodejno posodabljanje	95
9.2. Ročno posodabljanje	96
9.2.1. Ročno posodabljanje z weekly.exe	97
9.2.2. Ročno posodabljanje z zip arhivi	97
9.3. Posodobitvene nastavitve	99
9.3.1. Nastavitve lokacije posodobitev	99
9.3.2. Možnosti samodejnega posodabljanja	100
9.3.3. Nastavitve ročnega posodabljanja	101
9.3.4. Napredne nastavitve	101
Uporaba v praksi	103
10. Uporaba v praksi	105
10.1. Kako zaščititi računalnik pred škodljivimi grožnjami	105
10.2. Kako nastaviti opravila skeniranja	106
BitDefenderjev reševalni CD	107
11. Pregled	109
11.1. Kaj je KNOPPIX?	109
11.2. Sistemske zahteve	109
11.3. Vključena programska oprema	110
11.4. BitDefender Linux Security solutions	110
11.4.1. BitDefenderjev SMTP Proxy	110
11.4.2. BitDefenderjev oddaljeni administrator	111
11.4.3. BitDefenderjeva različica za Linux	111
12. LinuxDefenderjev kako	113
12.1. Ustavitev in zagon	113
12.1.1. Zagon LinuxDefenderja	113
12.1.2. Ustavitev LinuxDefenderja	114
12.2. Nastavitev Internetne povezave	115
12.3. BitDefenderjevo posodabljanje	116
12.4. Skeniranje za virusi	116
12.4.1. Kako dostopam do svojih podatkov?	116
12.4.2. Kako izvedem proivirusno skeniranje?	117
12.5. Naredite takojšnji e-poštni filter	117
12.5.1. Zahteve	118
12.5.2. E-poštna filtracijska rešitev	118
12.6. Izvedite glavni nadzor omrežja	119
12.6.1. Iskanje rootkit-ov	119
12.6.2. Nessus - omrežni skener	119
12.7. Preverite stanje delovnega spomina	120
Pomoč	121

13. Podpora	123
13.1. Tehnična podpora	123
13.2. Pomoč na spletu	123
13.2.1. BitDefender baza znanja	123
13.3. Kontaktne informacije	123
13.3.1. Spletni naslovi	124
13.3.2. Franšizne pisarne	124
Slovar izrazov	127



Licenca in garancija

V KOLIKOR SE Z NAVEDENIMI POGOJI NE STRINJATE, VAS PROSIMO, DA SI TEGA PROGRAMA NE NALOŽITE. Z IZBIRO MOŽNOSTI "SPREJMEM", "V REDU", "NADALJUJ", "DA" ALI Z NALOŽITVIJO IN KAKRŠNOKOLI UPORABO POTRJUJETE RAZUMEVANJE IN SPREJETJE NAVEDENIH POGOJEV TEGA SPORAZUMA.

Ti pogoji zajemajo BitDefenderjeve rešitve in storitve za domače uporabnike registrirane na vas, vključujoč sorodno dokumentacijo in vse posodobitve in nadgraditve aplikacij dostavljenih v okvirih kupljene licence ter sorodnih sporazumih, kot je določeno v tem dokumentu in vseh njegovih kopijah.

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.

V kolikor se ne strinjate s pogoji sporazuma ne naložite in ne uporabljajte BitDefenderja.

BitDefenderjeva različica za Linux. 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. SOFTWIN vam in zgolj vam na tem mestu dovoli uporabo programske opreme BitDefender.

PROGRAMSKA OPREMA. BitDefender lahko naložite in uporabljate na toliko računalnikih, za kolikor uporabnikov je izdana licenca. Na vsakega licenciranega uporabnika programa lahko naredite eno varnostno kopijo za obnovitvene namene.

LICENCE ZA NAMIZNE UPORABNIKE. Ta licenca zajema BitDefenderjevo programsko opremo, ki jo lahko naložite na en računalnik ter ne omogoča mrežnih storitev. Vsak primarni uporabnik lahko naloži in uporablja to programsko opremo na enem računalniku ter naredi eno varnostno kopijo v obnovitvene namene. Število primarnih uporabnikov je enako številu uporabnikov določenih na licenci.

POGOJI LICENCIRANJA. Licenčno obdobje se prične z dnem namestitve, kopiranja ali drugega načina uporabe programskega paketa BitDefender.

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.

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

RAZEN POSEBEJ OMENJENIH PRIMEROV OMENJENIH V TEM SPORAZUMU, SOFTWIN NE UPOŠTEVA DRUGIH GARANCIJ, KI NAJ BI BILE V POVEZAVI Z IZDELKOM, IZBOLJŠAVE, TRAJNOSTNE ALI ZAČASNE, ALI KATERIKOLI OSTALI MATERIALI (STVARN ALI NESTVARNI) ALI USLUGE IZ NJIHOVE STRANI. SOFTWIN VKLJUČUJE BREZ OMEJITEV, IMPLICIRANE GARANCIJE TRŽNOSTI, USTREZNOST ZA DOLOČENE NAMENE, NASLOV, NEVMEŠAVANJE, TOČNOST DATUMOV, TOČNOST INFORMACIJSKIH VSEBIN, SISTEMSKA INTEGRACIJA IN BREZ KRŠITEV S STRANI TRETJE OSEBE S FILTRIRANJEM, ONEMOGOČANJEM ALI ODSTRANJEVANJEM TAKŠNE PROGRAMSKE OPREME TRETJE OSEBE, VOHUNSKIH PROGRAMOV, PIŠKOTKOV, E-POŠTE, DOKUMENTOV, OGLASOV, PRIPADAJOČE POSTATUTU, ZAKONU, POTEKU POSLOV, NAVAD ALI TRGOVSKE UPORABE.



NAPAKE. Uporabniki, ki programsko opremo BitDefender preizkušajo ter ocenjujejo, nosijo tudi vse tveganje napak v delovanju te programske opreme. V nobenem primeru programska hiša SOFTWIN 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 SPOROČILO ZA UPORABNIKE. 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 sporazum bo obravnavan po zakonih Romunije in po mednarodnih regulativah o avtorskih pravicah. Za vse spore izhajajoče iz te licence so odgovorna sodišča v Romuniji.

Cene, stroški in dajatve za uporabo BitDefenderja se lahko spreminjajo brez predhodnega obvestila.

Neveljavnost odločb tega sporazuma ne izniči veljavnih odločb tega sporazuma.

BitDefender in BitDefenderjev logo sta blagovni znamki podjetja Softwin. Vse ostale znamke uporabljene v tem produktu ali pomožnemu materialu so lastnina njihovih lastnikov.

Licenca bo prenehala v renutku, ko bo kršen katerikoli pogoj pogodbe. Prav tako ne boste upravičeni do vračila kupnine s strani Softwin ali njihovih sodelavcev. Pogoji, ki se navezujejo na zaupnost in restrikcije uporabe, bodo veljale tudi po ukinitvi.

Softwin lahko spremeni te pogoje kadarkoli in ti novi pogoji se bodo avtomatično nanašali na verzije, ki vsebujejo spremenjene pogoje. Če se katerikoli pogoj izkaže za neizvedljivega ne bo vplival na validacijo ostalih izvedljivih pogojev.

V primeru nasprotij ali nestabilnosti med prevedenimi in originalnimi pogoji, bo prevladala angleška različica izdana s strani Softwina.

Kontakt: SOFTWIN Fabrica de Glucoza 5 72322-Sector 2 Bucharest Romania ali preko telefona: 40-21-2330780 ali faksa: 40-21-2330763 ali e-poštnega naslova: <office@bitdefender.com>.



Uvod

Hvala, da ste izbrali **BitDefender Antivirus v10** 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 v10**, podjetja in ekipe, ki ga je pripravila, navodila za namestitev ter konfiguracijo programa. Spoznali boste kako uporabljati **BitDefender Antivirus v10**, 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
<code>sample syntax</code>	Primeri sintaks so natisnjeni z manjšo pisavo.
http://www.bitdefender.com	Spletne povezave kažejo na zunanje lokacije, http ali ftp strežnike.
<code><support@bitdefender.com></code>	E-poštna sporočila/naslivi so vnešena v tekst za hitrejši kontakt.
"Uvod" (p. xiii)	Gre za notranjo povezavo na lokacijo v dokumentu.
filename	Datoteke in direktoriji so natisnjeni z manjšo pisavo.
option	Vse možnosti so natisnjene s krepko 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 je sestavljena iz petih delov, ki vsebujejo naslednje glavne teme: Opis in lastnosti, Namestitvev, Upravljalna konzola, Pomoč ter Uporaba v praksi. Še več, dodan je tudi slovarček z razlago nekaterih tehničnih izrazov.

O BitDefenderju. Kratak uvod v BitDefender. Razloži kaj sta BitDefender in Softwin.

Namestitvev. Navodila vas po korakih vodijo skozi namestitev programa BitDefender na računalnik. Gre za izčrpen opis postopka namestitve programa **BitDefender Antivirus v10**. 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.

Opis in lastnosti. **BitDefender Antivirus v10** poglavje hitrega vodiča obsega naslednje vsebine:

Upravljalna konzola. Opis osnovnih administrativnih ter vzdrževalnih možnosti programa BitDefender. Spoznali boste vse možnosti **BitDefender Antivirus v10**, kako registrirati program, kako preskenirati računalnik za virusi in kako nastaviti posodabljanje programa.

Uporaba v praksi. Za najboljši izkoristek vašega BitDefenderja natančno sledite tem navodilom.



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

Pomoč. Pomoč, če jo boste potrebovali. Vsebuje tudi razdelek z najpogostejšimi vprašanji.

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.



O BitDefenderju



1. Kaj je BitDefender?

BitDefender je vodilni proizvajalec na področju varnostnih rešitev, ki zadovoljujejo varnostne potrebe dandanašnjega računalniškega okolja. Podjetje ponuja enega izmed najučinkovitejših varnostnih programov in postavlja nove standarde varovanja. BitDefender ima preko 41 milijonov uporabnikov v 180ih državah. BitDefender ima poslovalnice v **ZDA**, **VB**, **Nemčija**, **Španija** and **Romunija**.

- Moduli protivirusne zaščite, požarnega zidu, protivohunske zaščite, proti nezaželeni pošti in starševske zaščite za poslovne in domače uporabnike;
- Razpon BitDefenderjevih izdelkov so namenjeni kompleksnim IT strukturam (delovne postaje, datotečni strežniki, poštni strežniki in gateway) v operacijskih sistemih Windows, Linux in FreeBS;
- Svetovna distribucija, izdelki na voljo v 18ih jezikih.
- Preprosta uporaba, čarovnik za nalaganje programa, ki vas vodi skozi proces inštalacije in vas vpraša le nekaj vprašanj.
- Mednarodno priznani izdelki: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, itd;
- Pomoč uporabnikom- pomoč uporabnikom je na voljo 24 ur na dan vseh 7 dni v tednu.
- Bliskovit odzivni čas na nove napade vašega računalnika.
- Najboljša stopnja zaznave;
- Vsakourne posodobitve podpisov novih virusov- avtomatski ali načrtovani ukrepi zaščite pred najnovejšimi virusi.

1.1. Zakaj BitDefender?

Dokazano. Najbolj odziven protivirusni proizvajalec. Bitdefenderjev hitri odziv v primeru izbruha virusa je bil dokazan začevši z izbruhom virusa CodeRed, Nimda in Sircam, kot tudi Badtrans.B, ter ostalih nevarnih in zlo namernih kod. BitDefender je bil prvi, ki je ponudil 'zdravilo' za te viruse, ter je omogočil dostop do le-teh, vsem sistemom, ki so bili okuženi. Sedaj, s širitvijo Klez virusa, v večih različicah, je takojšnja zaščita še enkrat postala prioriteta za vsak računalniški sistem.

Inovativen. Nagrajen za inovativnost s strani Evropske komisije in EuroCasea. BitDefender je prejel Evropsko IST nagrado, ki jo podeljuje Evropska komisija, ki jo predstavlja 18 akademij v Evropi. Sedaj, v osmem letu svojega delovanja Evropska

komisija podeljuje IST nagrade za izdelke, ki predstavljajo najboljšo evropsko inovativnost na področju informacijske tehnologije.

Obsežen. Pokriva vsa področja vašega omrežja in tako zagotavlja celovito zaščito za vaš sistem. BitDefenderjeve varnostne rešitve za poslovna okolja zadovoljujejo potrebe po varnosti v današnjem poslovnem svetu, s tem, ko ponujajo zaščito za majhna omrežja, pa vse do velikih strežnikov in več platformskih WAN omrežij.

Vaša dokončna zaščita. Zadnja obrambna črta za vse nevarnosti, ki grozijo vašemu sistemu. Ker zaznavanje virusov na osnovi pregledovanja kod ni vedno nudil popolne zaščite, je BitDefender izpopolnil zaznavanje virusov na osnovi obnašanja kod in s tem ponudil zaščito tudi pred novo nastalimi škodljivimi kodami. MIDAS (Malware Intrusion Detection Advanced System), poda zaščito na treh nivojih, kar zagotavlja neoporečnost sistema tudi pri najhitrejših izbruhih.

To so **Stroški**, ki se jim želi organizacija izogniti in za kar so varnostni izdelki tudi načrtovani, da preprečujejo:

- Napadi virusov
- Izguba komunikacije zaradi okuženih e sporočil
- Zlom e-pošte
- Čiščenje in obnavljanje sistemov
- Zmanjšana produktivnost končnih uporabnikov, zaradi nedosegljivosti sistemov
- Hekanje in neavtoriziran dostop, ki povzroča škodo

Nekatere **izboljšave in ugodnosti**, ki jih prinaša uporaba BitDefenderja:

- Poveča zanesljivost omrežja z ustavitvijo zlonamernih kod (npr., Nimda, Trojanski konji, DDoS).
- Zaščiti oddaljene uporabnike pred napadi na njihov sistem.
- Zmanjša administrativne stroške in omogoča hiter razvoj z BizDefenderjevimi poslovnimi rešitvami.
- Ustavi širjenje zlonamernih kod prek e-pošte, z uporabo Bitdefenderjeve e-poštne zaščite. Začasno ali stalno blokira neavtorizirane, ranljive in druge aplikacijske povezave.

Spletni klepet 24/7: <http://www.parametica.si>.

1.2. O SOFTWINU

Podjetje Softwin, ustanovljeno leta 1990, dobitnik nagrade IST 2002, je eno izmed vodilnih tehnioloških podjetij v vzhodnoevropski industriji programske opreme z letno rasjo višjo od 50% v zadnjih petih letih in 70% rastjo prometa s tujino.



SOFTWIN se je osredotočil na zagotavljanje programskih rešitev in storitev ki omogočajo hitro rastočim podjetjem reševanje kritičnih poslovnih izzivov in kapitalizacijo novih poslovnih priložnosti.

Zaradi aktivnosti na večini razvitih IT trgov v ZDA in EU se SOFTWIN razvija na 4 ih notranjih povezavah **poslovne povezave**:

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management



Namestitev



2. BitDefender Antivirus v10 Namestitev

BitDefender Antivirus v10 Namestitev poglavje hitrega vodiča obsega naslednje vsebine:

- Sistemske zahteve
- Koraki namestitve
- Čarovnik za namestitev
- Nadgradnja
- Odstranjanje, popravilo ali spreminjanje BitDefenderja

2.1. Sistemske zahteve

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

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Pentium II 350 MHz procesor ali zmogljivejši
- Vsaj 128 MB pomnilnika (priporočeno 256 MB)
- Vsaj 60 MB prostora na trdem disku
- Internet Explorer 5.5 ali novejši

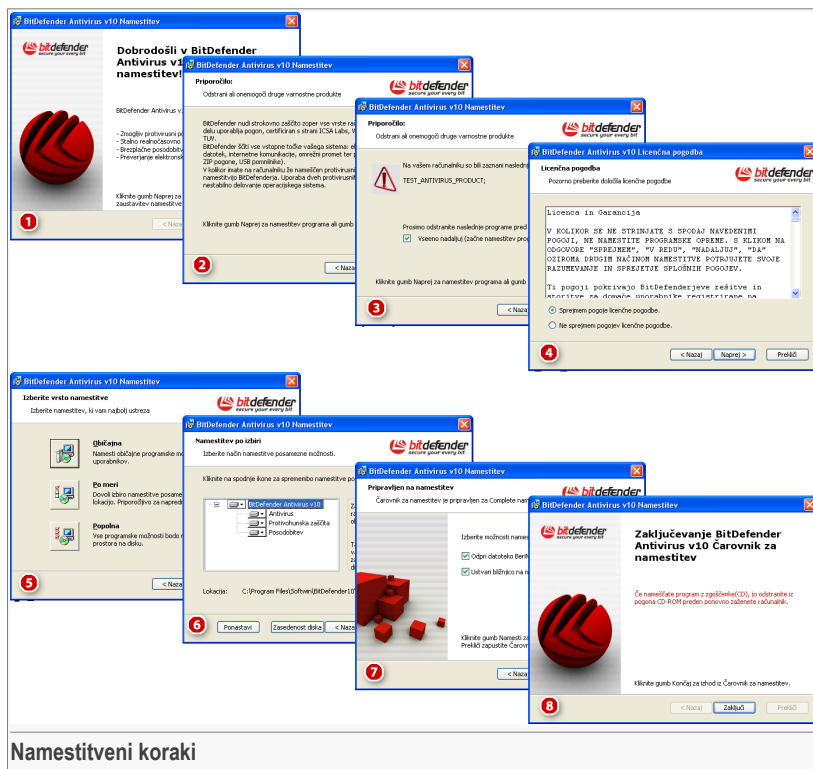
Microsoft Windows Vista 32-bit

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

BitDefender Antivirus v10 preizkusno različico lahko prenesete s strani <http://www.parametika.si>, ki je uradna stran podjetja Parametika d.o.o., posvečena informacijski varnosti.

2.2. Namestitveni koraki

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



Namestitveni koraki

1. Kliknite **Naprej** za nadaljevanje ali **Nazaj** za vrnitev na prvi korak.
2. Kliknite **Naprej** za nadaljevanje ali **Nazaj** za vrnitev na prvi korak.
3. BitDefender Antivirus v10 vas opozori, če imate na vašem računalniku nameščene druge protivirusne programe.



Pozor

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

Kliknite **Nazaj** za vrnitev na prejšnji korak ali **Prekliči** za prekinitev namestitve. Če želite nadaljevati, kliknite **Naprej**.

**Opomba**

Če BitDefender Antivirus v10 ne odkrije drugih protivirusnih programov na vašem sistemu, boste preskočili ta korak.

4. 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.
5. Izbirate lahko med različnimi vrstami namestitve: običajna, po meri ali popolna.

Običajno

Program bo nameščen z običajnimi možnostmi. To je priporočena izbira za večino uporabnikov.

Po meri

Možnost izbire komponent, ki jih želite namestiti. Priporočeno le za napredne uporabnike.

Popolna

Popolna namestitev programa. Vsi BitDefender moduli bodo nameščeni.

Če ste izbrali **Običajna** ali **Popolna**, boste preskočili korak 6.

