bitdefender
ANTIVIRUS v10

Uživatelská příručka

Antivirus

Antispyware

bitdefender
secure your every bit

BitDefender Antivirus v10

Uživatelská příručka

BitDefender

Vydáno 2007.03.12
Version 10.2

Právní oznámení


bitdefender
secure your every bit

Obsah

Licence a záruka

NESOUHLASÍTE-LI S PODMÍNKAMI TÉTO SMLOUVY, NEINSTALUJTE TENTO SOFTWARE. ZVOLENÍM "PŘIJÍMÁM", "OK", "POKRAČOVAT", "ANO" NEBO INSTALACÍ ČI JAKÝMKOLI POUŽÍVÁNÍM SOFTWARU DÁVÁTE NAJEVO, ŽE PLNĚ CHÁPETE A AKCEPTUJETE PODMÍNKY TÉTO SMLOUVY.

Tyto podmínky se vztahují na Vámi licencované řešení BitDefender a služby pro domácí uživatele, zahrnující související dokumentaci a jakoukoli aktualizaci aplikací dodanou skrze zakoupenou licenci nebo jakoukoli související smlouvu o službě stanovenou v dokumentaci nebo jakékoli její kopii.

Tato Licenční smlouva je právní smlouvou mezi Vámi (fyzickou či právní osobou) a společností SOFTWIN o použití výše jmenovaného softwarového produktu SOFTWINu, která zahrnuje počítačový software a může zahrnovat související média, tištěné materiály a "on-line" nebo elektronickou dokumentaci (dále označovanou jako "BitDefender"), přičemž všechny jeho části jsou chráněny mezinárodními autorskými právy a mezinárodními úmluvami. Instalací, kopírování nebo používáním BitDefenderu souhlasíte s tím, že jste vázáni s podmínkami této smlouvy.

Nesouhlasíte-li s podmínkami této smlouvy, neinstalujte nebo nepoužívejte BitDefender.

Licence BitDefender. BitDefender je chráněn autorskými právy a mezinárodními úmluvami o autorských právech, stejně jako ostatními zákony a úmluvami na ochranu duševního vlastnictví. BitDefender je licencovaný, nikoliv prodaný.

POSKYTNUTÍ LICENCE. SOFTWIN tímto Vám a pouze Vám poskytuje následující nevýhradní, limitovanou a nepřenosnou licenci na používání Bitdefenderu.

APLIKACE SOFTWARU. BitDefender můžete instalovat a používat na takovém počtu počítačů, na kolik uživatelů je vystavená licence. Můžete vytvořit jen jednu další kopii a to pouze pro účel zálohy.

DESKTOPOVÁ UŽIVATELSKÁ LICENCE. Tato licence platí na software BitDefender, který může být instalován na jediný počítač a který neposkytuje síťové služby. Každý prvotní uživatel může tento software instalovat na jediný počítač a může vytvořit jen jednu další kopii pro účel zálohy na jiné zařízení.

LICENČNÍ PODMÍNKY. Licencí garantované podmínky začínají datem, kdy instalujete, kopírujete nebo jinak použijete BitDefender a licence pokračuje pouze na počítači, na který byl původně instalován.

AKTUALIZACE. Pokud je BitDefender označen jako Aktualizovaná verze, musíte pro aktualizaci /v souladu s používáním BitDefenderu/ disponovat řádnou licencí na

používání produktu SOFTWIN. BitDefender označený jako Aktualizovaná verze nahrazuje a/nebo doplňuje produkt, který je bází pro takové aktualizace. Výsledný aktualizovaný produkt můžete používat pouze v souladu s podmínkami této Licenční smlouvy. Pokud je BitDefender aktualizací nějaké komponenty balíku softwarových programů, na které máte licenci jako na jediný produkt, může být BitDefender použit a přenesen pouze jako součást tohoto jediného balíku produktů a nesmí být oddělen pro použití na více než jednom počítači.