6. Če ste izbrali **Po meri**, se vam bo odprlo novo okno, ki bo prikazovalo vse BitDefender komponente, med katerimi lahko izbirate.

Če kliknete katerokoli komponento, se vam bo na desni izpisal kratek opis (prikazan bo tudi minimalni prostor, potreben na trdem disku). S klikom na ikono se odpre okno, kjer lahko izberete ali boste izbran modul namestili ali ne.

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 v10. Kliknite **Naprej**.

7. 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 v10 na namizju ob zaključku namestitve.

Kliknite **Namesti** za začetek namestitve programa.



Pomembno

Med namestitvijo se bo pojavil **čarovnik**. Čarovnik vam bo pomagal pri registraciji vašega **BitDefender Antivirus v10**, kreiranju BitDefender računa in konfiguriranju BitDefender zaščite za opravljanje pomembnih varnostnih opravil. Dokončajte delo s čarovnikom pred nadaljevanjem z naslednjim korakom.

8. Kliknite **Zaključ**i za dokončanje namestitve programa. Če ste izbrali privzeto možnost za namestitveno mapo, potem je v mapi `Program Files` ustvarjena nova mapa, imenovana `Softwin`. Le-ta pa vsebuje podmapo `BitDefender 10`.



Opomba

Operacijski sistem lahko od vas zahteva, da ponovno zaženete računalnik za dokončanje namestitve.

2.3. Namestitveni čarovnik

Med procesom namestitve se bo pojavil čarovnik, ki vam bo pomagal registrirati vaš **BitDefender Antivirus v10**, 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 v10 nameščen.

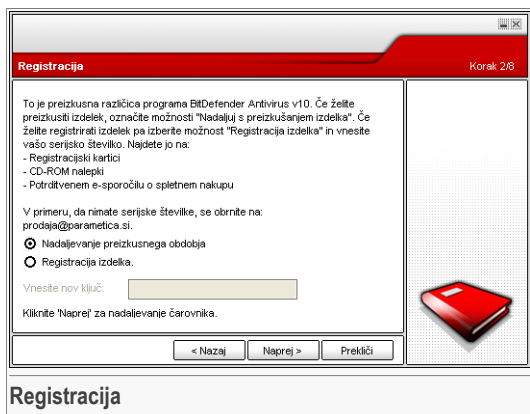


2.3.1. Korak 1/8 - BitDefender namestitveni čarovnik



Kliknite **Naprej**.

2.3.2. Korak 2/8 - Registracija BitDefender Antivirus v10



Izberite možnost **Registriraj izdelek** za registracijo **BitDefender Antivirus v10**. Vnesite licenčni ključ v polje **Vnesi nov ključ**.

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

Kliknite **Naprej**.

2.3.3. Korak 3/8 - Kreiranje BitDefender računa

Registracija izdelka Korak 3/8

Za dostop do BitDefender tehnične podpore in drugih storitev morate kreirati račun. Če le-tega že imate, vas prosimo za vnos zahtevanih podatkov. Če BitDefender računa še nimate, pa vpišite vaš elektronski naslov ter geslo.

E-pošta:

Geslo:


Ponovno vnesite geslo:

Ste pozabili geslo?

Preskoči ta korak

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

Prosimo za vnos veljavnega elektronskega naslova. Podrobitveno sporočilo bo poslano na vpisani naslov



Kreiranje računa

Nimam še BitDefender računa

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

Vnesite veljaven e-poštni naslov v polje **E-pošta**. Geslo vnesite v polje **Geslo**. Geslo potrdite v polju **Ponovi geslo**. Uporabite e-poštni naslov in geslo za prijavo v vaš račun na <http://myaccount.bitdefender.com>.



Opomba

Geslo mora biti dolgo vsaj štiri znake.

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.



Pomembno

Prosimo za aktivacijo računa pred nadaljevanjem na naslednji korak.

Če ne želite kreirati BitDefender računa, izberite **Preskoči ta korak**. Preskočili boste tudi naslednji korak čarovnika.

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



Že imam BitDefender račun

Če že imate aktivni račun, vnesite elektronski naslov in geslo vašega računa. Če vnesete napačno geslo, boste ponovno vprašani zanj, ko kliknete **Naprej**. Kliknite **V redu** za ponoven vnos gesla ali **Prekliči** za izhod iz čarovnika.

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

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

2.3.4. Korak 4/8 - Vnos podatkov o računu

Konfiguracija računa Korak 4/8


Prosimo vas, da izpolnite podatke o računu. Podatki so zaupni. Če že imate račun, vam bo čarovnik izpolnil podatke, ki ste jih vnesli ob prvem kreiranju.

Ime:

Primek:

Država:

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



Podatki o računu



Opomba

Ta korak boste preskočili, če ste izbrali možnost **Preskoči ta korak** v **tretjem koraku**.

Vnesite vaše ime in priimek ter izberite državo, v kateri prebivate.

Če že imate račun, vam bo čarovnik prikazal vse predhodno vnešene podatke. Le-te lahko po potrebi popravite.



Pomembno

Vnešeni podatki so zaupne narave.

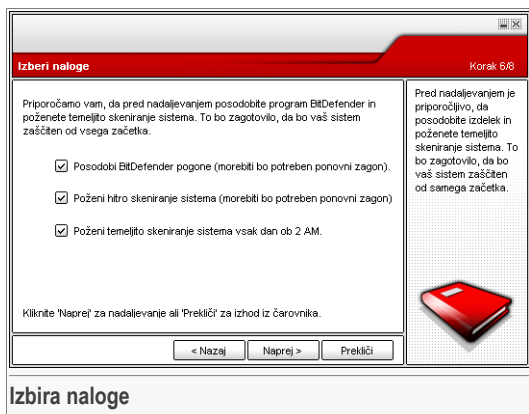
Kliknite **Naprej** za nadaljevanje ali **Prekliči** za izhod iz čarovnika.

2.3.5. Korak 5/8 - Več o RČPV



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

2.3.6. Korak 6/8 – Izbira opravil



Nastavite BitDefender Antivirus v10 za opravljanje pomembnih nalog za varnost vašega sistema.

Možnosti so naslednje:



- **Posodobitev BitDefender Antivirus v10 pogonov (morebiti bo potreben ponoven zagon)** - med naslednjim korakom se bodo BitDefender Antivirus v10 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 Antivirus v10 preveril, ali vaše datoteke v mapah `Windows` in `Program Files` niso okužene.
- **Poženi polno skeniranje sistema vsak dan ob 2h** - požene polno skeniranje sistema vsak dan ob 2h.



Pomembno

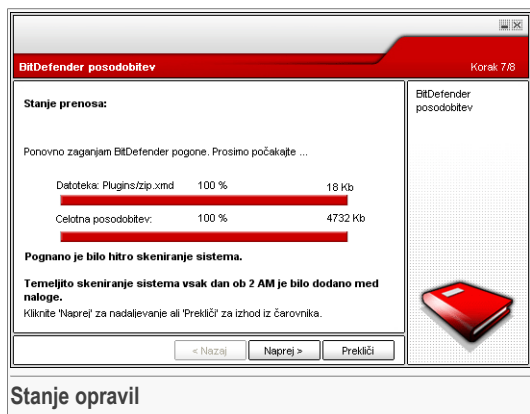
Priporočamo vam, da omogočite naslednje možnosti pred nadaljevanjem na naslednji korak. S tem boste zagotovili visoko varnost vašega sistema.

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

Z vračanjem na predhodne korake lahko spremenite vse nastavitve (kliknite **Nazaj**). V nadaljevanju namreč ni možna vrnitev na prejšnje korake.

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

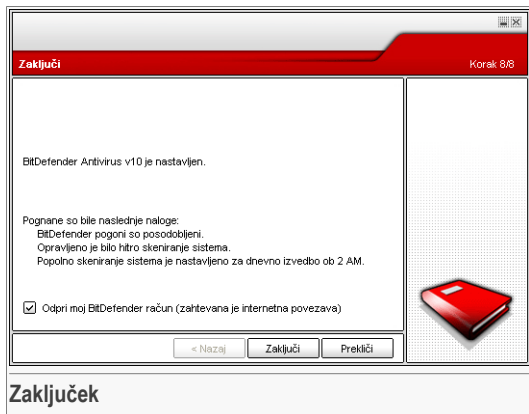
2.3.7. Korak 7/8 - Čakanje na dokončanje opravil



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.

2.3.8. Korak 8/8 - Povzetek



To je zadnji korak namestitvenega čarovnika.

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

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

2.4. 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 "[Namestitveni koraki](#)" (p. 9) sekciji.



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. 9).

**Pomembno**

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

2.5. Odstranjevanje, popravilo ali spreminjanje BitDefenderja

Če želite spremeniti, popraviti ali izbrisati **BitDefender Antivirus v10**, sledite poti iz Windows start menija: **Start** → **Programi** → **BitDefender 10** → **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:

- **Spremeni** - izberete nove komponente ali pa izbrisate že nameščene;
- **Popravi** - ponovno namestite tiste komponente, ki ste jih namestili pri prejšnji namestitvi;

**Pomembno**

Pred popravljanjem izdelka priporočamo, da shranite [BitDefender nastavitve](#). Ko se zaključi proces popravljanja, jih ponovno naložite.

- **Odstrani** - izbrisate vse nameščene komponente.

Za nadaljevanje izberite eno izmed navedenih možnosti. Za čisto namestitev priporočamo **Odstrani**. Ko je brisanje končano, je priporočljivo da izbrisate še mapo Softwin, ki se nahaja v mapi Program Files.



Opis in lastnosti



3. BitDefender Antivirus v10

Protivirusna in protivohunska programske rešitve za vaš osebni računalnik!

BitDefender Antivirus v10 je zmogljivo protivirusno orodje s številnimi varnostnimi mehanizmi. Enostavnost uporabe in samodejno posodabljanje naredita **BitDefender Antivirus v10** program tipa »namesti in pozabi«.

3.1. Protivirusna zaščita

BitDefenderjev protivirusni modul zagotavlja detekcijo in odstranitev vseh računalniških virusov, ki prežijo na Vaš sistem. Protivirusni modul uporablja robustno skeniranje, ki so ga potrdili ICSA Labs, Virus Bulletin, Checkmark, CheckVir and TÜV.

IZBOLJŠANA proaktivna detekcija. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) ustvari računalnik-v-računalniku, kjer zaganja programe in tako preverja za sumljivim obnašanjem programov. Ta nova tehnologija predstavlja dodatno plast zaščite za operacijski sistem, pred še nepoznanimi virusi, z zazanavanjem sumljive kode za katero še niso bile izdane definicije.

Stalna Protivirusna zaščita. Novi in izboljšani BitDefender-jevi mehanizmi za skeniranje bodo skenirali in očistili okužene datotek ob dostopu in tako minimizirali izgubo podatkov. Okuženi dokumenti so sedaj lahko očiščeni in obnovljeni, namesto, da bi jih bilo potrebno izbrisati.

NOVO odkrivanje in odstranjevanje rootkit orodij. Novi BitDefender modul odkriva rootkit orodja (škodljive programe, ki skriti skušajo prevzeti nadzor nad računalnikom) in jih odstrani.

NOVO spletno skeniranje. Spletni promet je sedaj filtriran v realnem času še preden doseže spletni brskalnik. Tako bo vaša spletna izkušnja bolj varna in prijetna.

Zaščita Peer-2-Peer in IM programov. Filtriranje programov za izmenjavo datotek in klepetalnic za virusi.

Popolna e-poštna zaščita. BitDefender teče na nivoju POP3/SMTP protokola in filtrira vhodna in izhodna e-sporočila ne glede na uporabljen poštni odjemalec (Outlook™, Outlook Express™, Windows Mail™, Netscape®, The Bat!™, idr.) brez dodatnih nastavitev.

3.2. Protivohunska zaščita

Nadzor in preprečevanje nevarnosti vohunskih programov se vrši v realnem času, še preden bi poškodovali vaš sistem. Ob uporabi obsežnih baz podatkov o vohunskih programih bo vaš računalnik dobro varovan.

Realnočasovna zaščita pred vohunskimi programi. 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.

Skeniranje in čiščenje vohunskih programov. BitDefender lahko skenira vaš sistem, ali le njegov del, za znanimi vohunskimi programi. Skeniranje uporablja stalno posodabljanje bazo definicij vohunskih programov.

NOVO zaščita zasebnosti. Zaščita zasebnosti preverja vaš spletni in e-poštni promet za osebnimi informacijami kot so številka bančne kartice, davčna številka ter ostale uporabniško določene vnose kot so gesla, deli gesel ipd.

Zaščita pred klicalniki. Nastavljiva zaščita pred klicalniki onemogoča škodljivim programom upravljanje z modemom in posledično preprečuje visoke telefonske račune.

Nadzor piškotkov. Požarni zid filtrira prihajajoče in odhajajoče piškotke in tako ohranja Vašo zasebnost med brskanjem po internetu.

Nadzor aktivnih vsebin. Blokira potencialno sumljive aplikacije kot so: ActiveX, Java Applets ali Java Scripts.

3.3. Druge lastnosti

IZBOLJŠANA namestitvev in uporaba. Konfiguracijski čarovnik se zažene takoj po namestitvi in uporabniku pomaga izbrati najprimernejše nastavitve za posodabljanje programa ter urnik opravil, pomaga pa tudi pri registraciji in aktivaciji programa.

IZBOLJŠANA uporabniška izkušnja. BitDefender je prenovil podobo uporabniškega vmesnika s poudarkom na enostavnosti uporabe in izogibanju nepreglednosti. Posledica tega je, da BitDefender v10 modulu zahtevajo bistveno manj posredovanja s strani uporabnika, povečani sta stopnji avtomatizacije in samodejnega učenja.

Vsakourne posodobitve. BitDefender se samodejno posodobi vsako uro, torej 24-krat dnevno, preko interneta, neposredno ali preko proxy strežnika. Izdelek se zna tudi sam popraviti, če je to potrebno seveda, s prenosom okvarjenih ali manjkajočih datotek iz BitDefender strežnikov. Lastniki BitDefender licence so torej upravičeni do brezplačnih posodabljanj in posodobitev programske opreme.



24-urna tehnična podpora. Podpora je na voljo na spletu, kjer najdemo obsežne podatkovne baze z odgovori na pogosto zastavljena vprašanja.

Reševalni disk. BitDefender Antivirus v10 se nahaja na t. i. bootable CD-ju. Ta CD lahko uporabimo za analizo/popravljanje/čiščenje okuženega sistema, ki se ne zažene več.



4. BitDefenderjevi moduli

BitDefender Antivirus v10 vsebuje naslednje module: **Splošno**, **Antivirus**, **Antispyware** in **Posodobitev**.

4.1. Splošno modul

BitDefender je nameščen povsem konfiguriran za maksimalno varnost.

Splošno - v tem razdelku nastavljate splošni nivo varnosti in opravljate nujne varnostne naloge. Tu lahko tudi registrirate izdelek in vidite povzetek vseh osnovnih nastavitvev, podrobnostih o programu in kontaktnih informacijah.

4.2. Modul Antivirus

BitDefender varuje računalnik pred virusi s skeniranjem vaših datotek, elektronske pošte in ostalih vsebin, ki vstopajo v vaš računalnik. S protivirusnim modulom imate dostop do vseh BitDefender nastavitvev in funkcij.

Zaščita pred virusi je razdeljena na dve metodi:

- **Skeniranje ob dostopu** - Prepreči novim virusom vstop v sistem. Sistem se imenuje Virusni Ščit (virus shield) – podatki so skenirani že ob vstopu v računalnik. Na primer, ko odprete Wordov dokument, bo BitDefender pregledal cel document, še preden se bo ta dejansko odprl. Prav tako BitDefender skenira vso e-pošto takoj ob prejetju le-te.
- **Skeniranje na zahtevo** - Zazna že obstoječe viruse. Gre za klasično skeniranje, ki ga sproži uporabnik, ki izbere kateri trdi disk, mapo ali datoteko želi skenirati.

4.3. Modul Antispyware

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. Učinkoviti 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.

4.4. Posodobitveni modul

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.

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**.

Nastavitve posodabljanja pa lahko nastavite na dva načina:

- **Avtomatično posodabljanje** - program se avtomatično poveže na BitDefenderjev strežnik in preveri za posodobitve. Če so bile izdane nove posodobitve, se BitDefender avtomatično posodobi. Avtomatično posodobitev lahko izvedete kadarkoli s pritiskom na tipko **Posodobi zdaj** v modulu **Posodobitve**.
- **Ročno posodabljanje** - uporabnik mora na računalnik prenesti posodobitve in jih namestiti.



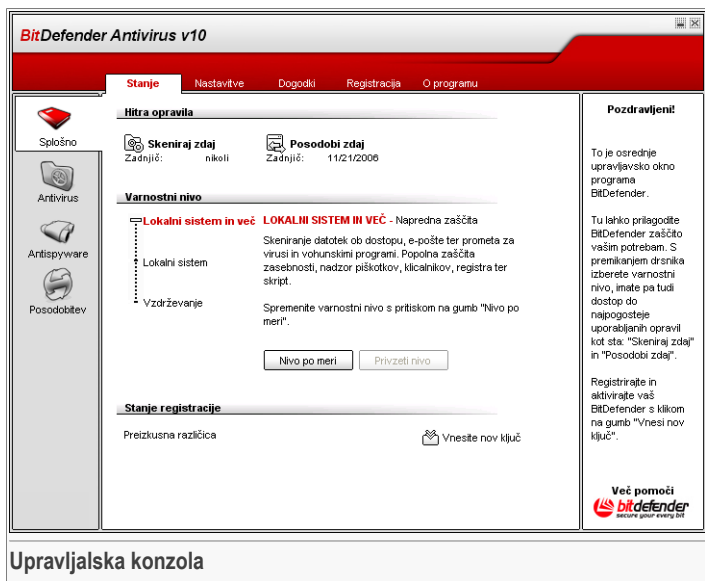
Upravljalna konzola



5. Pregled

BitDefender Antivirus v10 je bil zasnovan s centralno upravljsko konzolo, ki omogoča nastavljanje možnosti vseh BitDefender modulov. Drugače povedano – odprte upravljske konzole zadostuje za dostop do vseh modulov: **Antivirus**, **Antispyware** in **Posodobitev**.

Za dostop do upravljske konzole uporabite Windows Start meni in sledite poti **Start** → **Programs** → **BitDefender 10** → **BitDefender Antivirus v10** ali še hitreje, dvokliknite **BitDefender ikono** v sistemskem kotičku.



Na levi strani upravljske konzole se nahaja izbirnik modulov:

- **Splošno** - v tem razdelku nastavlja splošni nivo varnosti in opravljate nujne varnostne naloge. Tu lahko tudi registrirate izdelek in vidite povzetek vseh osnovnih nastavitev, podrobnosti o programu in kontaktnih informacijah.
- **Antivirus** - v tem razdelku lahko nastavite modul **Antivirus**.
- **Antispyware** - v tem razdelku lahko nastavite modul **Antispyware**.
- **Posodobitev** - v tem razdelku lahko nastavite modul **Posodobitev**.

Na desni strani upravljaljske konzole vidite informacije o razdelku, v katerem se nahajate. Možnost **Več pomoči**, ki se nahaja v desnem spodnjem kotu, odpre datoteko s **Pomočjo**.

5.1. Sistemski kotiček

Ko je konzola minizirana, se bo v sistemskem koticu pojavila ikona:



BitDefender ikona v sistemskem koticu

Če dvokliknete to ikono, se bo odprla upravljaljska konzola. Desni klik odpre vsebinski meni, ki ponuja hitre upravljaljske možnosti programa BitDefender:

- **Prikaži / Zapri** - odpre upravljaljsko konzolo ali jo pomanjša v sistemski koticek.
- **Pomoč** - odpre elektronsko dokumentacijo.
- **Splošno** - upravljanje modula **Splošno** module.
 - **Vnesi nov ključ** - požene čarovnika za registracijo, ki vam bo pomagal skozi proces registracije.
 - **Uredi račun** - požene čarovnika, ki vam bo pomagal kreirati BitDefender račun.
- **Antivirus** - upravljanje **Antivirus** modula.
 - **Realnočasovna zaščita je omogočena / onemogočena** - prikaže stanje **realnočasovne zaščite** (enabled / disabled). Izberite to možnost za vklop ali izklop realnočasovne zaščite.
 - **Skeniranje** - odpre podmeni, v katerem lahko izberete eno izmed skenirnih nalog, ki so na voljo v razdelku **Skeniranje**.
- **Antispyware** - upravljanje **Antispyware** modula.
 - **Vedenjska protivohunska zaščita je omogočena / onemogočena** - prikaže stanje **vedenjske antispyware zaščite** (omogočena / onemogočena). Izberite to možnost za vklop ali izklop vedenjske protivohunske zaščite.
 - **Napredne nastavitve** - omogočajo nastavitve protivohunskih možnosti.
- **Posodobitev** - upravljanje z modulom **Posodobitev**.
 - **Posodobi zdaj** - izvede takojšnjo posodobitev.



- **Samodejno posodabljanje je omogočeno / onemogočeno** - prikaže stanje **samodejnega posodabljanja** (omogočeno / onemogočeno). Izberite to možnost za vklop ali izklop samodejnega posodabljanja.
- **Izhod** - zapre aplikacijo. Z izbranjem te možnosti, bo izginila tudi ikona. Če želite zopet odpreti konzolo, jo morate ponovno pognati s Start menija.

Opomba



Če onemogočite enega ali več BitDefender modulov, se bo ikona spremenila v črno bravo. Tako boste vedeli, da so nekateri moduli onemogočeni, brez da bi odprli upravljalno konzolo.

Ikona bo utripala, ko bo na voljo posodobitev.

5.2. Vrstica aktivnosti skeniranja

Vrstica aktivnosti 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 vas bo obveščala o morebitni neaktivnosti virusne zaščite z rdečim križcem v okencu (**Datoteke**). Tako boste vedeli ali ste zaščiteni brez da bi odprli upravljalno konzolo.

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

Opomba



Za popolno skritje tega okna, onemogočite možnost **Omogoči vrstico aktivnosti skeniranja (graf na zaslonu)** (v modulu **Splošno**, odsek **Nastavitve** section).



6. Splošno modul

Poglavje **Splošni** vsebuje naslednje teme:

- Splošne informacije
- Nastavitve glavnega okna
- Dogodki
- Registracija vaše kopije
- O programu



Opomba

Za več informacij o **Splošnem** modul si oglejte izsek o "*Splošno modul*" (p. 27).

6.1. Osrednja administracija

Za dostop do tega razdelka kliknite na zavihek **Stanje** v modulu **Splošno**.

The screenshot shows the BitDefender Antivirus v10 main interface. The window title is "BitDefender Antivirus v10". The interface has a red header with navigation tabs: "Stanje", "Nastavitve", "Dogodki", "Registracija", and "O programu". The "Stanje" tab is active. On the left is a sidebar with icons for "Splošno", "Antivirus", "Antispyware", and "Posodobitev". The main content area is divided into sections: "Hitra opravila" (Quick fixes) with "Skeniraj zdaj" (Last scan: nikoli) and "Posodobi zdaj" (Last update: 11/21/2006); "Varnostni nivo" (Security level) showing "LOKALNI SISTEM IN VEČ - Napredna zaščita" (Local system and more - Advanced protection) with a description of scanning and protection, and buttons for "Nivo po meri" (Custom level) and "Privzeti nivo" (Default level); "Stanje registracije" (Registration status) showing "Preizkusna različica" (Trial version) and a "Vnesite nov ključ" (Enter new key) button. On the right is a "Pozdravljen!" (Welcome!) message and a "Več pomoči" (More help) link with the BitDefender logo.

Ta odsek vsebuje informacije o stanju vaše BitDefender licence. Tu se lahko registrirate in preverite, do kdaj velja vaša licenca.

6.1.1. Hitra opravila


BiDefender omogoča hiter dostop do esencialnih varnostnih opravil. Z uporabo teh opravil lahko posodobljate BitDefender, skenirate sistem ali blokirate promet.

Ta skeniranje celotnega sistema kliknite  **Skeniraj zdaj**. Pojavilo se bo oknoskeniranje in začelo se bo popolno skeniranje sistema.



Pomembno

Priporočamo vam da opravite obširno skeniranje sistema vsaj enkrat na teden. Za več informacij o opravljenih skeniranjih in procesih skeniranja si oglejte [Skeniranje na zahtevo](#) in teh navodilih za uporabo.

Samodejno posodabljanje je moč izvesti kadarkoli s klikom na možnost  **Posodobi zdaj**. Počakajte nekaj sekund, da se zaključi proces posodabljanja ali preglejte [Posodobitve](#).



Opomba

Za več podrobnosti o procesih posodabljanja si oglejte [Samodejno posodabljanje](#) v teh navodilih za uporabo.

6.1.2. Stopnja varnosti

Izbirate lahko med različnimi stopnjami varnosti, ki najbolj ustrezajo vašim potrebam. Povlecite drsnik po skali do željene stopnje varnosti.

Obstajajo tri vrste pravil:

Stopnja varnosti	Opis
Obstojnost	Da bi se zaščitili pred vohunskimi programi, imejte Protivohunska zaščita omogočeno. Samo posodabljanje BitDefenderja. Uporabna za sistemske administratorje, čeprav ne ponuja zaščite.
O mrežje zaupanjem	z Protivirusna zaščita. Posebej priporočamo za računalnike brez mrežnega ali medmrežnega dostopa. Zelo majhna obremenitev računalnika. Skenirane bodo vse datoteke.



Stopnja varnosti	Opis
Lokalni sistem in več	Protivirusna in protivohunska zaščita Posebej priporočamo za računalnike brez mrežnega ali medmrežnega dostopa. Zelo majhna obremenitev računalnika. Skenirane bodo vse datoteke.

BitDefender Antivirus v10 Namestitev poglavje hitrega vodiča obsega naslednje vsebine:

Varnostni nivo lahko nastavite s klikom na **Nivo po meri**. V oknu, ki se pojavi, izberite BitDefender zaščitne možnosti, ki jih želite omogočiti in kliknite **V redu**.

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

6.1.3. Registracija

Ta odsek vsebuje informacije o stanju vaše BitDefender licence. Tu se lahko registrirate in preverite, do kdaj velja vaša licenca.

Za vnos novega ključa kliknite  **Vpišite nov ključ**. Dokončajte [registration wizard](#) tza uspešno registracijo BitDefenderja.

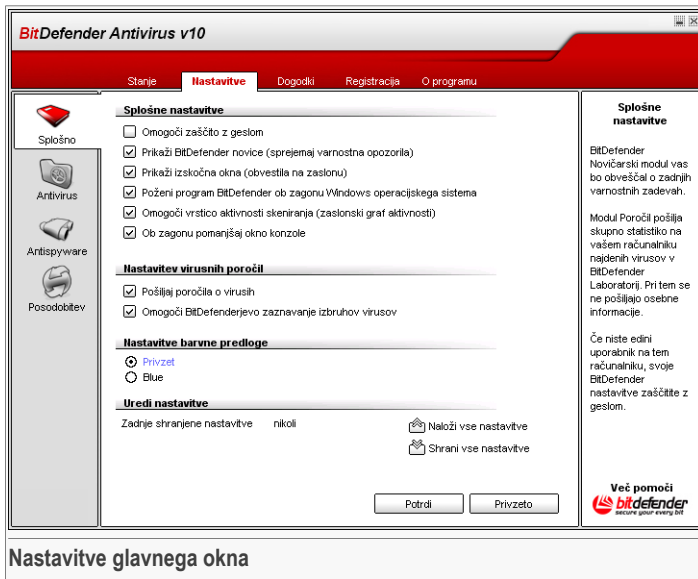


Opomba

Za več informacij o procesu registracije si oglejte [Registracija izdelka](#).

6.2. Nastavitve glavnega okna

Za dostop do teh možnosti kliknite zavihek **Nastavitve** v modulu **Splošno**.



Nastavitve glavnega okna

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

Na voljo so 4 kategorije: **Splošne nastavitve**, **Nastavitve poročil o virusih**, **Nastavitve vmesnika** in **Upravljalne nastavitve**.

6.2.1. Nastavitve poročil

- **Omogoči zaščito z geslom** - omogoči zaščito BitDefender nastavitvev 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

Geslo

Ponovno vnesite

Geslo naj bo dolgo vsaj 8 znakov.

Potrditev gesla

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

Od sedaj naprej boste za spremembo nastavitve programa vedno morali vnesti geslo.



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.



Opomba

Priporočamo, da ohranite to možnost izbrano.

- **Omogoči orodno vrstico dejavnosti skeniranja (prikaz dejavnosti produkta)** - omogoči/onemogoči **Orodna vrstica dejavnosti**.
- **Poženi minimizirano** - minimizira BitDefender upravljalno konzolo ob zagonu. V "sistemskem kotičku" se pokaže ikona BitDefender.

6.2.2. Nastavitve 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.

6.2.3. Nastavitve vmesnika

Omogoča izbiranje barve sheme upravljalne konzole. Če želite izbrati drugo bravno shemo, preprosto kliknite nanjo.

6.2.4. Upravljalne nastavitve

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.

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

6.3. Dogodki

Za dostop do teh možnosti kliknite zavihek **Dogodki** v modulu **Splošno**.



BitDefender Antivirus v10

Stanje Nastavitve **Dogodki** Registracija O programu

Seznam dogodkov

Izberite vir:

Vrsta	Datum	Čas	Opis	Vir
Informacije	11/21/2...	7:01:30 ...	Posodobitev je uspela	Posoc
Informacije	11/21/2...	7:03:01 ...	Skeniranje končano	Antivi

Filter Počisti dnevnik Osveži

Dnevnik dogodkov

Opozorila in izvalna dejanja ob odkritih virusih ter volunskih programih, opozorilih požarnega zidu, poskusih vdorov in dostopov do blokiranih spletnih strani so zabeležena z nemono priprave kar najboljše varnostne politike na vašem sistemu.

Zabeležene dogodke je moč filtrirati po posebnih modulih ali pomembnosti.

Pritisek gumba "Počisti poročila" bo permanentno izbrisal vse vnose.

Več pomoči

 BitDefender
 Antivirus - Firewall - Anti-Spyware - Anti-Malware

Dogodki

Vsi dogodki, ki se zgodijo v zvezi s programom BitDefender, jih program zabeleži v tem delu.

Obstajajo 3 vrste dogodkov: **Informacije**, **Opozorilo** in **Kritično**.

Primeri dogodkov:

- **Informacije** - se prikaže, ko je skenirano e sporočilo;
- **Opozorilo** - ko je bila zaznana sumljiva datoteka;
- **Kritično** - ko je bila zaznana okužena datoteka.

Za vsak dogodek so na voljo naslednje informacije: datum in ura, ko se je dogodek zgodil, manjši opis in vir (**Protivirusna zaščita**, **Požarni zid**, **Protivohunska zaščita** or **Posodobitve**). Dvokliknite na dogodek, da vidite njegove lastnosti.

Te dogodke lahko filtrirate na dva načina(po vrsti ali po viru):

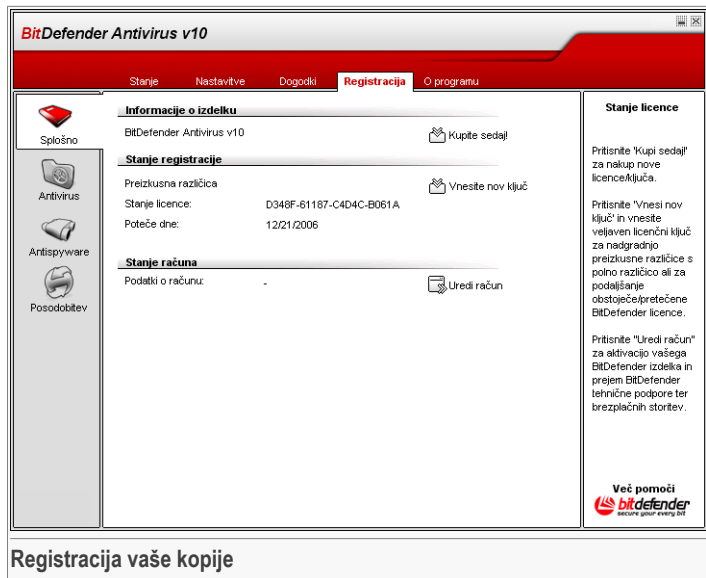
- Kliknite **Filter** za izbiro, katere tipe dogodkov želite videti.
- Izberite vir dogodkov iz padajočega menija.

Če je **glavno Bitdefenderjevo okno** odprto na zavihku **Dogodki** v trenutku, ko se dogodek zgodi, morate klikniti na **Osveži**, da se novi dogodek prikaže.

Da izbrišete vse dogodke, kliknite na **Počisti zapisnik**.

6.4. Registracija vaše kopije

Za dostop do teh možnosti kliknite zavihek **Registracija** v modulu **Splošno**.



Ta odsek vsebuje informacije o stanju vaše BitDefender licence. Tu se lahko registrirate in preverite, do kdaj velja vaša licenca.

Nov licenčni ključ lahko kupite s klikom na gumb **Kupi**.

S klikom na **Vpišite nov ključ** lahko registrirate nov produkt, spremenite registracijski ključ ali prilagodite račun. Za spremembe nastavitvev računa kliknite **Uredi račun**. V obeh primerih se bo pojavil čarovnik za registracijo.

6.4.1. Čarovnik za registracijo

Nastavitveni čarovnik ima 5 korakov.



Korak 1/5- BitDefenderjev čarovnik za registracijo

BitDefender namestitveni čarovnik Korak: 1/5

Pozdravljeni v BitDefender namestitvenem čarovniku.

Ta čarovnik vam bo pomagal registrirati izdelek in aktivirati vaš BitDefender račun.

Kliknite **Naprej** za nadaljevanje čarovnika.

Pozdravno okno

Kliknite **Naprej**.

Korak 2/5 - Registracija BitDefenderja

Registracija Korak: 2/5

To je preizkusna različica programa BitDefender Antivirus v10. Če želite preizkusiti izdelek, označite možnost "Nadaljuj s preizkušanjem izdelka". Če želite registrirati izdelek pa izberite možnost "Registracija izdelka" in vnesite vašo serijsko številko. Najdete jo na:

- Registracijski kartici
- CD-ROM naleplki
- Potrditvenem e-sporočilu o spletnem nakupu

V primeru, da nimate serijske številke, se obrnite na: prodaja@parameteca.si.

Nadaljevanje preizkusnega obdobja
 Registracija izdelka.

Vnesite nov ključ:

Kliknite **Naprej** za nadaljevanje čarovnika.

Registracija

Izberite možnost **Registriraj izdelek** za registracijo **BitDefender Antivirus v10**. Vnesite licenčni ključ v polje **Vnesi nov ključ**.

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

Kliknite **Naprej**.

Korak 3/5 - Kreiranje BitDefender računa

Registracija izdelka Korak 3/5

Za dostop do BitDefender tehnične podpore in drugih storitev morate kreirati račun. Če le-tega že imate, vas prosimo za vnos zahtevanih podatkov. Če BitDefender računa še nimate, pa vpišite vaš elektronski naslov ter geslo.

E-pošta:


Geslo:

Ponovno vnesite geslo:

Ste pozabili geslo?

Preskoči ta korak

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



< Nazaj Naprej > Prekliči

Kreiranje računa

Nimam še BitDefender računa

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

Vnesite veljaven e-poštni naslov v polje **E-pošta**. Geslo vnesite v polje **Geslo**. Geslo potrdite v polju **Ponovi geslo**. Uporabite e-poštni naslov in geslo za prijavo v vaš račun na <http://myaccount.bitdefender.com>.



Opomba

Geslo mora biti dolgo vsaj štiri znake.

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.



Pomembno

Prosimo za aktivacijo računa pred nadaljevanjem na naslednji korak.

Če ne želite kreirati BitDefender računa, izberite **Preskoči ta korak**. Preskočili boste tudi naslednji korak čarovnika.

Kliknite **Naprej**.



Že imam BitDefender račun

Če že imate aktivni račun, vnesite elektronski naslov in geslo vašega računa. Če vnesete napačno geslo, boste ponovno vprašani zanj, ko kliknete **Naprej**. Kliknite **V redu** za ponoven vnos gesla ali **Prekliči** za izhod iz čarovnika.

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

Kliknite **Naprej**.

Korak 4/5 - Vnos podatkov o računu

Konfiguracija računa Korak 4/5

Prosimo vas, da izpolnite podatke o računu. Podatki so zaupni. Če že imate račun, vam bo čarovnik izpolnil podatke, ki ste jih vnesli ob prvem kreiranju.

Ime:

Priimek:

Država:

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

< Nazaj Naprej > Prekliči

Podatki o računu



Opomba

Ta korak boste preskočili, če ste izbrali možnost **Preskoči ta korak** v **tretjem koraku**.

Vnesite vaše ime in priimek ter izberite državo, v kateri prebivate.

Če že imate račun, vam bo čarovnik prikazal vse predhodno vnešene podatke. Le-te lahko po potrebi popravite.

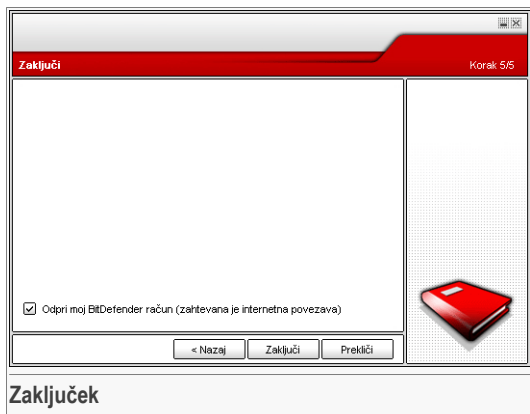


Pomembno

Vnešeni podatki so zaupne narave.

Kliknite **Naprej**.