AUTORSKÉ PRÁVO. Všechna práva, tituly a zájmy vztahující se k BitDefenderu a všechna autorská práva k BitDefenderu (zahrnující mj. obrázky, fotografie, loga, animace, video, audio, hudbu, text a "applety" včleněné do BitDefenderu), průvodní tištěné materiály a veškeré kopie BitDefenderu jsou ve vlastnictví společnosti SOFTWIN. BitDefender je chráněn autorskými zákony a mezinárodními smlouvami. Proto musíte s BitDefenderem nakládat jako s jiným autorsky chráněným materiálem s jedinou výjimkou: BitDefender můžete instalovat na jiný počítač a zachovat tak originál pro zálohovací nebo archivační účely. Nesmíte kopírovat tištěné materiály provázející BitDefender. Veškeré autorské právní dokumenty musíte vytvářet a přikládat v původní formě ke všem kopiiím vytvořeným bez ohledu na médium nebo formu v níž se BitDefender vyskytuje. BitDefender nesmíte sublicencovat, pronajímat, prodávat nebo nabízet formou leasingu. Nesmíte provádět reverse funkcionalit, budovat, rekompilovat, rozebírat, vytvářet deriváty, modifikovat, překládat, nebo vyvíjet jakékoliv úsilí směrované k objevení zdrojového kódu BitDefenderu.

OMEZENÁ ZÁRUKA. SOFTWIN zaručuje, že médium, na němž je BitDefender distribuován, je bez vady po období 30 dnů od data dodání BitDefenderu. V případě poruchy během záruky hovoří ve Váš prospěch fakt, že SOFTWIN, na základě svého rozhodnutí, může vyměnit defektní médium proti stvrzence za poškozené médium, nebo nahradit peníze, které jste za BitDefender zaplatili. SOFTWIN nezaručuje nepoškoditelnost či bezchybnost BitDefenderu, nebo že chyby budou opraveny. SOFTWIN nezaručuje, že BitDefender splní Vaše požadavky.

KROMĚ JIŽ VÝSLOVNĚ UVEDENÉHO V TÉTO DOHODĚ, ODMÍTÁ TÍMTO SOFTWIN VEŠKERÉ DALŠÍ ZÁRUKY ZA BITDEFENDER, AŤ JIŽ VÝSLOVNÉ NEBO KONKLUDENTNÍ, S OHLEDEM NA PRODUKTY A PODPORU VZTAHUJÍCÍ SE K TĚMTO ČI JINÝM MATERIÁLŮM (HMOTNÝM ČI NEHMOTNÝM) NEBO SLUŽBÁM S NIMI DODÁVANÝM. SOFTWIN TÍMTO VÝSLOVNĚ ODMÍTÁ JAKÉKOLI KONKLUDENTNÍ ZÁRUKY, AŤ JIŽ VÝSLOVNÉ NEBO KONKLUDENTNÍ, VČETNĚ KONKLUDENTNÍCH ZÁRUK MERKANTABILITY, ZPŮSOBILOSTI KE ZVLÁŠTNÍMU ÚČELU NEBO NEPORUŠENÍ, SPRÁVNOSTI DAT, SPRÁVNOSTI OBSAŽENÝCH INFORMACÍ, SYSTÉMOVÉ INTEGRACE A NEPORUŠOVÁNÍ PRÁV TŘETÍCH STRAN, FILTROVÁNÍ, ZNEFUNKČŇOVÁNÍ NEBO ODTRAŇOVÁNÍ SOFTWARU TŘETÍCH STRAN, A TAKÉ SPYWARE, ADWARE, COOKIES, E-MAILY, DOKUMENTY, REKLAMY NEBO PODOBNÉ, ZE ZÁKONA VYCHÁZEJÍCÍ PRÁVO

POUŽÍVÁNÍ.TATO ZÁRUKA JE EXKLUSIVNÍ A „IN LIEU" PRO VŠECHNY OSTATNÍ ZÁRUKY, AŤ JIŽ VÝSLOVNÉ NEBO KONKLUDENTNÍ. TATO ZÁRUKA VÁM DÁVÁ SPECIFICKÁ PRÁVA. JE VŠAK MOŽNÉ, ŽE POŽÍVÁTE JINÁ PRÁVA, KTERÁ SE V JEDNOTLIVÝCH STÁTECH MOHOU LIŠIT.