Korak 5/5 - Povzetek



To je zadnji korak tega čarovnika. Tu lahko z vrnitvijo (klik na gumb **Nazaj**) spremenite katerokoli nastavitvev.

Če ne želite spremeniti karkoli, kliknite **Končaj** za zaprtje čarovnika.

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

6.5. O programu

Za dostop do teh možnosti kliknite zavihek **O programu** v modulu **Splošno**.



BitDefender Antivirus v10

Stanje
Nastavitve
Dogodki
Registracija
O programu

Splošno

Antivirus

Antispyware

Posodobitev

Informacije o izdelku

BitDefender Antivirus v10 - Različica 108
(c) 2001-2006 SOFTWIN. Vse pravice pridržane.

Kontakt

Spletna stran: www.parametica.si
E-pošta: prodaja@parametica.si
Telefon: +386 1 5657917
Faks: +386 1 5657918
Spletna stran: www.parametica.si

Tehnična podpora

Tehnična podpora: podpora@parametica.si
FAQ: <http://www.bitdefender.com/support/faq.htm>
KB: <http://kb.bitdefender.com/>

O programu BitDefender

BitDefender(tm) ponuja varnostne rešitve za zaščito sodobnih računalniških okolij. Uporablja ga več kot 41 milijonov domačih in poslovnih uporabnikov v več kot 180 državah.

BitDefender(tm) ima certifikate vseh večjih neodvisnih preizkuševalcev varnostnih rešitev - ICSA Labs, CheckMark in Virus Bulletin ter je tudi edini varnostni izdelek, ki je prejel IST nagrado.

Več pomoči
BitDefender

Splošne informacije

V tem razdelku lahko pregledate stanje vašega izdelka.

BitDefender nudi zaščito za zadovoljitev potreb po varnosti v današnjem računalniškem okolju. BitDefender tako ščiti že več kot 41 milijonov domačih in poslovnih uporabnikov v več kot 180 državah po vsem svetu.

BitDefender™ je testiran in certificiran v vseh pomembnejših organizacijah - **ICSA Labs**, **CheckMark** in **Virus Bulletin**, in je edini varnostni produkt, ki je dobil nagrado **IST Prize**.

Spletni klepet 24/7: <http://www.parametica.si>.



7. Modul Antivirus

Poglavje **Protivirusna zaščita** vsebuje naslednje teme:

- Skeniranje ob dostopu
- Skeniranje na zahtevo
- Karantena



Opomba

Za več informacij o **Protivirusna zaščita** si ogledajte del o *“Modul Antivirus”* (p. 27).

7.1. Skeniranje ob dostopu

Za dostop do teh možnosti kliknite zavihek **Zaščita** v modulu **Splošno**.

BitDefender Antivirus v10

Zaščita Skeniranje Karantena

Realnočasovna zaščita je omogočena

Zadnjič: nikoli Skeniraj zdaj

Nivo zaščite

Agresiven **PRIVZETO** - Standardna varnost, nizka poraba virov

- Skeniraj vse datoteke
- Skeniraj prihajajočo in odhajajočo e-pošto
- Skeniraj za virusi in vohunskimi programi
- Ne skeniraj internetnega (HTTP) prometa
- Dejanje ob okuženih datotekah: Očisti, Zavрни
- Skeniraj z B-HAVE (hevristična analiza)

Strpen

Statistika

Zadnja skenirana datoteka: c:\documents and settings\vdanciu\Recent\av Ink Več statistike

Promet 0 120 s

0s 50s

Zaščita v realnem času

Ta razdelek vsebuje najpomembnejše nastavitve realnočasovne zaščite ter statistiko. BitDefender skenira datoteke ob dostopu za virusi, vohunskimi programi in drugimi škodljivimi kodami.

Povlecite drsnik za izbiro želenih nastavitvev nivoja zaščite (za izbiro prednastavljene vrednosti) ali pa določite lastne nastavitve s pritisikom na gumb "Nivo po meri". Če niste prepričani, kaj bi izbrali, ohranite privzete nastavitve.


Več pomoči
 bitdefender
 PROTECT YOUR SYSTEM 2011

Realnočasovna zaščita

V tem razdelku lahko nastavite **Realnočasovna zaščita** in si ogledate informacije o njeni aktivnosti. **Realnočasovna zaščita** ščiti vaš računalnik s skeniranjem elektronske pošte, dolvleke spletnih vsebin in vseh odprtih datotek.

**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.

7.1.1. Nivoji zaščite

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

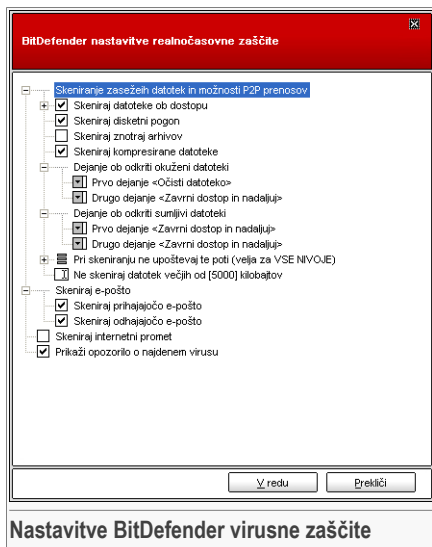
Na voljo so 3 stopnje zaščite:

Nastavitev nivoja zaščite	Opis
Dovoli	<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 analizador. Okužene datoteke se obravnava na način: očisti datoecko/zavrni dostop.</p>
Privzeto	<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 analizador. Okužene datoteke se obravnava na način: očisti datoecko/zavrni dostop.</p>
Agresivno	<p>Višja 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 analizador. Okužene datoteke se obravnava na način: očisti datoecko/zavrni dostop.</p>

Napredni uporabniki si želijo prednosti nastavljanja nastavitvev, 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**. Odrplo se bo sledeče okno:



Možnosti skeniranja so organizirane kot razširljiv meni, podoben tistim v Windows okolju.

Kliknite kvadrat s "+" za odprtje možnosti in kvadrat z "-", da zaprete možnost.

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
Skeniraj odprte datoteke	Skeniraj vse datoteke Skenirane bodo vse odprte datoteke.
Skeniraj izvršilne datoteke	Skeniraj le izvršilne datoteke 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.

Možnost	Opis
Skeniraj datoteke z definirano končnico	Skenirane bodo le datoteke s končnico, ki jo določi uporabnik. Končnice morajo biti ločene s podpičjem ";".
Končnice, ki so iz vzete iz skeniranja	Skenirane bodo vse datoteke razen tistih s končnico, ki jo določi uporabnik. Končnice morajo biti ločene s podpičjem ";".
Skeniraj za nevarnimi programi	Skenira za nevarnimi programi. Te datoteke bodo obravnavane kot okužene. Programi, ki vsebujejo reklamno vsebino, bodo morebiti prenehali delovati, ko bo ta možnost omogočena. Izberite Preskoči klicne dostope in aplikacije med skeniranjem , če želite izvzeti takšne datoteke iz skeniranja.
Skeniraj gibki disk ob dostopu	Skenira gibke diske, ob dostopu.
Skeniraj znotraj arhivov	Skenirane bodo tudi odprte arhivirane datoteke. Z omogočenjem teh možnosti boste upočasnili delovanje računalnika.
Skeniraj kompresirane datoteke	Skenirane bodo vse stisnjene datoteke.
Prva akcija	Izberete lahko eno izmed naslednjih dejanj:
Onemogoči dostop in nadaljuj	V primeru okužene datoteke, je dostop do te datoteke onemogočen.
Očisti datoteko	Očisti okuženo datoteko.
Izbriši datoteko	Brez opozorila izbriše okužene datoteke.
Premakni datoteko v Karanteno	Okužene datoteke so premaknjene v karanteno.
D r u g o dejanje	Izberite drugo dejanje.
Onemogoči dostop in nadaljuj	V primeru okužene datoteke, je dostop do te datoteke onemogočen.
Izbriši datoteko	Brez opozorila izbriše okužene datoteke.
Premakni datoteko v Karanteno	Okužene datoteke so premaknjene v karanteno.



Možnost	Opis
Ne skeniraj datotek večjih od[x] Kb	Vtipkajte največjo dovoljeno velikost datotek za skeniranje. Če je vnesena vrednost enaka 0 Kb, bodo skenirane vse datoteke.
Izvzemi poti iz skeniranja(velja za vse stopnje)	Kliknite "+" za izvzetje mape. Možnost se bo razširila v novo možnost <i>Nova zadeva</i> . Kliknite okno nove zadeve in izberite mapo, ki jo želite izvzeti. Izbrane mape, bodo izključene iz skeniranja, neglede na izbrano stopnjo zaščite (ne samo za Stopnja po meri).

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

Možnosti so naslednje:

Možnost	Opis
Skeniraj prihajajočo pošto	Skenira vso prihajajočo pošto.
Skeniraj odhajajočo pošto	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.

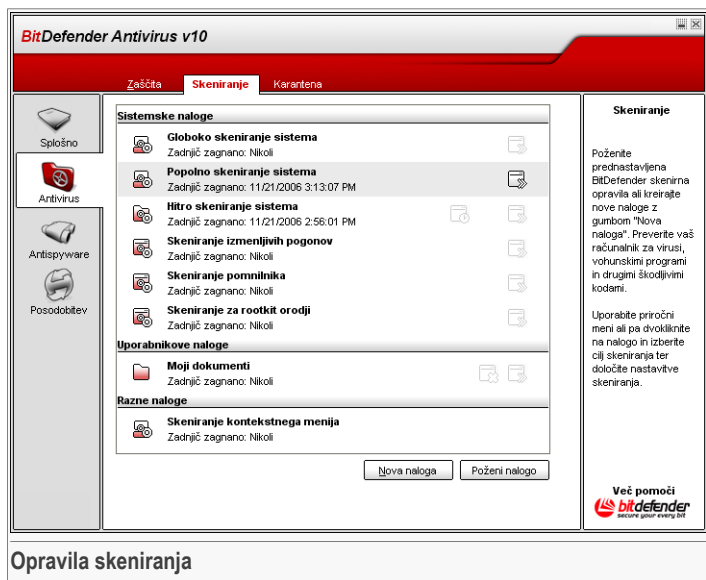
Ob odkriti sumljivi datoteki je v opozorilnem oknu moč pognati tudi čarovnika, ki vam bo pomagal poslati datoteko v BitDefender Laboratorij na dodatno analizo. Če vpišete svoj elektronski naslov, boste prejeli tudi dodatne informacije o poročilu.

Kliknite **Potrdi** za shranitev sprememb.

Če si želite vrniti na prednastavljeno stopnjo, kliknite **Privzeta stopnja**.

7.2. Skeniranje na zahtevo

Za dostop do teh možnosti kliknite zavihek **Skeniranje** v modulu **Antivirus**.



Tukaj se nahajajo nastavitve skeniranja, ki jih BitDefender uporablja na vašem računalniku.

Glavna BitDefender-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.

7.2.1. Opravila skeniranja

Možnost skeniranja na zahtevo ja osnovana na opravilih skeniranja. Uporabnik lahko pregleda računalnik z uporabo prednastavljenih opravil ali lastnih (uporabniško določena opravila).

Obstajajo tri kategorije opravil skeniranja.



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



Prednastavljena opravila	Opis
Globoko skeniranje	sistemsko Pregleda celoten sistem in vse arhive pred virusi in vohunskimi programi.
Popolno skeniranje	sistemsko Pregleda celoten sistem, razen arhivov, pred virusi in vohunskimi programi.
Hitro sistemsko skeniranje	Pregleda vse programe pred virusi in vohunskimi programi.
Skeniranje pogonov	zamenljivih Pregleda zamenljive pogone virusi in vohunskimi programi.
Skeniraj pomnilnik	Pregleda pomnilnik pred znanimi vohunskimi grožnjami.
Skeniraj pred rootkiti	Pregleda pomnilnik pred zlonamernimi kodami.

- **Uporabnikova opravila** - vsebije opravila, ki jih je definiral uporabnik.
Opravilo *Moji dokumenti* je na voljo. Uporabite to opravilo za skeniranje dokumentov iz mape *Moji dokumenti*.
- **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

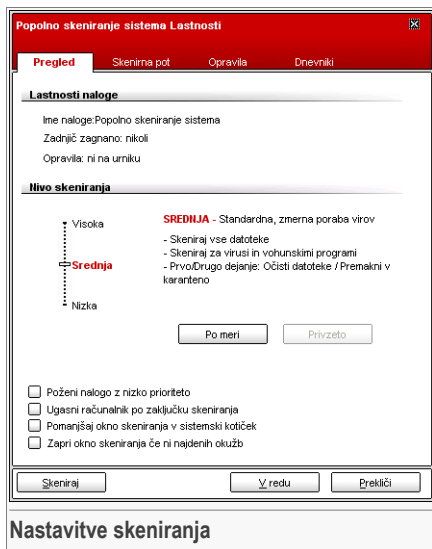
Ni na voljo za sistemska opravila. Ne morete odstraniti sisemskega opravila.

-  **Skeniraj** - prične izvajati opravila in poženetakojšnje skeniranje.

7.2.2. Nastavitve opravil skeniranja

Vsako opravilo skeniranja ima svoje **Lastnosti** okno, kjer lahko skonfigurirate nastavitve skeniranja, določite tarče skeniranja, določite poteke opravil ali pogledate sporočila. Za odprtje tega okna dvokliknite opravilo. Odprlo se vam bo sledeče okno:

Nastavitve skeniranja



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

Stopnja skeniranja

Najprej izberete stopnjo skeniranja. Povlecite drsnik po skali in izberite ustrezno stopnjo skeniranja.

Obstajajo 3 stopnje skeniranja:

Nastavitev nivoja Opis zaščite

Nizka	Zmerna učinkovitost detekcije. Majhna obremenitev sistema. Programi so pregledani pred virusi. Polek skeniranja na osnovi podpisov virusov, uporablja program tudi metodični analizator. Postopki z okuženimi datotekami so sledeči: očisti datoteko/premakni v karanteno.
Srednja	Dobra učinkovitost detekcije. Zmerna obremenitev sistema.



Nastavitev nivoja Opis zaščite

Programi so pregledani pred virusi in vohunskimi programi. Polek skeniranja na osnovi podpisov virusov, uporablja program tudi metodični analizator. Postopki z okuženimi datotekami so sledeči: očisti datoteko/premakni v karanteno.

Visoka

Visoka učinkovitost detekcije. Velika obremenitev sistema.

Programi so pregledani pred virusi in vohunskimi programi. Polek skeniranja na osnovi podpisov virusov, uporablja program tudi metodični analizator. Postopki z okuženimi datotekami so sledeči: očisti datoteko/premakni v karanteno.



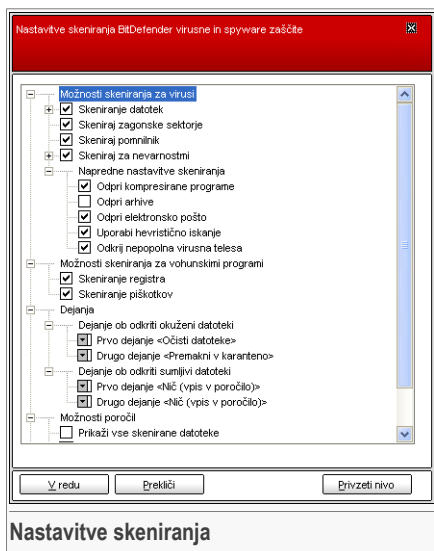
Pomembno

To **Skeniraj pred rootkit**-i opravilo ima enake stopnje skeniranja. Obstajajo različne možnosti:

- **Nizka** - skenirani so sam o procesi. Nobeno dejanje se ne izvrsi na zaznane objekte.
- **Srednja** - Skenirane so datoteke in procesi. Nobeno dejanje se ne izvrsi na zaznane objekte.
- **Visoka** - Datoteke in procesi so pregledani pred skritimi objekti. Zaznani objekti so preimenovani.

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 lastne nastavitve skeniranja. Odrplo se bo sledeče okno:



Možnosti skeniranja so organizirane kot razširljiv meni, podoben tistim v Windows okolju.

Možnosti skeniranja so zbrane v petih kategorijah:

- **Možnosti skeniranja za virusi**
- **Možnosti skeniranja za vohunskimi programi**
- **Možnosti dejanja**
- **Možnosti poročil**
- **Ostale možnosti**

Kliknite kvadrat s "+" za odprte možnosti in kvadrat s "-", da zaprete možnost.



Pomembno

Za **Skeniraj pred Rootkit-i** opravila so na voljo v teh kategorijah: **Možnosti skeniranja Rootkit**, **Možnosti poročil** in **Ostale možnosti**. Iz prve kategorije izberete kaj želite skenirati (datoteke ali spomin) in nastavite naloge, ki se bodo izvrševale na zaznanih objektih (**Nič (log objects)/Rename files**). Zadnji dve kategoriji sta identični spodaj opisani.

- 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**.



Možnost	Opis
Skeniraj datoteke	<p>vse Skenirane bodo vse odprte datoteke.</p> <p>Skeniraj le izvršilne datoteke 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.</p> <p>Skeniraj datoteke z d e f i n i r a n o končnico Skenirane bodo le datoteke s končnico, ki jo določi uporabnik. Končnice morajo biti ločene s podpičjem ",".</p> <p>Izvzemi datoteke s končnico Skenirane bodo vse datoteke razen tistih s končnico, ki jo določi uporabnik. Končnice morajo biti ločene s podpičjem ",".</p>
Skeniraj zagonske sektorje	Skenirani bodo zagonski sektorji.
Skeniraj pomnilnik	Skenira pomnilnik pred virusi in ostalimi zlonamernimi programi.
Skeniraj za nevarnostmi	<p>Skenira za drugimi grožnjami poleg virusov kot npr klicalniki in reklamnimi programi. Te datoteke bodo obravnavane kot okužene. Programi, ki vsebujejo reklamno vsebino, bodo morebiti prenehali delovati, ko bo ta možnost omogočena.</p> <p>Izberite Izvzemi aplikacije ali klicne povezave , če želite izvzeti takšne datoteke.</p>
Napredne možnosti skeniranja	<p>O d p r i k o m p r e s i r a n e p r o g r a m e Skenirane bodo stisnjene datoteke.</p> <p>Odpri arhive Skenirane bodo arhivske datoteke.</p> <p>Odpri arhive elektronske pošte Skeniran bo e-poštni arhiv.</p> <p>Uporabi metodično iskanje Uporabljeno bo metodično skeniranje datotek. Cilj tega skeniranja je odkriti še neznane</p>

Možnost	Opis
	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.
Išči viruse	nepopolne Zaznava nepopolnih virusov.

- Določite cilj skeniranja za vohunskimi datotekami (procesi, piškotki in pomnilnik). Vse to poteka z izbiranjem določenih možnosti iz kategorije **Možnosti skeniranja za vohunskimi programi**.

Možnost	Opis
Skeniraj register	Skenira vnose v register.
Skeniraj piškotke	Skenira datoteke piškotkov.

- Določite dejanje ob odkriti okuženi ali sumljivi datoteki. Odprite možnosti pod **Možnosti dejanja** za pregled vseh možnosti.

Izberite dejanja ob odkriti okuženi ali sumljivi datoteki. Za okužene ter sumljive datoteke lahko določite različna dejanja. Izberete lahko tudi drugo dejanje, če je prvo neuspešno.

Dejanje	Opis
Nič (vpis v poročilo)	Nobeno dejanje ne bo uporabljeno pri okuženih datotekah. Datoteke bodo prikazane v poročilu.
Poziv uporabnika za izbiro dejanje	Ko bo odkrita okužena datoteka, se bo odprlo novo okno, kjer boste lahko izbirali, kaj želite storiti. Glede na pomembnost datoteke lahko izberete, da jo BitDefender očisti, izolira, izbriše ali premakne v karanteno.
Očisti datoteke	Očisti okuženo datoteko.
Izbriše datoteke	Brez opozorila izbriše okužene datoteke.
Premakni datoteke v karanteno	Premakne okužene datoteke v karanteno.



Dejanje	Opis
Preimenuj datoteke	Spremeni končnico okuženim datotekam. Nova končnica je: <code>.vir</code> . S preimenovanjem datotek se onemogoči sposobnost zaganjanja in širjenja virusa. Obenem so take datoteke najbolj primerne za laboratorijsko analizo.



Pomembno

Preimenuj datoteke ima podoben učine na skrite datoteke (rootkiti). Nova končnica zaznanih datotek bo `.bd.ren`. S preimenovanjem zaznanih datotek se izniči možnost izvršitve in širjenja šptencialne infekcijem, prav tako pa ostajajo shranjene za nadaljnjo analizo.

- Določite možnosti za datoteke s poročili. Odprite **Možnosti poročil** za pregled vseh možnosti.

Možnost	Opis
Prikaži vse skenirane datoteke	Prikaže vse skenirane datoteke in njihov status (okužene ali ne). Ta možnost zelo upočasni vaš računalnik.
Izbriše prijave starejše od [x]dni	V tem polju lahko specificirate kako dolgo mora biti poročilo v Prijave skeniranja del. Izberite to možnost in določite nov časovni interval. Prednastavljeni interval je 180 dni.



Opomba

Poročila lahko vidite v odseku **Poročilo skeniranja** v delu **Lastnosti**.

- Določite preostale možnosti. Odprite možnost **Ostale možnosti**, kjer lahko izbirate med naslednjimi možnostmi:

Možnost	Opis
Pošlji sumljive datoteke v BitDefender laboratorij	Program vas bo po končanem skeniranju vprašal ali naj sumljive datoteke pošlje v analizo v BitDefender laboratorij.

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

Kliknite **Potrdi** za shranitev sprememb.

Izbira drugih možnosti

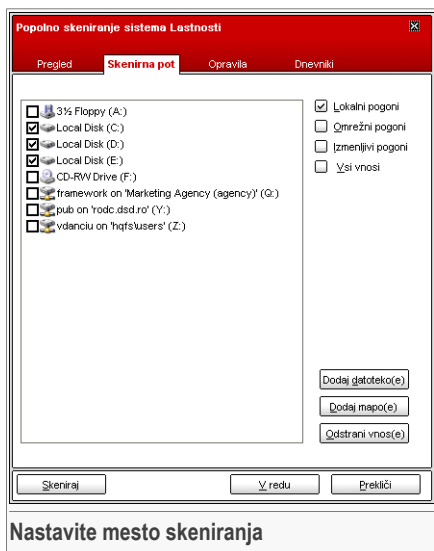
Na voljo je tudi več splošnih možnosti skeniranja:

Možnost	Opis
Poženi skeniranje z nizko prioriteto	Zmanjša prioriteto procesu skeniranja. To bo omogočilo hitrejše delo drugih programov in podaljšalo čas skeniranja.
Izklop računalnika po končanem skeniranju	Ugasne računalnik, ko se process skeniranja zaključi.
Pošlji sumljive datoteke v BitDefender laboratorij	Program vas bo po končanem skeniranju vprašal ali naj sumljive datoteke pošlje v analizo v BitDefender laboratorij.
Minimiranje skeniranja v sistemski kotiček	Minimira okno skeniranja v sistemski kotiček . Dvokliknite ikono BitDefender za ponovni prikaz.

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

Nastavite mesto skeniranja

Dvokliknite izbrano opravilo in nato kliknite **Poti skeniranja** za vstop v ta del.



Nastavite mesto skeniranja.

Ta del vsebuje naslednje gumbce:

- **Dodaj datoteko(e)** - odpre brskalno okno, kjer lahko izberete datoteke, ki jih želite skenirati.
- **Dodaj mapo(e)** - podobno kot zgornje, le da s tem gumbom izbirate mape namesto datotek.

Opomba



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

- **Odstrani vnos(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 vnosi**.

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

Načrtovalec

Dvokliknite izbrano opravilo in nato kliknite **Načrtovalec** za vstop v ta del.

Popolno skeniranje sistema Lastnosti

Pregled Skenirna pot **Opravlja** Dnevnik

Lastnosti

Opravila: vsake 7 dni, naslednje skeniranje: 11/21/2006 4:54:46 PM

Opravlja

ni na urniku

Enkrat

Periodično

Ob vsaki: 7 dni

Datum pričetka: 11/21/2006

Ura pričetka: 5:46 PM

Skeniraj V redu Preklici

Načrtovalec

Tukaj lahko vidite ali je opravilo bilo načrtovano in spremenite te nastavitve.



Pomembno

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.

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 **Start Datum/Čas**

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

Prijave skeniranja

Dvokliknite izbrano opravilo in nato kliknite **Prijave skeniranja** za vstop v ta del.

Popolno skeniranje sistema Lastnosti

Pregled Skenirna pot Opravitila **Dnevniki**

Stanje	Datum in čas	Povzetek
ni najdenih virusov	11/21/2006 2:03:55 PM	Skeniranje preklicano

Pokaži dnevnik Izbrisi dnevnik

Skeniraj V redu Preklici

Prijave skeniranja

Tukaj lahko vidite poročila istvarjena vsakič, ko je bila ustvarjeno novo opravilo. Vsako poročilo ima informacije o svojem statusu (očiščeno/okuženo), datum in točen čas skeniranja ter povzetek(skeniranje končano).

Na voljo sta dva gumba:

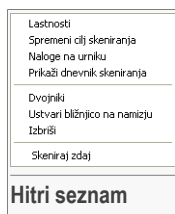
- **Prikaži prijave** - odpre izbrano poročilo.
- **Izbriši prijavo** - izbriše izbrano poročilo.

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**.

7.2.3. Hitri seznam

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



Možnosti so naslednje:

- **Lastnosti** - odpre okno **Lastnosti**, **Pregled** kjer lahko spreminjate nastavitve uzbranih opravil;
- **Spremeni mesta skeniranja** - odpre okno **Lastnosti Skeniraj poti**, kjer lahko spreminjate mesta skeniranja za izbrana opravila.
- **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.

- **Kreiraj bližnjico na namizju** - kreira bližnjico na namizju
- **Izbriši** - izbriše izbrano nalogo.



Opomba

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

- **Skeniraj sedaj** - takoj izvede izbrano nalogo in prične s takojšnjim skeniranjem.

**Pomembno**

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

7.2.4. Skeniranje na zahtevo

BitDefender ponuja 4 načine skeniranja na uporabnikovo pobudo/zahtevo:

- **Takojšnje skeniranje** - za skeniranje vašega računalnika za virusi prosimo sledite naslednjim korakom;
- **Vsebinsko skeniranje** - desni klik na datoteko ali mapo in izberite BitDefender Antivirus v10;
- **Povleci in izpusti skeniranje** - z načinom povleci in izpusti dodate datoteke ali mape v **Vrstica aktivnosti skeniranja**;

Takojšnje skeniranje

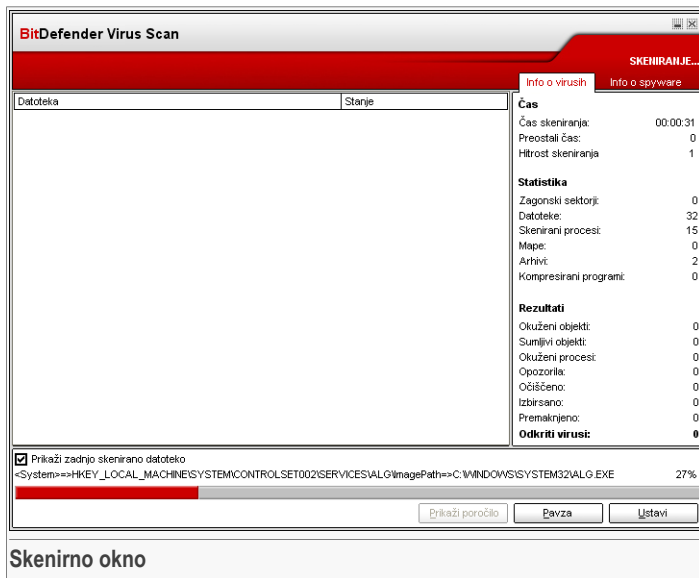
Za skeniranje vašega računalnika ali dela le tega, lahko uporabite predstavljenih opravil skeniranja ali pa ustvarite svoja opravila. Obstajata dva načina kako ustvariti opravilo skeniranja:

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

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

Preden ukažete BitDefender-ju da skenira celotni sistem, morate zagotoviti, da je BitDefender popolnoma posodobljen, z najnovejšimi protivirusnimi bazami, ker se novi virusi odkrivajo dnevno. Datum zadnje posodobitve lahko preverite v spodnjem delu modula **Posodobitev**.

Za pričetek skeniranja izberite opravilo skeniranja iz seznama in kliknite gumb **Skeniraj zdaj**. Kliknete lahko tudi **Izvrši opravilo**. Pojavilo se bo Skenirno okno



V **sistemski kotichek** se bo med skeniranjem pojavila ikona.

Med skeniranjem bo BitDefender prikazoval potek skeniranja in vas obvestil o morebitnih odkritih okužbah. Na desni strani lahko preverite statistiko skeniranja. Odvisno od cilja skeniranja pa so na voljo tudi podatki o vohunskih datotekah ter virusih. Če je na voljo več podatkov, kliknite na ustrezen zavihek za podrobnosti o procesu skeniranja.

Izberite kvadrata, ki pripada **Prikaži zadnje skenirano datoteko**, če želite, da vam BitDefender prikaže informacije o zadnji skenirani datoteki.



Opomba

Proces bo lahko trajal kar nekaj minut, odvisno od velikosti vašega trdega diska in števila datotek na njem.

Na voljo so trije gumbi:

- **Ustavi** - odpre novo okno, od kjer lahko končate proces skeniranja. Kliknite **Da** in **Zapri** za izhod iz okna skeniranja.
- **Pavza** - začasno ustavite skeniranje – nadaljujete s klikom na **Nadaljuj**.
- **Prikaži poročilo** - odprlo se bo poročilo o skeniranju.



Opomba

Če kliknete z desnim gumbom miške na delujoče opravilo, se bo pojavil hitri(vsebinski) seznam, ki vam bo omogočil uporabo skenirnega okna. Možnosti (**Pavza / Nadaljuj**, **Stop in Stop&Zapri**) so podobni gumbom v skenirnem oknu.

Če **Opozori uporabnika pred akcijo** Možnost se nahaja v **Lastnosti** oknu, ko je okužena datoteka zaznana se bo pojavilo opozorilno okno in vas vprašalo kakšno akcijo naj izvede.



Prikaže se ime datoteke in ime virusa.

Izberete lahko eno izmed naslednjih dejanj:

- **Očisti** - očisti okuženo datoteko;
- **Izbriši** - izbriše okuženo datoteko;
- **Premakni v karanteno** - premakne okuženo datoteko v mapo karantene;
- **Prezri** - prezre alarm. Okužena datoteka bo ostala nedotaknjena.

Če skenirate mapo in želite da bi dejanje veljalo za vse datoteke v mapi, omogočite **Uporabi za vse**.



Opomba

Če možnost **Očisti** ni na voljo, to pomeni, da datoteke ni mogoče očistiti. V takem primeru je najpametneje izolirati datoteko s premikom v karanteno in jo poslati v BitDefender-jeve laboratorije na podrobno analizo.

Kliknete **V redu**.

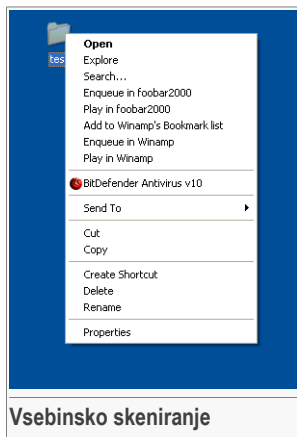


Opomba

Dokument s poročilom o skeniranju je samodejno shranjen v odseku **Poročilo skeniranja** v delu **Lastnosti**.

Vsebinsko skeniranje

Na datoteko, ki jo želite skenirati, kliknite z desnim miškinim gumbom in izberite **BitDefender Antivirus v10**.

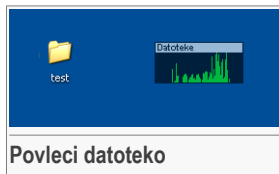


Vsebinsko skeniranje

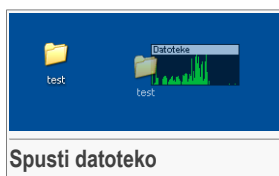
Spreminjate lahko možnosti skeniranja in pregleda poročil datotek z dostopom do okna **Lastnosti** v **Seznam vsebinskega skeniranja** task.

Povleci in izpusti skeniranje

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



Povleci datoteko



Spusti datoteko



Če je zaznana okužena datoteka se pojavi **opozorilno okno**, ki vas vpraša kakšno dejanje naj izvede na okuženo datoteko.

V obeh primerih se bo prikazalo **Skenirno okno**.

7.2.5. Skeniranje proti rootkitom

BitDefender je odgovor na najnovejše varnostne grožnje. Detektor Rootkit-ov, izredno učinkovit protivirusni in protivohunski modul. BitDefender sedaj odkrije rootkit-e z iskanjem skritih datotek, map ali procesov. Še več, lahko zaščiti vaš sistem s preimenovanjem slabih datotek ki uporabljajo rootkit-e.

Za skeniranje pred rootkit-i poženite **skeniraj za rootkit-i** opravilo. Pojavilo se bo skenirno okno.



Pomembno

Ko iščete rootkit-e vamm svetujemo, da nastavite BitDefender tako, da ne bo izvajal nobenih dejanj na skrite datoteke.

Po koncu skeniranja lahko pregledate rezultate. Če so bili zaznane skrite datoteke, jih pazljivo pregledajte: Prisotnost skritih datotek lahko nakazuje na možen vdor.

V kolikor ste prepričani, da so datoteke zlonamerne, vam priporočamo da nastavite **Preimenuj datoeke** akcijo in ponovno poženete **Skeniraj za rootkit-i** opravilo. Na ta način bodo skrite datoteke blokirane.



Pozor

NISO VSE SKRITE DATOTEKE ZLONAMERNE! Preden preimenujete skrito datoteko, se prepričajte, da ne pripadajo aplikacijam ali sistemu. Preimenovanje takih datotek lahko povzroči napake v delovanju sistema.

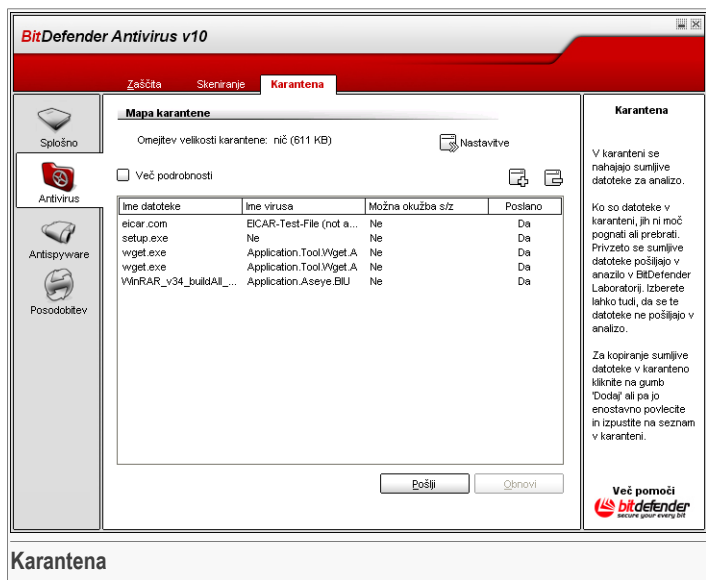


Pomembno

Če so vam vdrli v sistem, potem je samo ena varna pot, da se znebite vsiljivcev in sicer reinstalacija sistema.

7.3. Karantena

Za dostop do teh možnosti kliknite zavihek **Karantena** v modulu **Antivirus**.



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 pripomorete k hitrejšemu odkrivanju novih virusov.


Komponenta, ki omogoča nadzorovanje izoliranih datotek se imenuje **Karantena**. Modul je bil zasnovan s funkcijo za samodejno pošiljanje datotek v BitDefender-jeve laboratorije.

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 pognan ali prebran.

Kliknite  **Dodaj** Če želite datoteke dodati v karanteno. Če želite premakniti datoteko v karanteno, pa kliknite **Izbrši iz prvotne lokacije**. Hitrejša metoda je, da sumljive datoteke s funkcijo «povleci in izpusti» enostavno prestavite na seznam karantene.



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**.



Pomembno

Pred pošiljanjem morate podati še nekaj dodatnih informacij. Kliknite **Nastavitve** in izpolnite polja v odseku **Nastavitve pošiljanja obvestil** kot je prikazano spodaj.

Kliknite **Nastavitve**, da odprete napredne možnosti karantene. Pojavilo se bo naslednje okno:



Možnosti karantene so razporejene v dve kategoriji:

- **Nastavitve karantene**
- **Podnastavitve**



Opomba

Kliknite kvadrat s "+" za odprtje možnosti in kvadrat z "-", da zaprete možnost.

Nastavitve karantene

- **Omeji velikost mape Karantena** - nadzoruje velikost mape karantene. Privzeto je ta vrednost 12.000 KB. Če želite spremeniti to vrednost, vtipkajte novo vrednost v ustrezno polje. Če izberete možnost **Samodejno izbrisi stare datoteke**, bodo ob

dodajanju novih datotek v polno karanteno starejše datoteke samodejno izbrisane. S tem se bo naredil prostor za novo dodane datoteke.

- **Samodejno pošlji karanteno** - samodejno pošlje datoteke v karanteni v BitDefender-jeve laboratorije na podrobno analizo. V minutah lahko nastavite čas med pošiljanjem dveh zaporednih datotek v polju **Pošlji vsakih x minut**.
- **Samodejno izbriši poslane datoteke** - samodejno izbriše poslane datoteke takoj, ko so bile poslane v laboratorij na podrobno analizo.
- **'Povleci in spusti' nastavitve** - če uporabljate metodo Povleci in izpusti za dodajanje datotek v Karanteno, lahko tu določite, kaj naj se zgodi ob premiku.