ODMÍTNUTÍ ODŠKODNĚNÍ. Každý, kdo používá, testuje nebo hodnotí BITDEFENDER, přebírá veškerá rizika kvality a provozu BitDefenderu. V žádném případě není SOFTWIN odpovědný za škody všeho druhu, včetně přímých či nepřímých škod /bez limitace/ vyplývajících z použití, provozu nebo doručení BitDefenderu, dokonce ani kdyby byl SOFTWIN upozorňován na existenci nebo možnost takových škod. NĚKTERÉ STÁTY NEDOVOLUJÍ OMEZENÍ NEBO VYNĚTÍ ODPOVĚDNOSTI ZA NÁHODNÉ NEBO NÁSLEDNÉ ŠKODY, TAKŽE NĚKTERÁ VÝŠE UVEDENÁ OMEZENÍ NEBO VYNĚTÍ SE VÁS NEMUSÍ TÝKAT. V ŽÁDNÉM PŘÍPADĚ NEPŘEKROČÍ VYČÍSLENÍ ODPOVĚDNOSTI SOFTWINu VÝŠI PRODEJNÍ CENY, KTEROU JSTE ZA BITDEFENDER ZAPLATILI. Odmítnutí a omezení vyložená výše budou aplikována bez ohledu na to, zda akceptujete nebo používáte, hodnotíte nebo testujete BitDefender.

DŮLEŽITÉ UPOZORNĚNÍ PRO UŽIVATELE. DŮLEŽITÉ UPOZORNĚNÍ PRO UŽIVATELE. TENTO SOFTWARE NENÍ ODOLNÝ PROTI CHYBÁM A NENÍ DESIGNOVÁN NEBO ZAMÝŠLEN PRO POUŽITÍ V NEBEZPEČNÉM PROSTŘEDÍ VYŽADUJÍCÍM BEZCHYBNÝ VÝKON NEBO OPERACE. TENTO SOFTWARE NENÍ VHODNÝ PRO POUŽITÍ PŘI OPERACÍCH LETECKÉ NAVIGACE, NUKLEÁRNÍCH ZAŘÍZENÍ NEBO KOMUNIKAČNÍCH SYSTÉMŮ, ZBRAŇOVÝCH SYSTÉMŮ, PŘÍMÉ NEBO NEPŘÍMÉ ZÁCHRANNÉ SYSTÉMY, KONTROLU VZDUŠNÉHO PROVOZU NEBO APLIKACE ČI INSTALACE,KDE BY SELHÁNÍ MOHLO VÉST K SMRTI, VÁŽNÉ FYZICKÉ ÚJMĚ NEBO ŠKODĚ NA MAJETKU.

OBECNÉ. Tato smlouva se bude řídit rumunskými zákony a mezinárodními regulacemi a úmluvami o autorských právech. Výhradní jurisdikce a soudní rozhodování ve sporech, vyvstávajících z této Licenční smlouvy, může být v kompetenci rumunských soudů.

Ceny, náklady a poplatky za použití BitDefenderu se mohou bez předchozího upozornění změnit.

V případě neplatnosti kteréhokoliv ustanovení této smlouvy, nebude mít neplatnost tohoto ustanovení vliv na platnost zbývajících částí smlouvy.

BitDefender a loga BitDefenderu jsou obchodní známkou společnosti SOFTWIN. Všechny ostatní ochranné známky použité v produktu nebo přidružené materiály jsou ve vlastnictví příslušných majitelů.

Licence bude při porušení jakékoli její části okamžitě a bez předchozího upozornění ukončena. Jako důsledek ukončení smlouvy nebude možné požadovat od SOFTWINu

ani od prodejců BitDefenderu odškodnění. Po ukončení smlouvy zůstanou nadále v platnosti všechny podmínky týkající se omezení použití důverných informací.

SOFTWIN může tyto podmínky kdykoliv změnit a tyto upravené podmínky budou automaticky uplatňovány u odpovídajících verzí software s těmito upravenými podmínkami distribuovaného. Je-li jakákoli část těchto podmínek shledána neplatnou a nevynutitelnou, nebude to mít efekt na zbývající platné a vynutitelné části smlouvy.