Podnastavitve

- **Vaš e-naslov** - v primeru, da želite prejemati e-pošto od naših strokovnjakov, glede sumljivih datotek, ki ste jih poslali na analizo, vnesite vaš e-poštni naslov.

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



8. Modul Antispyware

Poglavje **Protivohunska zaščita** vsebuje naslednje teme:

- Stanje protivohunske zaščite
- Napredne nastavitve - Nadzor zasebnosti
- Napredne nastavitve-Nadzor registra
- Napredne nastavitve-Nadzor klicanja
- Napredne nastavitve-Nadzor piškotkov
- Napredne nastavitve-Nadzor skript
- Sistemske informacije

Opomba



Za več informacij o **Protivohunska zaščita** si oglejte izsek o "*Modul Antispyware*" (p. 27).

8.1. Status protivohunske zaščite

Za dostop do teh možnosti kliknite zavihek **Stanje** v modulu **Antispyware**.

BitDefender Antivirus v10

Stanje | Sistem

Protivohunska zaščita je omogočena

Modul varovanja zasebnosti je onemogočen Napredne nastavitve:

Nivo zaščite

- Agresiven **PRIVZETO**
 - Nadzor zasebnosti je onemogočen
 - Nadzor registra je omogočen
 - Nadzor klicanja je omogočen
 - Nadzor piškotkov je onemogočen
 - Nadzor skript je onemogočen
- Privzeto
- Strpen

Antispyware statistika

Blokirani zasebni podatki:	0
Blokirani vnosi v register:	0
Blokirani klicalniki:	0
Blokirani piškotki:	0
Blokirane skripta:	0

Antispyware nastavitve

BitDefender preverja številna mesta na vašem sistemu, kjer se lahko nahajajo vohunski programi in preverja za spremembami obstoječih programov.

Poznane vohunske programe blokira v realnem času, prav tako tudi piškotke in klicalnike.

Več pomoči
 bitdefender
 BODAC spolno varnost 2011

Status protivohunske zaščite

V tem odseku lahko nastavite modul **Zaščita pred nezaželeno pošto** in vidite informacije o njegovi aktivnosti.



Pomembno

Za preprečevanje vohunskim programom, da bi okužil vaš sistem, imejte **Behavioristična protivohunska zaščita** omogočeno.

Na dnu lahko vidite statistiko **Statistika protivirusne zaščite**.

Protivohunska zaščita zaščiti vaš računalnik preko petih kontrolnih točk.

- **Nadzor zasebnosti** - ščiti vaše zasebne podatke s filtriranjem odhajajočega HTTP in SMTP prometa po pravilih, ki ste jih ustvarili na delu [Zasebnost](#).
- 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.
- **nadzor klicanja** - zahteva vaše dovoljenje kadarkoli se želi telefon povezati na modem.
- 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](#).

8.1.1. Nivoji zaščite

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

Na voljo so 3 stopnje zaščite:

Nastavitev zaščite	nivoja	Opis
Dovoli		Omogočen je samo Nadzor registra
Privzeto		Omogočena sta Nadzor registra in Nadzor klicanja .
Agresivno		Omogočeni so Nadzor registra , Nadzor klicanja in Nadzor zasebnosti .

Nivo zaščite lahko spremenite s klikom na **Nivo po meri**. V oknu, ki se pojavi, izberite protivohunske ukrepe, ki jih želite omogočiti, in kliknite **V redu**.

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

8.2. Napredne nastavitve-nadzor zasebnosti

Za dostop do tega dela kliknite [Napredne nastavitve](#) v **Protivohunski zaščiti del Status**



Korak 1/3 - Določi vrste pravil in podatke

BitDefender čarovnik Korak 1/3

Ime pravila

Vrsta pravila

Podatki o pravilu

Vsi vnešeni podatki so kodirani. Za dodatno varnost ne vnašate popolnih podatkov, ki jih želite zaščititi.

< Nazaj Naprej > Prekliči

Nastavite tipe pravil in podatke

Vpišite ime pravila v polje za urejanje.

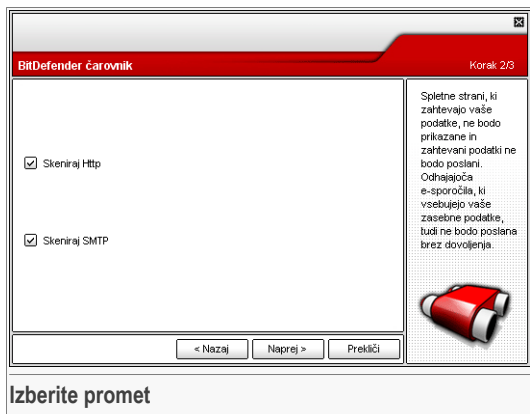
Nastaviti morate naslednje parametre:

- **Dejanje** - Izberite akcijo pravila in sledeče dogodke.
- **Podatki pravila** - Vnesite podatke o pravilu.

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 tip prometa, ki želite, da ga BitDefender skenira. Naslednje možnosti so na voljo:

- **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.

Kliknite **Naprej**.



Korak 3/3 – Opis pravila

BitDefender čarovnik
Korak 3/3

Opis pravila

kreditna kartica

Vnesite opis tega pravila. Opis bo vam ali drugim administratorjem pomagal odkriti, katere informacije blokirate.

◀ Nazaj
Zaključ
Prekliči

Opiše pravilo

Vnesite kratek opisa dovoljenja v polje za urejevanje.

Kliknite **Končaj**.

Tu lahko vidite pravila razporejena v tabelo.

Za izbrisanje pravila, ga izberite in kliknite **Izbriši**. Za začasno ustavev pravila, brez, da bi ga izbrisali označite okence pred pravilom.

Za urejanje pravila ga izberite in kliknite gumb **Uredi** ali dvokliknite pravilo. Pojavi se naslednje okno:

BitDefender čarovnik
Korak 3/3

Ime pravila

Vrsta pravila

Podatki o pravilu

Skeniraj http promet

Skeniraj Sntp promet

Opis pravila

kreditna kartica

V redu
Prekliči

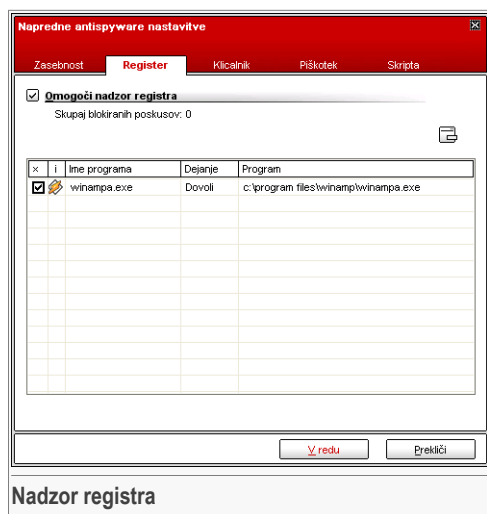
Uredite pravilo

Tukaj lahko spremenite ime, opisin parametre dovoljenj(tip, podatki, promet). Kliknite **V redu**

Kliknite **Potrdi** za shranitev sprememb.

8.3. Napredne nastavitve-Nadzor registra

Za dostopdo tega dela kliknite **Napredne nastavitve protivohunske zaščite** (pojdite na **Protivohunska zaščita Status** in kliknite  **Napredne nastavitve**)in kliknite**Registry**

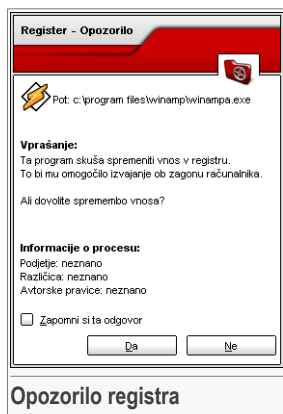


Nadzor registra

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.




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 kvadratka: **Zapomni si ta odgovor**.



Opomba

Vaše odločitve bodo temelji seznama pravil.

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



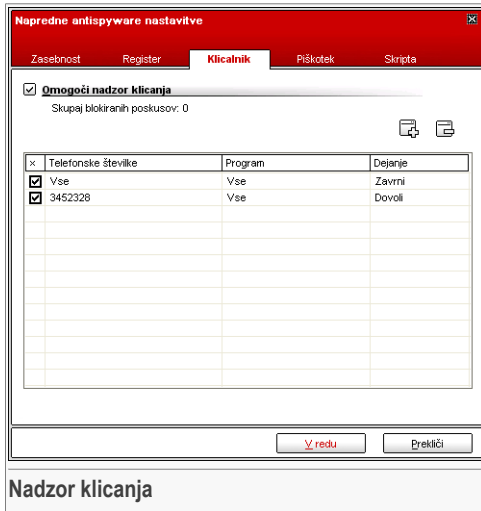
Opomba

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

Kliknite **V redu** da zaprete okno.

8.4. Napredne nastavitve-Nadzor klicanja

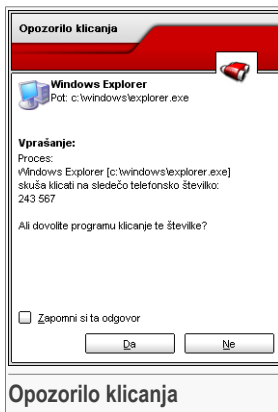
Za dostop v ta del kliknite **Napredne nastavitve protivohunske zaščite**(pojdite na **Protivohunska zaščita**Status in kliknite  **Napredne nastavitve**) in kliknite **Kliči**



Nadzor klicanja

Klicatelji so aplikacije, ki uporabljajo vaš modem za klicanje na oddaljene stacionarne številke brez vaše vrednosti in tako zelo povečajo vaš račun za telefon.

Z **Nadzor klicanja** nadzorujete vse povezave, ki jih vršijo različni programi. Ta funkcija nadzoruje računalniški modem in uporabnika takoj obvesti, ko želi neka aplikacija vzpostaviti povezavo na katerokoli številko. BitDefender vas prosi za potrditev / zavrnitev v sledečem oknu:



Opozorilo klicanja

Okno prikazuje ime aplikacije in telefonsko številko.

Izberite **Zapomni si ta odgovor** in izberite **Da** ali **Ne** in ustvarjeno bo novo pravilo o (ne)dovoljenih povezavah tega programa. Ko bo ta aplikacija ponovno želela vzpostaviti to povezavo, 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 **Kliči** in na voljo za dodatne nastavitve.



Pomembno

Pravila so podana v vrstnem redu po njihovi prioriteti, začeniš z vrha. Uporabite funkcijo Povleci in spusti pravila, če želite spremeniti vrstni red/prioriteto pravil.

Za izbris pravila, ga izberite in kliknite **Izbriši** . Za spreminjanje in nastavljanje pravila samo dvojno kliknite nanj. Za začasno ustaveitev pravila, brez, da bi ga izbrisali označite okence pred pravilom.

Pravila se lahko vnesejo avtomatsko (skozi opozorilno okno) ali ročno (kliknite gumb **Dodaj** in izberite parametre za pravilo). Odprl se bo čarovnik za nastavitve.

8.4.1. Čarovnik za nastavitve

Nastavitveni čarovnik ima 2 koraka.

Korak 1/2 - Izbira programa in dejanja

Nastavitve parametrov:

- **Aplikacije** - Izberite aplikacijo, ki se nanaša na to pravilo. Izberete lahko eno aplikacijo (kliknite **Izberi aplikacijo**, preiščite **Prebrskaj** in dodajte izbrano aplikacijo) ali vse aplikacije (kliknite **Vse**).
- **Dejanje** - Izberite katero dejanje naj pravilo izvrši.

Dejanje	Opis
Dovoli	Dejanje bo dovoljeno.
Zavrni	Dejanje bo zavrnjeno.

Kliknite **Naprej**.

Korak 2/2 - Izbira telefonskih števil

Izbira telefonskih števil

Izberite telefonsko številko

Vse
 Določi telefonsko številko

Izberite Vse če želite, da to pravilo velja za vse telefonske številke.

Ustvarite lahko tudi pravilo klicanja le določenih telefonskih števil, ki naj jih uporablja posamezen program (npr. za dostop do interneta ali faksirne naprave).

Izberite **Določi telefonsko številko** vnesite telefonske številke za katere želite, da pravilo neklicanja velja in kliknite **Dodaj**.



Opomba

Na seznamu blokiranih števil lahko uporabljate tudi zvezdice (*), na primer: 1900* (to pomeni da bodo blokirane vse številke, ki se začnejo z 1900).

Če označite možnost **Vse**, se bo to pravilo upoštevalo za vse številke. Če želite izbrisati številko, kliknite **Odstrani**.



Opomba

Ustvarite lahko tudi pravilo, ki dovoli določenemu programu klicanje samo določenih števil (naprimer ponudnik interneta ali storitev obveščanja po faksu).

Kliknite **Končaj**.

Kliknite **Potrdi** za shranitev sprememb.



8.5. Napredne nastavitve-Nadzor piškotkov

Za dostop do tega dela vstopite v **Napredna protivohunska zaščita** (pojdi na **Protivirusna zaščita Status** in kliknite  **Napredne nastavitve**) in kliknite **Piškotki**

Nadzor piškotkov

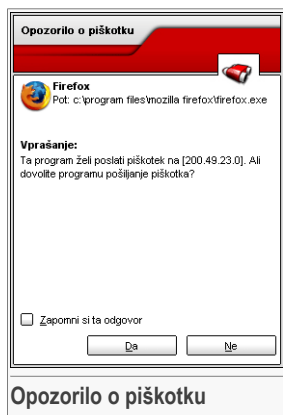
Smer	Domena	Dejanje	
<input checked="" type="checkbox"/>	Oboje	200.49.23.0	Dovoli
<input checked="" type="checkbox"/>	Oboje	gsp.ltraffic.ro	Dovoli
<input checked="" type="checkbox"/>	Oboje	ltraffic.ro	Dovoli
<input checked="" type="checkbox"/>	Oboje	140.251.103.1	Dovoli
<input checked="" type="checkbox"/>	Izhodni	Vse	Zavrne

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.

In 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:



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 **Nadzorom 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**.



Pomembno

Pravila so podana v vrstnem redu po njihovi prioriteti, začenši z vrha. Uporabite funkcijo Povleci in spusti pravila, če želite spremeniti vrstni red/prioriteto pravil.

Za izbris pravila, ga izberite in kliknite **Izbriši**. Za spreminjanje in nastavljanje pravila samo dvojno kliknite nanj. Za začasno ustavitev pravila, brez, da bi ga izbrisali označite okence pred pravilom.

Pravila se lahko vnesejo avtomatsko (skozi opozorilno okno) ali ročno (kliknite gumb **Dodaj** in izberite parametre za pravilo). Odprl se bo čarovnik za nastavitve.

8.5.1. Čarovnik za nastavitve

Nastavitveni čarovnik ima 1 korak.



Korak 1/1 - Izberite naslov, dejanje in smer


Izбира naslova, dejanja ter smeri
Korak: 1/1

Vnesi domeno

Vse

Vnesi domeno

Izberite spletne strani ter domene, katerih piškotke želite sprejeti ali zavrniti. Piškotki so uporabljani za hranjenje informacij o obisku in nastavitvah posameznih spletnih strani. Nekatere spletne strani ne bodo delovale pravilno brez uporabe piškotkov. Imate kakšna vprašanja?



Izberi ukaz

Dovoli

Zavrni

Izberi smer

Izhodni

Vstopni

Oboje

Izberite naslov, dejanje in smer

Nastavitve parametrov:

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

Dejanje	Opis
Dovoli	Dovoli izvajanje piškotkov izbrane domene.
Zavrni	Zavrne izvajanje piškotkov izbrane domene.

- **Smer** - izberite smer prometa.

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

Kliknite **Končaj**.

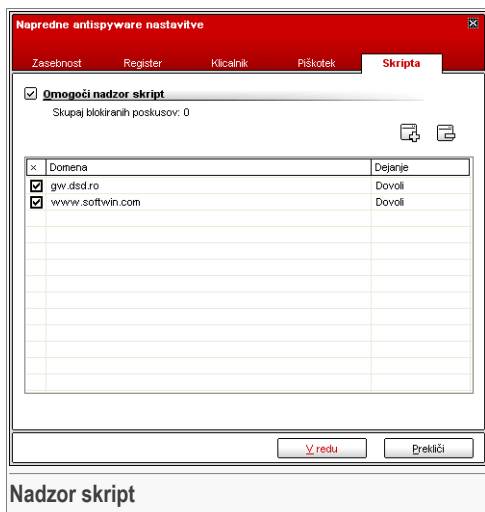
**Opomba**

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

Kliknite **Potrdi** za shranitev sprememb.

8.6. Napredne nastavitve-Nastavitve skripte

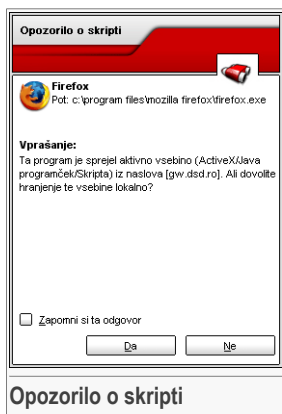
Za dostop do tega dela vstopite v **Napredne nastavitve protivirusne zaščite** (pojdite na **Protivirusna zaščita**, **Status** in kliknite **Napredne nastavitve**) **Skripta**.



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:



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**.



Pomembno

Pravila so podana v vrstnem redu po njihovi prioriteti, začenši z vrha. Uporabite funkcijo Povlec in spusti pravila, če želite spremeniti vrstni red/prioriteto pravil.

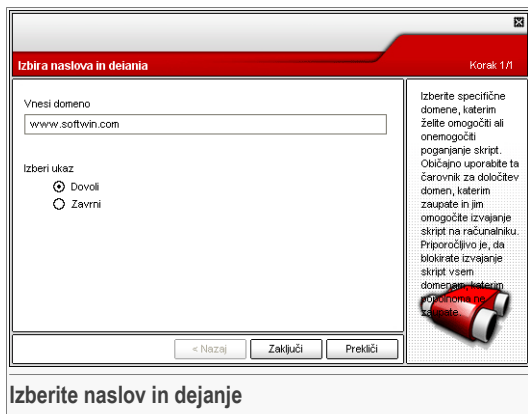
Za izbris pravila, ga izberite in kliknite  **Izbriši**. Za spreminjanje in nastavljanje pravila samo dvojno kliknite nanj. Za začasno ustavitev pravila, brez, da bi ga izbrisali označite okence pred pravilom.

Pravila se lahko vnesejo avtomatsko (skozi opozorilno okno) ali ročno (kliknite gumb  **Dodaj** in izberite parametre za pravilo). Odprl se bo čarovnik za nastavitve.

8.6.1. Čarovnik za nastavitve

Nastavitveni čarovnik ima 1 korak.

Korak 1/1 - Izbira naslova in dejanja



Nastavitve parametrov:

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

Dejanje	Opis
Dovoli	Skripte na tej domeni se bodo izvajale.
Zavrni	Skripte na tej domeni se ne bodo izvajale.