V případě diskuze nebo rozporuplností mezi překlady této smlouvy do jiných jazyků, bude za jedinou správnou považována verze anglická, vydaná společnstí SOFTWIN.

Kontakt: SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, tel. č.: 40-21-2330780 nebo Fax:40-21-2330763, e-mailová adresa: <office@bitdefender.com>.

Předmluva

Tato příručka je určena všem uživatelům, kteří zvolili **BitDefender Antivirus v10** jako bezpečnostní řešení pro své osobní počítače. Informace uvedené v této knize jsou vhodné nejen pro počítačové odborníky, ale jsou přístupné každému, kdo umí pracovat pod Windows.

Tato kniha vám podrobně popíše produkt **BitDefender Antivirus v10**, společnost a tým, jenž program vytvořili, vás provedou instalačním procesem a naučí vás, jak jej správně nakonfigurovat. Najdete zde informace o tom, jak používat **BitDefender Antivirus v10**, jak aktualizovat, vyzkoušet a přizpůsobit svým představám. Naučíte se i jak z BitDefenderu dostat to nejlepší.

Přejeme vám příjemnou a užitečnou lekci.

1. Konvence použité v této knize

1.1. Typografické konvence

V knize bylo pro zlepšení čitelnosti použito několik textových stylů. Jejich význam je uveden v následující tabulce.

Vzhed	Popis
`sample syntax`	Syntaxe je psána písmem se `stejnou roztečí`.
http://www.bitdefender.com	Webové stránky jsou umístěny na externích HTTP nebo FTP serverech.
`<support@bitdefender.com>`	E-mailové zprávy jsou pro přehled o kontaktních informacích vložené v textu.
„Předmluva“ (str. xiii)	Toto je odkaz směřující na nějaké místo v dokumentu.
`filename`	Soubory a adresáře jsou psány písmem se `stejnou roztečí`.
option	Všechna nastavení jsou zvýrazněna **tučným** písmem.
`sample code listing`	Části kódů jsou psány písmem se `stejnou roztečí`.

1.2. Poznámky k textu

Poznámky jsou v textu graficky označeny, nabízejí vám ke stávajícímu odstavci dodatečné informace.

Poznámka

Poznámka je jen krátké shrnutí textu. Ačkoli ji můžete vynechat, mohou poznámky poskytnout cenné informace jako např. zvláštní funkce nebo odkaz na související téma.

Důležité

Toto vyžaduje vaši pozornost a není doporučeno toto přeskočit. Obvykle poskytuje ne rozhodující, avšak významné informace.

Varování

Toto je důležitá informace, se kterou byste měli zacházet se zvýšenou opatrností. Nic nezkazíte tím, budete-li se držet pokynů. Toto varování byste si měli přečíst a porozumět mu, jelikož popisuje něco velice choulostivého.

2. Uspořádání knihy

Kniha se skládá ze sedmi částí a obsahuje následující témata: O BitDefenderu, Instalace produktu, Popis a vlastnosti, Řídící konzole, Doporučený postup, Záchranné CD BitDefenderu a Odborná pomoc. Navíc obsahuje významový slovník a dodatky, které pomáhají objasnit různé aspekty BitDefenderu, jež by mohly způsobovat technické problémy.

O BitDefenderu. Krátký úvod do BitDefenderu.

Instalace produktu. Instrukce vás krok za krokem provedou instalací BitDefenderu na počítači. Toto je komplexní průvodce instalací **BitDefender Antivirus v10**. Počínaje nezbytnými předpoklady pro úspěšnou instalaci, jste stále vedeni v průběhu celého instalačního procesu. V případě, že byste potřebovali BitDefender odinstalovat, je na konci uveden proces odinstalace.

Popis a vlastnosti. BitDefender Antivirus v10 - vlastnosti a moduly.

Řídící konzole. Popis základní administrativy a údržby BitDefenderu. V kapitolách jsou podrobně popsána všechna nastavení **BitDefender Antiviru v10**, dále je zde vysvětleno, jak zaregistrovat produkt, jak otestovat váš počítač a jak vykonávat aktualizace.Jste naučeni jak nakonfigurovat a používat všechny moduly BitDefenderu.