Kliknite **Končaj**.

Kliknite **Potrdi** za shranitev sprememb.

8.7. Sistemske informacije

Za dostop do teh možnosti kliknite zavihek **Informacije o sistemu** v modulu **Antispyware**.



BitDefender Antivirus v10

Stanje **O Sistemu**

Trenutne sistemske nastavitve

Storitve gonilnikov (100)

- Microsoft ACPI Driver
- Microsoft Kernel Acoustic Echo Canceller
- AFD
- Intel AGP Bus Filter
- RAS Asynchronous Media Driver
- Standard IDE/ESDI Hard Disk Controller
- ATM ARP Client Protocol
- Audio Stub Driver
- bdtdll
- BDFSDRV
- BDRSDRV**
- C-Dilla
- CD-ROM Driver

Tip zagona: Samodejno
 Objekt: Y??:C:\Program Files\Softwin\BitDefender10\bdrsdrv.sys
 Datoteka: bdrsdrv.sys
 Pot: C:\Program Files\Softwin\BitDefender10\bdrsdrv.sys
 No File Information: C:\Program Files\Softwin\BitDefender10\bdrsdrv.sys

[Odstrani] [Pojdi na] [Osveži]

Informacije o sistemu

Tukaj lahko vidite in spremenite vse ključne sistemske nastavitve: zagon in ugašanje sistema, zagnane procese, sistemske datoteke, zagnane servise.

Gre za kritične sistemske nastavitve, zato jih ne spreminjajte, če to ni resnično nujno potrebno.

Več pomoči
bitdefender
 Microsoft® - pravi partner

Sistemske informacije

Tu si lahko ogledate in spremenite ključne nastavitve.

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

Na voljo so trije gumbi:

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



9. Posodobitveni modul

Poglavje **Posodobitev** vsebuje naslednje teme:

- Samodejno posodabljanje
- Ročno posodabljanje
- Nastavitve posodobitev



Opomba

Za več informacij o **Posodabljanju** si oglejte izsek o "*Posodobitveni modul*" (p. 28).

9.1. Samodejno posodabljanje

Za dostop do teh možnosti kliknite zavihek **Posodobitev** v modulu **Posodobitev**.

BitDefender Antivirus v10

Posodobitev | Nastavitve

Samodejno posodabljanje je omogočeno

Zadnjič skenirano	11/21/2006 7:01:04 PM	
Zadnjič posodobljeno	11/21/2006 7:01:30 PM	Posodobiti zdaj

Lastnosti virusnih definicij

Virusni podatki	343853	
Različica pogona	7.10066	Seznam virusov

Stanje prenosa

Datoteka:	0 %	0 kb
Celotna posodobitev	0 %	0 kb

Posodobi BitDefender

Kliknite 'Posodobiti zdaj' za preverjanje novih posodobitev.

BitDefender izdelki so se zmogni samodejno popraviti, po potrebi tudi s prenosom poškodovanih datotek s spletnih strežnikov BitDefender.

Priporočamo, da imate vedno omogočeno možnost 'Samodejna posodobitev'.

Več pomoči
 bitdefender
 PROJEKT ZAŠTITE PRED VIRUSI

Samodejno posodabljanje


V tem razdelku lahko pregledate informacije v zvezi s posodobitvami.

**Pomembno**

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

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.

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.

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

9.2. Ročno posodabljanje

Ta metoda dovoljuje namestitev zadnjih virusnih definicij. Za namestitev posodobitve programa uporabite **Samodejno posodabljanje**.

**Pomembno**

Uporabite ročno posodabljanje, kadar samodejno posodabljanje ni na voljo, ali kadar računalnik ni priključen na omrežje (Internet).

Ročno posodabljanje lahko izvedete na dva načina:



- Z `weekly.exe` datoteko;
- Z `zip` arhivi.

9.2.1. Ročno posodabljanje z `weekly.exe`

Posodobitveni paket `weekly.exe` je izdan vsak petek in vsebuje vse nove protivirusne definicije in tehnike skeniranja, ki so na voljo v času izdaje.

Za posodobitev BitDefenderja z `weekly.exe` sledite naslednjim korakom:

1. Prenesite [weekly.exe](#) in ga shranite na disk.
2. Poiščite prenešeno datoteko in jo dvokliknite za zagon posodobitvenega čarovnika.
3. Kliknite **Naprej**.
4. Kliknite na okence pred **Sprejemem pogoje licenčnega sporazuma** in kliknite **Naprej**.
5. Kliknite **Namestitev**.
6. Kliknite **Končaj**.

9.2.2. Ročno posodabljanje z `zip` arhivi

Na strežniku za posodobitve se nahajata dve datoteki, ki vsebujeta vse nove protivirusne definicije in tehnike skeniranja: `cumulative.zip` in `daily.zip`.

- `cumulative.zip` je izdan vsak ponedeljek in vsebuje vse nove protivirusne definicije in tehnike skeniranja, ki so na voljo v času izdaje.
- `daily.zip` je izdan vsak dan in vsebuje vse nove protivirusne definicije in tehnike skeniranja, ki so na voljo v času izdaje.

Glede na to, da je BitDefender grajen na osnovi storitvene arhitekture, je procedura za zamenjavo virusnih definicij različna glede na operacijski sistem, ki ga uporabljate.

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP

Sledite naslednjim korakom:

1. **S spleta prenesite ustrezno posodobitev.** Če je ponedeljek, prosimo prenesite s spleta datoteko [cumulative.zip](#) in jo shranite na trdem disku. Sicer prenesite

datoteko [daily.zip](#) ter jo shranite na disku. Če je to vaša prva ročna posodobitev, prosimo prenesite obe datoteki.

2. Zaustavitev BitDefender protivirusne zaščite.

- **Zaprte BitDefender upravljalno konzolo.** Desno kliknite BitDefenderjevo ikono v [sistemskem kotičku](#) in izberite možnost **Izhod**.
- **Odprite storitev.** Kliknite **Start**, zatem **Nadzorna plošča**, dvokliknite **Skrbniška orodja** in kliknite **Storitev**.
- **Ustavite BitDefender Virus Shield storitev.** Izberite storitev **BitDefender Virus Shield** iz seznama in kliknite **Ustavi**.
- **Ustavite BitDefender Scan Server storitev.** Izberite storitev **BitDefender Scan Server** iz seznama in kliknite **Ustavi**.

3. Ekstrahirajte vsebino arhiva.

Začenši z `cumulative.zip` potem ko ste prenesli obe datoteki. Ekstrahirajte vsebino v mapo `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` in dovolite prepis obstoječih datotek.

4. Ponovno poženite BitDefender protivirusno zaščito.

- **Zaženite storitev BitDefender Scan Server.** Izberite storitev **BitDefender Scan Server** iz seznama in kliknite **Zaženi**.
- **Zaženite storitev BitDefender Virus Shield.** Izberite storitev **BitDefender Virus Shield** iz seznama in kliknite **Zaženi**.
- **Odprite [BitDefender upravljalno konzolo](#).**

Windows 98, Windows Millennium

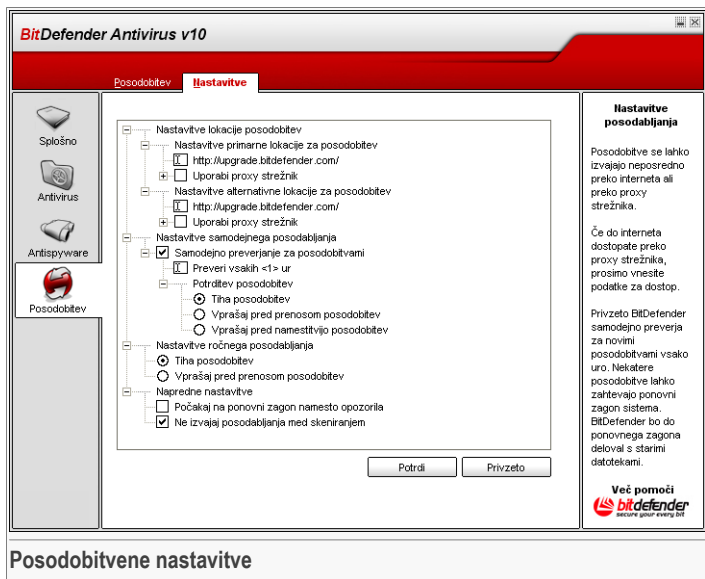
Sledite naslednjim korakom:

1. **S spleta prenesite ustrezno posodobitev.** Če je ponedeljek, prosimo prenesite s spleta datoteko [cumulative.zip](#) in jo shranite na trdem disku. Sicer prenesite datoteko [daily.zip](#) ter jo shranite na disku. Če je to vaša prva ročna posodobitev, prosimo prenesite obe datoteki.
2. **Ekstrahirajte vsebino arhiva.** Začenši z `cumulative.zip` potem ko ste prenesli obe datoteki. Ekstrahirajte vsebino v mapo `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` in dovolite prepis obstoječih datotek.
3. **Ponovno zaženite računalnik.**



9.3. Posodobitvene nastavitve

Za dostop do teh možnosti kliknite zavihek **Posodobitev** v modulu **Nastavitve**.



Posodobitve se lahko izvedejo preko lokalnega omrežja, preko interneta, direktno ali preko proxy strežnika.

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.



Opomba

Kliknite kvadrček "+", da možnost razširite in kvadrček "-", da jo zaprete.

9.3.1. Nastavitve lokacije posodobitev

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

- **Posodobitvena lokacija** - Če ste povezani v lokalno omrežje, ki ima Bitdefenderjeve podpise virusov shranjene lokalno, te nastavitve spremenite tu. Privzeta možnost je: <http://upgrade.bitdefender.com>.
- **Uporaba proxy strežnika** - V primeru, da podjetje uporablja proxy strežnik, kliknite to možnost. Potrebovali boste naslednje podatke:
- **Proxy nastavitve** - vpišite IP ali ime proxy strežnika in vrata, katera bo BitDefender uporabljal za dostop do strežnika.

**Pomembno**

Sintaksa: ime:vrata ali ip:vrata.

- **Uporabnik proxyja** - vpišite uporabniško ime, ki ga bo proxy strežnik prepoznal.

**Pomembno**

Sintaksa: domena\uporabnik.

- **Geslo proxyja** - vpišite veljavno geslo za prej navedenega uporabnika.

9.3.2. Možnosti samodejnega posodabljanja

- **Samodejno preverjanje za posodobitvami** - BitDefender avtomatično preverja Bitdefenderjeve strežnike za nove posodobitve.
- **Preveri vsake x ure** - Nastavitev, ki pove BitDefenderju na koliko časa naj preveri za nove posodobitve. Privzeti časovni interval je 1 ura.
- **Tiha posodobitev** - Bitdefender sam prenese in namesti posodobitve.
- **Vprašaj pred prenosom posodobitev** - vsakič, ko bodo posodobitve na voljo, vas bo program vprašal, pred prenosom.
- **Vprašaj pred namestitvijo posodobitev** - vsakič, ko bo posodobitev prenesena, vas bo program vprašal pred namestitvijo.

**Pomembno**

Če izberete **Vprašaj pred prenosom posodobitev** ali **Vprašaj pred namestitvijo posodobitev** in zaprete in **ugasnete** glavno okno, se avtomatično posodabljanje ne bo izvedlo.



9.3.3. Nastavitve ročnega posodabljanja

- **Tiha posodobitev** - ročno posodabljanje se bo izvedlo avtomatično in v ozadju.
- **Vprašaj pred prenosom posodobitev** - vsakič, ko boste izvedli ročno posodobitev, vas bo program vprašal pred prenosom in namestitvijo.



Pomembno

Če izberete **Vprašaj pred prenosom posodobitev** in zaprete in **ugasnete** glavno okno, se ročno posodabljanje ne bo izvedlo.

9.3.4. Napredne 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.

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



Uporaba v praksi



10. Uporaba v praksi

Poglavje **Optimalno delovanje** vsebuje naslednje teme:

- Kako zaščititi računalnik pred škodljivimi grožnjami
- Kako nastaviti opravila skeniranja

10.1. Kako zaščititi računalnik pred škodljivimi grožnjami



Sledite tem korakom za zaščito vašega računalnika pred virusi, vohunskimi programi in drugimi zlonamrnimi programi:

1. **Dokončajte namestitvenega čarovnika.** Med procesom namestitve se bo pojavil **čarovnik**. Pomagal vam bo registrirati BitDefender program in kreirati BitDefender račun z namenom pridobitve brezplačne tehnične podpore. Prav tako vam bo pomagal nastaviti BitDefender zaščito za opravljanje pomembnih varnostnih nalog.



Pomembno

Če imate BitDefender Rescue CD, preskenirajte vaš sistem pred namestitvijo BitDefender programa. S tem boste zagotovili, da se na vašem sistemu ne nahajajo morebitni škodljivi programi.

2. **BitDefender posodobitev.** Če niste dokončali namestitvenega čarovnika med procesom namestitve, opravite ročno posodobitev (odpravite se v modul **Posodobitev** v razdelek, **Posodobitev** in kliknite  **Posodobí zdaj**).
3. **Skeniranje celotnega sistema.** Odprite modul **Protivirusna zaščita**, razdelek **Zaščita** in kliknite  **Skeniraj zdaj**.



Opomba

Polno skeniranje sistema lahko poženete tudi v razdelku **Skeniranje**. Izberite možnost **Polno skeniranje sistema** in kliknite **Poženi nalogo**.

4. **Prepreči okužbo.** V razdelku **zaščita** ohranite **realnočasovno zaščito** omogočeno, saj vas le-ta ščiti pred virusi, vohunskimi programi in drugimi škodljivimi aplikacijami. Nastavite **nivo zaščite**, ki najbolj odgovarja vašim potrebam. Lahko ga **prilagodite** kadarkoli s klikom na **Nivo po meri**.

**Pomembno**

Nastavite vaš BitDefender Antivirus v10 tako, da bo skeniral sistem vsaj enkrat tedensko z zpeljavo **urnika** in izbiro možnosti **Polno skeniranje sistema** iz razdelka **Skeniranje**.

5. **Ohranite vaš BitDefender redno posodabljan.** V modulu **Posodobitev**, v razdelku **Posodobitev** ohranite **Samodejno posodabljanje** omogočeno, saj vaš ščiti pred najnovejšimi grožnjami.
6. **Nastavitev skeniranja celotnega sistema.** Odpravite se v razdelek **Skeniranje** in nastavite BitDefender **skeniranje vašega sistema** vsaj enkrat tedensko z **načrtovanje** v nalogi **Polno skeniranje sistema**.

10.2. Kako nastaviti opravila skeniranja

Sledite tem korakom za kreiranje in nastavitve nalog skeniranja:

1. **Kreiranje nove naloge.** Odpravite se v razdelek **Skeniranje** in kliknite **Novo opravilo**. Odprlo se bo okno **Lastnosti**.

**Opomba**

Novo nalogo lahko kreirate tudi s **podvajanjem** že obstoječe naloge. To naredite z desnim klikom in izbiro možnosti **Podvoji** iz menija bližnjic. Dvokliknite možnost **Podvoji** in odprlo se vam bo okno **Lastnosti**.

2. **Nastavitev nivoja skeniranja.** Odpravite se v razdelek **Pregled** in nastavite **nivo skeniranja**. Če želite, lahko **prilagodite** nastavitve skeniranja s klikom na **Po meri**.
3. **Nastavite mesto skeniranja.** Odpravite se na razdelek **Pot skeniranja** in izberite **stvari, ki jih želite skenirati**.
4. **Načrtuj opravila.** Če je naloga skeniranja kompleksna, jo morebiti želite nastaviti za kasnejši čas, ko npr. vaš računalnik miruje. To bo BitDefender-ju pomagalo opraviti natančno skeniranje vašega sistema. Odpravite se v razdelek **Opravila** pod možnost **načrjuj opravilo**.



BitDefenderjev reševalni CD

BitDefender Antivirus v10 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 vdelana 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.



11. Pregled

Prednosti

- Takojšnja e-poštna zaščita (Protivirusna zaščita/Zaščita pred nezaželjeno pošto)
- Antivirusna rešitev za vaš trdi disk
- NTFS projekt za zapisovanje
- Dezinfekcija okuženih datotek na Windows XP particijah

11.1. Kaj je KNOPPIX?

Citat iz <http://knopper.net/knoppix>:

“KNOPPIX is a bootable CD with a collection of GNU/Linux (<http://www.linux.com/>) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk.”

11.2. Sistemske zahteve

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

Tip 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

64 MB (priporočeno 128 MB).

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 Linuxdefender 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 kartica

Za normalen prikaz boste potrebovali grafično kartico, ki je sposobna prikazati vsaj resolucijo 800x600.

11.3. Vključena programska oprema

BitDefenderjev reševalni Cd vsebuje naslednje programske pakete.

- BitDefenderjev SMTP Proxy (Zaščita pred nezaželeno pošto in protivirusna zaščita)
- BitDefenderjev oddaljeni administrator (spletno osnovana konfiguracija)
- BitDefenderjeva Linux verzija (antivirus skener) + GTK vmesnik
- BitDefenderjeva dokumentacija (PDF in HTML format)
- BitDefenderjevi dodatki (Artwork in Leaflets)
- Linux-Kernel 2.6
- Prevzet NFTS projekt za zapisovanje
- LUFSS - Linux Userland File System
- Orodja za obnovitev in sistemska popravila, tudi za druge operacijske sisteme
- Omrežna in varnostno analizna orodja za omrežne administratorje
- Amanda – varnostno kopiranje
- thttpd
- Analizator omrežnega prometa, IPTraf IP LAN nadzornik
- Nessus omrežno varnostni nadzornik
- QTParted in partimage, razdeljevalec particij, shranjevalna in obnovitvena rešitev
- Adobe Acrobat Reader
- Mozilla Firefox spletni brskalnik

11.4. BitDefender Linux Security solutions

LinuxDefender CD vključuje BitDefenderjev SMTP Proxy Antivirus/Antispam za Linux, BitDefenderjevega oddaljenega administratorja (spletno osnovan vmesnik za konfiguracijo BitDefenderjevega SMTP Proxy) ter BitDefenderjevo Linux verzijo na zahtevo antivirus skeniranje.

11.4.1. BitDefenderjev SMTP Proxy

BitDefenderjev Linux strežnik za pošto - SMTP Proxy je zavarovana varnostna rešitev za pregled vsebine, ki zagotavlja antivirusno in antispam zaščito na nivoju prehoda, s skeniranjem vsega e-poštnega prometa, za vse vrste poznanih in nepoznanih zlo namernih kod. Kot rezultat edinstvene zaščitene tehnologije, je BitDefender za poštne strežnike kompatibilen z večino obstoječih e-poštnih platform in je potrjen, torej certificiran, s strani "RedHat Ready".



Te protivirusne rešitve in rešitve zaščite pred nezaželeno pošto skenira, dezinficira in filtrira ves poštni promet za vsak obstoječi poštni strežnik, ne glede na platformo in operacijski sistem. BitDefenderjev SMTP Proxy je zagnan ob zagonu sistema in skenira ves prihajajoči poštni promet. Za konfiguracijo BitDefenderjevega SMTP Proxya sledite navodilom spodaj.