Doporučený postup. Následujte tyto instrukce a udělejte pro svůj BitDefender to nejlepší.

Záchranné CD BitDefenderu. Popis Záchranného CD BitDefenderu. Pomáhá porozumět a používat možnosti nabízené tímto bootovatelným CD.

Odborná pomoc. Místo, kam byste se měli podívat, pokud nefunguje vše podle předpokladů.

Významový slovník. Slovník se vám pokusí vysvětlit některé technické a odborné výrazy, které můžete najít na stránkách tohoto dokumentu.

3. Vaše připomínky

Rádi uvítáme vaše připomínky k této knize. Testovali jsme a ověřeili všechny informace dle našich možností. Napište nám prosím o všech vadách, které naleznete v této knize, nebo jak byste ji zlepšili, abyste nám pomohli pro vás vytvořit co možná nejlepší dokumentaci.

Dejte nám vědět zasláním e-mailu na <documentation@bitdefender.com>.

Důležité

Piště prosím všechny vaše e-maily, vztahující se k dokumentaci, v angličtině. Jen tak bude komunikace účinná.

O BitDefenderu

1. Kdo je BitDefender?

BitDefender je vedoucí světový poskytovatel bezpečnostních řešení, které vyhovují dnešnímu počítačovému prostředí. Společnost nabízí jednu z nejrychlejší a nejefektivnjší řady bezbečnostního software, určujícího nové standardy prevence hrozeb, včasné detekce a ochrany. BitDefender poskytuje své produkty a služby více než 41 miliónům domácnostem a společnostem v takřka 180 zemích světa. Pobočky BitDefenderu jsou ve **Spojených státech**, **Spojeném království**, **Německu**, **Španělsku** a **Rumunsku**.

- Přináší antivirus, firewall, antispyware, antispam a rodičovskou kontrolu firemním i domácím uživatelům;
- Rozsah produktů Bitdefender je zamýšlen pro implementování do komplexních IT struktur (pracovní stanice, souborové servery, poštovní servery a brány) na platformách Windows, Linux a FreeBSD;
- Celosvětová distribuce, produkty jsou dostupné v 18ti jazycích;
- Snadno použitelný díky průvodci instalací, který uživatele provede instalačním procesem s minimem dotazů;
- Mezinárodně certifikované produkty: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, atd;
- Hodinová péče o zákazníky - tým péče o zákazníky je připraven 24 hodin denně, 7 dní v týdnu;
- Bleskově rychlá odpověď na nové počítačové útoky;
- Nejrychlejší detekce;
- Každou hodinu aktualizace virových signatur - automatické nebo naplánované akce poskytují ochranu proti nejnovějším virům.

1.1. Proč BitDefender?

Osvědčený. Nejlépe reagující antivirový výrobce. Pohotová reakce BitDefenderu v případě epidemie počítačových virů byla potvrzena i posledními propuknutími virů CodeRed, Nimda a Sircam, ale také Badtrans.B nebo dalších nebezpečných, rychle se šířících, záludných kódů. BitDefender byl první, kdo poskytl protiopatření proti těmto kódům a volně je zpřístupnil na internetu pro všechny poškozené. Nyní, s pokračující expanzí viru Klez - v různých verzích, se okamžitá antivirová ochrana stává stále více potřebnou pro jakýkoliv počítačový systém.

Inovační. Oceněný za inovaci Evropskou komisí a EuroCase. BitDefender byl prohlášen vítězem evropské ceny IST, oceněn Evropskou komisí a představiteli 18 akademií v Evropě. Nyní, v její osmileté tradici, se evropská cena IST stala oceněním pro nové produkty, které reprezentují nejlepší evropské inovace v oblasti informační technologie.

Komplexní. Pokryje každý jednotlivý bod vaší sítě, poskytujíc kompletní ochranu. Bezpečnostní řešení BitDefender pro podnikové prostředí uspokojí požadavky na ochranu dnešního obchodního prostředí. Umožňuje spravovat všechny komplexní hrozby, jež mohou ohrozit síť, od malých lokálních oblastí až po velké multi-servery, multi-platformové WANy.

Vaše neproniknutelná ochrana. Poslední hranice proti všem možným hrozbám pro váš počítačový systém. Jelikož detekce virů založená na kódové analýze nenabízela vždy dobré výsledky, implementoval BitDefender ochranu založenou na chování programů, které zajišťují ochranu proti nově vzniklým nebezpečím.

Toto jsou **náklady** jimž se organizace snaží vyhnout a kterým bezpečností produkty mají zabránit:

- Útoky Wormů (Červů)
- Ztráta spojení kvůli infikovaným e-mailům
- E-mailové selhání
- Čištění a obnova systému
- Ztráta produktivity koncových uživatelů, kvůli nedosažitelnosti systémů
- Hackerství a neoprávněné přístupy, které mohou způsobit velké škody

Některé současné **vývojové trendy a výhody** mohou být splněny použitím BitDefender bezpečnostní soupravy. Můžete tak:

- Zvětšit síťovou dostupnost zastavením šíření záludných kódových útoků (např. Nimda, Trojští koně, DDoS).
- Chránit vzdálené uživatele před útoky.
- Rychle snížit náklady na administrativu a prostor s BitDefender Enterprise centrální správou.
- Zastavit šíření škodlivých programů přes e-mail používáním BitDefender e-mailové ochrany v síťových serverech. Dočasným nebo permanentním blokováním připojení neautorizovaných, poškoditelných a nákladných aplikací.

Podrobnější informace o BitDefenderu můžete získat na stránkách: http://www.bitdefender.com.

Instalace produktu

2. Instalace BitDefender Antivirus v10

Sekce **Instalace BitDefender Antivirus v10** této uživatelské příručky obsahuje následující témata:

- Systémové požadavky
- Instalační kroky
- Průvodce počátečním nastavením
- Aktualizace
- Odstranění, oprava nebo modifikace BitDefenderu

2.1. Systémové požadavky

Pro zajištění správného fungování produktu, ověřte před instalací, zda jsou splněny následující systémové požadavky:

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

- Procesor Pentium II 350 MHz nebo vyšší
- Minimálně 128 MB paměti RAM (doporučeno 256 MB)
- Minimálně 60 MB volného místa na pevném disku
- Internet Explorer 5.5 (nebo vyšší)

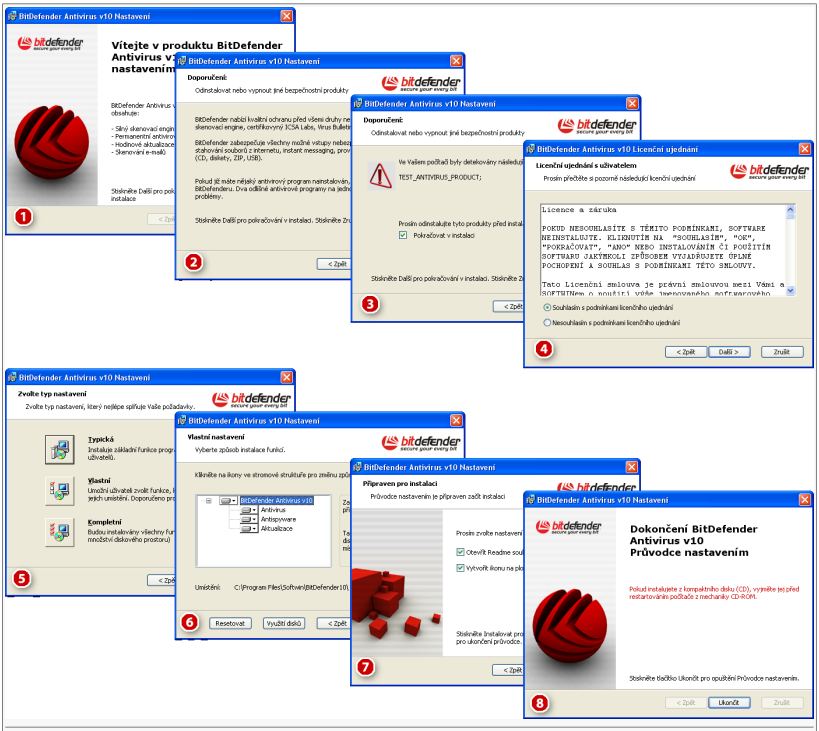
Microsoft Windows Vista 32-bit

- Procesor 800 MHz nebo rychlejší
- Minimálně 512 MB paměti RAM (doporučen 1 GB)
- Minimálně 60 MB volného místa na pevném disku