11.4.2. BitDefenderjev oddaljeni administrator

BitDefenderjeve storitve lahko konfigurirate in upravljate preko oddaljenega administratorja (po konfiguraciji vašega omrežja), ali preko lokalnega sistema:

1. Zaženite Internetni brskalnik in naložite URL BitDefenderjevega oddaljenega administratorja: <https://localhost:8139> (ali dvokliknite ikono Bitdefenderjevega oddaljenega administratorja nanamizju)
2. Vpišite se z »bd« uporabniškim imenom in »bd« geslom
3. Izberite SMTP Proxy iz menija
4. Nastavite Real SMTP strežnik in vrata
5. Dodajte e-poštne domene k usmerjevalniku
6. Dodajte omrežne domene k usmerjevalniku
7. Izberite "Zaščita pred nezaželeno pošto" iz menija za nastavitve možnosti nezaželene pošte
8. Izberite "Protivirusna zaščita" iz menija za nastavitve protivirusnih možnosti (možnost akcije ob najdenem virusu, lokacija karantene)
9. Dodatno, lahko nastavite Obveščanje po pošti in vpisne možnosti (!logger)

11.4.3. BitDefenderjeva različica za Linux

Antivirusni skener vključen v LinuxDefender je integriran direktno v namizje. Ta verzija vsebuje GTK+ grafično okolje.

Pregledujte trde diske, ali priključene pomnilniške naprave na sistem, desno kliknite na katero koli datoteko, ali mapo izberite Skeniraj z BitDefenderjem. BitDefender bo pregledal izbrane elemente in prikazal poročilo. Za bolj natančne možnosti preglejte BitDefenderjevo Linux dokumentacijo in **/opt/BitDefender/lib/bdc**.



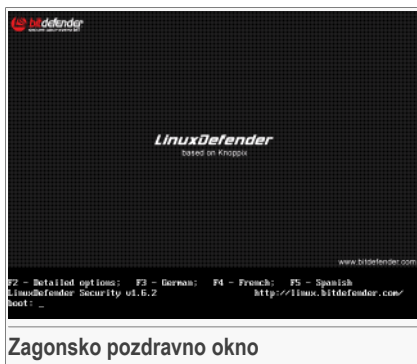
12. LinuxDefenderjev kako

12.1. Ustavitev in zagon

12.1.1. Zagon LinuxDefenderja

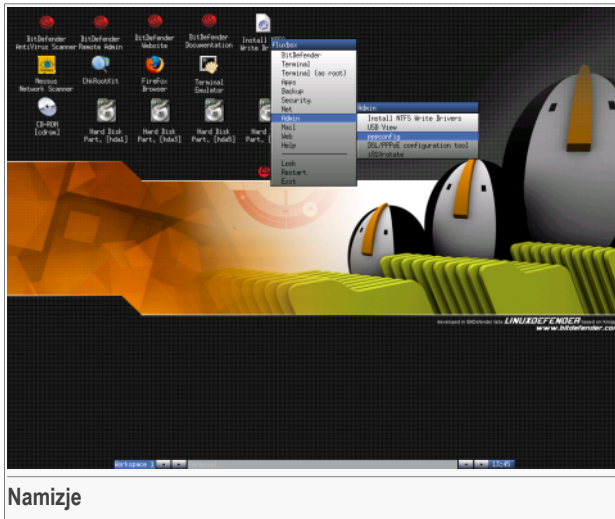
Za zagon CDja, nastavite BIOS, da se bo sistem zagnal s CD-ROMa, vstavite Cd v pogon in ponovno zaženite računalnik. Prepričajte se, da se vaš sistem lahko zažene s CD-ROMa.

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



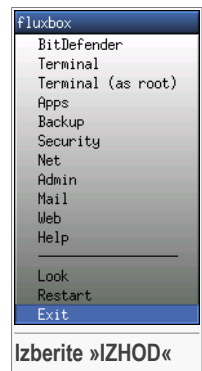
Pritisnite **F2** za izčrpne možnosti. Pritisnite **F3** za izčrpne možnosti v nemščini. Pritisnite **F4** za izčrpne možnosti v francoščini. Pritisnite **F5** za izčrpne možnosti v španščini. Za hiter zagon s privzetimi možnostmi pritisnite **ENTER**.

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



12.1.2. Ustavitev LinuxDefenderja

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.



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
Sent all processes the TERM signal.....
Sent all processes the KILL signal.....
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb unmounted
/randisk unmounted
could not mount /KNOPPIX - trying /dev/cloop instead
/dev/root unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.

```

Počakaj na to sporočilo ob ugašanju

12.2. Nastavitev Internetne povezave

Če ste v DHCP omrežju in dostopate do interneta preko omrežne kartice, bi se morala internetna povezava vzpostaviti samodejno ob zagonu. V primeru, da se to ne zgodi, lahko nastavite dostop ročno, s tem, da sledite naslednjim korakom.

1. Odprite LinuxDefenderjev meni (desni klik) in izberite ukaz **Terminal** za odprtje konzole.
2. Vtipkajte **netcardconfig** v odprto okno terminala za zagon konfiguracijskega orodja.
3. Če ste v DHCP omrežju, izberite **da** (če niste prepričani vprašajte omrežnega administratorja). Drugače si oglejte navodila spodaj.
4. Sedaj bi morala biti povezava nastavljena. Svoj IP naslov in nastavitve omrežne kartice si lahko ogledate, če vtipkate **ifconfig**.
5. Če imate statični IP naslov (ne uporabljate DHCP), izberite **Ne** pri DHCP vprašanju.
6. Sledite navodilom na zaslonu. Če niste prepričani, kaj morate napisati, se posvetujte z omrežnim administratorjem za podrobnosti.

V primeru, da so bile vse nastavitve pravilno konfigurirane, lahko preverite svojo povezavo s ping-anjem `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Če uporabljate klicno povezavo izberite **pppconfig** iz LinuxDefenderjevega administracijskega menija. Nato sledite navodilom na zaslonu.

12.3. BitDefenderjevo posodabljanje

BitDefender uporablja sistemski spomin za posodabljanje. Na ta način lahko posodobite podpise virusov, orodja za skeniranje ali podatkovne baze za antispam, četudi zaganjate sistem iz nespremenljivega medija, kot je CD.

Prepričajte se, da imate vzpostavljeno povezavo na internet. Nato odprite BitDefenderjev Oddaljeni administrator in izberite **Posodobitev** iz levega menija. Pritisnite **Posodobi zdaj**, da preverite za možne posodobitve.

Posledično lahko izvajate še druge ukaze za posodabljanje iz terminala.

```
# /opt/BitDefender/bin/bd update
```

Vsi procesi posodabljanje se zapišejo v dnevnik, ki si ga lahko ogledate z naslednjim ukazom.

```
# tail -f /ramdisk/BitDefender/var/log/bd.log
```

Če uporabljate Proxy za zunanjo povezavo, morate nastaviti Proxy nastavitve v **Posodobitve** meniju, zavihek **konfiguracija**.

12.4. Skeniranje za virusi

12.4.1. Kako dostopam do svojih podatkov?

Prevzet NFTS projekt za zapisovanje

NTFS bralna podpora je na voljo ob uporabi [NTFS pisni projekt](#). Za delovanje boste potrebovali 2 datoteki iz vaše Windows namestitve: `ntoskrnl.exe` in `ntfs.sys`. Trenutno so podprti samo Windows XP gonilniki, seveda pa lahko uporabite te gonilnike tudi za dostop do Windows 2000/NT/2003 particij.

Namestitev NTFS gonilnikov

Za dostop in pisanje na NFTS particije morate najprej namestiti NFTS gonilnike. Če uporabljate FAT particije in potrebujete samo dostop do branja vaših podatkov, enostavno priklopite particije in do njih dostopate kot do Linux particij.



Za dodajanje podpore za NTFS particije namestite gonilnike iz vašega trdega diska, USB ključev ali iz Windows Update. Priporočeno je, da uporabite gonilnike iz varnega vira, saj so lahko lokalni gonilniki okuženi z virusi, ali pokvarjeni.

Dvokliknite **Install NTFS Write Drivers** namizno ikono za zagon **BitDefender NTFS nameščevalec**. Izberite prvo možnost, če želite namestiti gonilnike iz lokalnega trdega diska.

Če so gonilniki na običajni lokaciji, uporabite **Hitro iskanje**, da najdete gonilnike.

Posledično lahko specificirate, kje so gonilniki nahajajo, lahko pa jih prenesete iz Windows Update SP1.

Gonilniki niso nameščeni na trdi disk pač pa jih LinuxDefender spravi v spomin za dostop do NTFS particij. Če program namesti dostop do particij, dvokliknite ikono diska na namizju in pregledujte vsebino. Za nadomestek Raziskovalca uporabite Midnight Commander iz LinuxDefenderja ali vpišite **mc** v konzoli.

12.4.2. Kako izvedem proivirusno skeniranje?

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.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Nato kliknite **SZačni skenirati**.

Če želite nastaviti protivirusne opcije, izberite **Nastavi protivirusno zaščito** zavihek iz levega dela programa.

12.5. Naredite takojšnji e-poštni filter

LinuxDefender lahko uporabite za ustvarjanje ad-hoc filtra za e-pošto, brez namestitve kakršne koli programske opreme na trdi disk, ali spreminjanja poštnega strežnika. LinuxDefender postavite pred svoj strežnik in mu dovolite, da skenira ves SMTP promet in ga nato preusmeri na pravi poštni strežnik.

12.5.1. Zahteve

Potrebovali boste osebni računalnik s Pentium 3 ali novejšo, vsaj 256 MB Rama in CD-Rom za zagon. LinuxDefender bo potreboval dostop do SMTP prometa namesto pravega poštnega strežnika. Je več načinov konfiguracije teh nastavitev.

1. Spremenite IP naslov vašega pravega poštnega strežnika in stari IP naslov dodelite LinuxDefenderju
2. Spremenite DNS zapise, tako, da bo MX vnos za vašo domeno kazal na Linuxdefenderja
3. Nastavite e-poštne odjemalce, da bodo uporabljali LinuxDefender kot SMTP strežnik
4. Spremenite nastavitve požarnega zidu, za pošiljanje naprej oziroma preusmerjanje vse SMTP povezave na Linuxdefenderja namesto na pravi e-poštni strežnik

LinuxDefenderjev Kako ne bo podal razlage za napake pri zgoraj navedenih možnostih. Za več informacij preglejte [Linux Networking guides](#) in [Netfilter documentation](#).

12.5.2. E-poštna filtracijska rešitev

Zaženite LinuxDefenderjev CD in počakajte, da bo X windows sistem delujoč.

Za konfiguracijo BitDefenderjevega SMTP Proxy, dvokliknite **BitDefender oddaljeni administrator** ikono na namizju. Odprlo se bo novo okno. Za uporabniško bđime in bđgeslo uporabite, za vpis v Bitdefenderjev Oddaljeni administrator.

Po uspešnem vpisu boste lahko spreminjali SMTP Proxy nastavitve.

Izberite **SMTP Proxy** za nastavitve, katerega izmed pravih e-poštnih strežnikov želite zaščititi pred neželeno pošto in virusi.

Izberite zavihek **E-poštne domene** za vnos vseh e-poštnih domen, za katere želite prejemati pošto.

Kliknite **Dodaj e-poštno domeno** ali **Dodaj domeno za okrnjeno pošto** in sledite navodilom na zaslonu.

Izberite zavihek **Omrežne domene** za vnos vseh omrežij, za katere želite usmerjati e-pošto.

Kliknite **Dodaj omrežno domeno** ali **Dodaj okrnjeno omrežno domeno** in sledite navodilom na zaslonu.

Izberite **Protivirusna zaščita** iz levega menija, za izbiro dejanja, ko je odkrit virus in za ostale antivirusne nastavitve.

Sedaj se ves SMTP promet skenira in filtrira strani BitDefenderja. Po privzetih nastavitvah se vsa okužena sporočila očistijo ali izbrišejo in vsa neželena sporočila,



ki jih skenira BitDefender, se označijo kot [NEZAŽELENA POŠTA] in pojavi se glava, kjer program ponudi uporabniku možnosti (X-BitDefender-Nezaželena pošta: Da/Ne), ki olajša uporabniku prepoznavnost.

12.6. Izvedite glavni nadzor omrežja

Poleg svojih zmožnosti za obnovo podatkov, filtriranja pošte in zaščite pred zlo namernimi kodami, je v Linuxdefenderja integriranih nekaj orodij, ki lahko izvedejo temeljit pregled in nadzor gostitelja in omrežja. Možna je tudi izvedba forenzičnih analiz okuženih sistemov, z uporabo varnostnih orodij, ki so integrirane v Linuxdefenderja. Preberite spodnje vrstice, da se seznanite, kako izvedete pregled in nadzor nad lokalnim gostiteljem in omrežjem.

12.6.1. Iskanje rootkit-ov

Preden začnete preverjati za varnostne luknje na omrežnih računalnikih, najprej preglejte, da LinuxDefender ni okužen. Izvedete lahko skeniranje za virusi, kot je opisano v **Skeniraj za Virusi** sekciji ali pa naredite pregled za Unixove Rootkite.

Najprej priklopite vse particije, dvokliknite njihove namizne ikone ali uporabite **priklopi** ukaz v konzoli. Nato dvokliknite **ChkRootKit** ikono da preverite vsebino CD-ja ali zaženite **chkrootkit** ukaz iz konzole s stikalom `-r NEWROOT`, kjer specificirate nov root direktorij.

```
# chkrootkit -r /dev/hda3
```

Če je rootkit orodje odkrito, ga bo program prikazal **POUDARJENO** z velikimi črkami.

12.6.2. Nessus - omrežni Skener

Nessus je najpopularnejši odprtokodni skener ranljivosti uporabljan v 75.000 organizacijah po vsem svetu. Mnoge največje organizacije znatno zmanjšujejo stroške z uporabo Nessusa za določanje poslovnih nevarnosti naprav in aplikacij v podjetju.

—www.nessus.org

Nessus je eden izmed najbolj priljubljenih odprto kodnih programov za preverjanje ranljivosti na svetu, ki ga uporablja preko 75.000 organizacij po vsem svetu. Veliko svetovnih organizacij se zaveda pomembnosti manjšanja izdatkov z uporabo Nessusa in zaščito proti škodljivim vdorom v njihove sisteme.

Dvokliknite **Nessus Varnostni skener** ikono na namizju ali vtipkajte **startnessus** iz Terminala. Počakajte na novo okno. Glede na vašo strojno opremo lahko traja do 10

minut, da se Nessus naloži skupaj z več kot 5000 vtičniki, ki vsebujejo baze podatkov o večini ranljivosti. Za uporabniško ime uporabite `knoppix` in `knoppix` za geslo, da se lahko povežete.

Kliknite zavihek **Target selection** in vnesite IP ali gostiteljsko ime računalnika, ki ga želite skenirati za ranljivosti. Prepričajte se, da ste nastavili vse možnosti skeniranja glede na vaše omrežje, ali konfiguracijo sistema, da si prihranite nepotrebne opcije skeniranja in čas, ter dobite bolj natančen rezultat. Nato kliknite **Start the scan**.

Ko se bo proces skeniranja končal, bo Nessus prikazal poročilo o najdenih ranljivostih in priporočila. Poročilo lahko shranite v več poljubnih formatov, med drugim tudi v HTML in si ga ogledate pozneje v internetnem brskalniku.

12.7. Preverite stanje delovnega spomina

Po navadi, kadar obnašanje sistema začne slabeti (se obesi, se samodejno ponovno zažene,...), je kriv sistemski spomin. Preverite lahko RAM čipe z **memtest** programom, kot je to opisano spodaj.

Zaženite vaš sistem z LinuxDefenderjem. Vtipkajte **memtest** pri zagonu in pritisnite Enter.

Program bo takoj začel preverjati pomnilniške enote in bo izvedel več testov za RAM enote. Prav tako lahko spremenite nastavitve za opcije, katere teste bo izvedel in ostale nastavitve s pritiskom na tipko `c`.

Popolni memtest lahko traja tudi do 8 ur, glede na količino rama in hitrosti. Priporočeno je, da izvedete vse teste za preverjanje vseh RAM pomnilniških enot. Prav tako lahko prekinete teste s pritiskom na tipko `ESC`.

Če se odločite za nakup nove strojne opreme (celotnega sistema, ali samo posameznih komponent), je priporočljivo, da uporabite LinuxDefender in memtest za pregled komponent in kompatibilnosti.



Pomoč



13. Podpora

13.1. Tehnična 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>. Za hitrejši odziv vam priporočamo, da v elektronsko pošto dodate čimveč podrobnosti o programu BitDefender, vašem sistemu in karseda natančno opišete težavo.

13.2. Pomoč na spletu

13.2.1. 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>.

13.3. Kontaktne informacije

Učinkovita komunikacija je ključ do uspeha. V zadnjih 10-ih letih je podjetje SOFTWIN 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>
Tehnična podpora: <podpora@parametica.si>
Dokumentacija: <documentation@bitdefender.com>
Partnerji: <partners@bitdefender.com>
Marketing: <prodaja@parametica.si>
Odnosi z javnostmi: <info@parametica.si>
Zaposlitvene priložnosti: <jobs@bitdefender.com>
Poročila o virusih: <virus_submission@bitdefender.com>
Poročila o neželenih vsebinah: <spam_submission@bitdefender.com>
Poročila o zlorabah: <abuse@bitdefender.com>
Spletna stran: <http://www.parametica.si>
FTP strežnik: <ftp://ftp.bitdefender.com/pub>
Lokalni distributerji: 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.

Nemčija

Softwin GmbH
Predstavništvo za zahodno evropo
Karlsdorferstrasse 56
88069 Tettngang
Nemčija
Telefon: 07542/94 44 44
Fax: 07542/94 44 99
E-pošta:<info@bitdefender.com>
Prodaja: <prodaja@parametica.si>
<http://www.parametica.si>
Tehnična podpora: <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>
Prodaja: <prodaja@parametica.si>
Splet: <http://www.bitdefender.co.uk>
Tehnična podpora: <podpora@parametica.si>

Španija

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

U.S.A

BitDefender, LLC
Dunajska 106
1000 Ljubljana
Tehnična podpora:
E-pošta: <support@bitdefender.com>
Podpora strankam: 01/565-79-17
<http://www.bitdefender.com>

Romania

SOFTWIN
5th Fabrica de Glucoza St.
Poštni predal 52-93
Bucharest
Tehnična podpora: <suport@bitdefender.ro>
Prodaja: <sales@bitdefender.ro>
Tel: +40 21 2330780
Fax: +40 21 2330763
Spletna stran produkta: <http://www.bitdefender.ro>



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 disket 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 računalnik, 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, tiskalnike, 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.

Nezaželjena 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 zastojnih 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.

Sistemske koticke

Sistemske koticke 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 nastavitvev.

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 priloženk 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.