BitDefender Antivirus v10 může být pro vyzkoušení stáhnut ze stránky http://www.bitdefender.com, webové stránky společnosti SOFTWIN věnované bezpečnosti dat.

2.2. Instalační kroky

Najděte instalační soubor a poklepejte něj myší. Tím bude spuštěn průvodce, který vás bude provázet instalačním procesem.



Instalační kroky

1. Klikněte na **Další** pro pokračování nebo klikněte na **Zrušit** pokud chcete ukončit instalaci.
2. Klikněte na **Další** pro pokračování nebo klikněte na **Zpět** pro návrat k prvnímu kroku.
3. BitDefender Antivirus v10 vás bude varovat, pokud máte v počítači nainstalován jiný antivirový produkt.

Varování

Před instalací je doporučeno odinstalovat ostatní detekované antivirové produkty. Společný běh dvou či více antivirových produktů na počítači ve stejnou dobu může způsobit nestabilitu systému.

Klikněte na **Zpět** pro návrat na předchozí krok nebo na **Zrušit** pro ukončení instalace. Pokud chcete pokračovat, klikněte na **Další**.

Poznámka

Pokud BitDefender Antivirus v10 nedetekoval ve vašem počítači žádné jiné antivirové produkty, můžete tento krok přeskočit.

4. Přečtěte si Licenční ujednání, zvolte **Souhlasím s podmínkami Licenčního ujednání** a klikněte na **Další**. Pokud nesouhlasíte s těmito podmínkami, klikněte na **Zrušit**. Instalační proces bude opuštěn a instalace ukončena.
5. Můžete si zvolit jeden z druhů instalace: typická, vlastní, nebo kompletní.

   Typická
   Program bude nainstalován s nejčastěji užívanými volbami. Tato verze je doporučována většině uživatelů.

   Vlastní
   Můžete si vybrat kompotenty, které si přejete nainstalovat. Doporučeno pouze pro pokročilé uživatele.

   Kompletní
   Plná instalace produktu. Budou nainstalovány všechny moduly BitDefenderu.

   Pokud si zvolíte **Typická** nebo **Kompletní**, přeskočíte krok 6.
6. Pokud jste si vybrali **Vlastní**, objeví se nové okno obsahující všechny komponenty BitDefenderu a budete si moci zvolit ty, které si přejete nainstalovat.

   Při kliknutí na kteroukoliv komponentu se na pravé straně objeví krátký popisek (včetně informace o minimálním požadovaném místě na pevném disku). Kliknete-li na ikonu jakékoli kompenenty, zobrazí se okno, kde budete moci zvolit, zda chcete vybraný modul nainstalovat nebo ne.

   Můžete si zvolit složku, do níž chcete produkt instalovat. Výchozí složka je `C:\Program Files\Softwin\BitDefender 10`.

   Pokud chcete zvolit jinou složku, klikněte na **Procházet** a v okně, které se otevře, vyberte složku, do níž má být BitDefender Antivirus v10 nainstalován. Poté klikněte na **Další**.
7. Jako výchozí jsou nastaveny tyto volby:
   - **Otevřít soubor Čti mě** - na konci instalace se otevře soubor Čti mě.
   - **Vytvořit ikonu na ploše** - pro umístění zástupce BitDefenderu na plochu na konci instalace.

   Pro spuštění instalace klikněte na **Instalovat**.

Důležité

Během instalačního procesu bude spuštěn průvodce, který vám pomůže s registrací vašeho **BitDefender Antiviru v10**, vytvořením svého BitDefender účtu a nastavením a přípravou těch nejdůležitějších bezpečnostních úloh.
Pro pokračování k dalšímu kroku dokončete proces průvodce.

8. Klikněte na **Ukončit** pro dokončení instalace produktu. Pokud jste si zvolili výchozí nastavení instalační cesty, bude v `Program Files` vytvořena nová složka pojmenovaná `Softwin`, která obsahuje podsložku `BitDefender 10`.

Poznámka

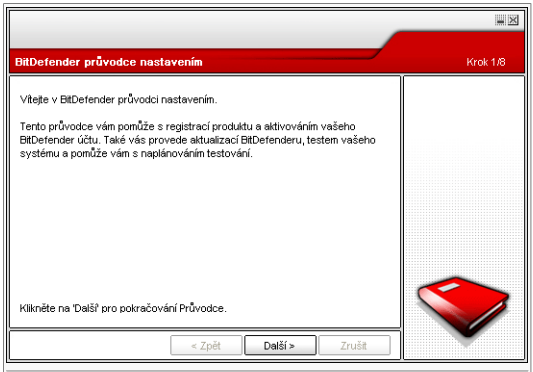
Možná budete požádáni, abyste pro dokončení instalačního procesu restartovali systém.

2.3. Průvodce počátečním nastavením

Během instalačního procesu bude spuštěn průvodce, který vám pomůže s registrací vašeho **BitDefender Antiviru v10**, vytvořením svého BitDefender účtu a nastavením a přípravou těch nejdůležitějších bezpečnostních úloh.

Dokončení tohoto průvodce není povinné; nicméně vám jeho dokončení doporučujeme, abyste tak ušetřili čas a zajistili bezpečí vašeho systému ještě před tím, než bude BitDefender Antivirus v10 nainstalován.

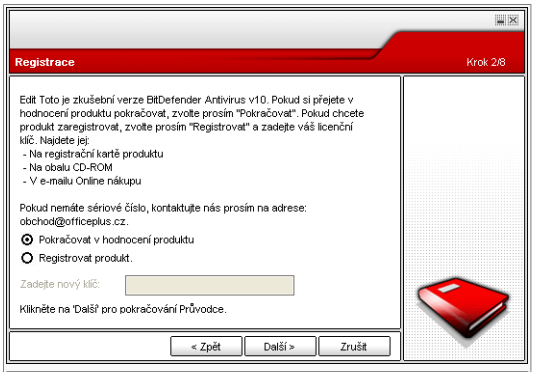
2.3.1. Krok 1/8 - BitDefender Průvodce počátečním nastavením



Uvítací okno

Klikněte na **Další**.

2.3.2. Krok 2/8 - Registrace BitDefender Antiviru v10



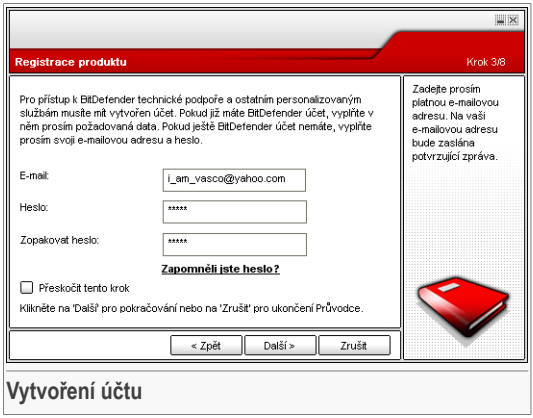
Registrace

Zvolte **Registrovat produkt** pro registraci **BitDefender Antiviru v10**. Licenční klíč zadejte v poli **Vložit nový klíč**.

Pro pokračování v hodnocení produktu zvolte **Pokračovat v hodnocení produktu**.

Klikněte na **Další**.

2.3.3. Krok 3/8 - Vytvoření BitDefender účtu



Vytvoření účtu

Nemám BitDefender účet

Pro získání bezplatné BitDefender technické podpory a dalších zdarma dostupných služeb musíte mít vytvořen účet.

Do pole **E-mail** zadejte platnou e-mailovou adresu. Zvolte si heslo a zadejte jej do pole **Heslo**. Heslo potvrďte přepsáním do pole **Zopakovat heslo**. Použijte tuto e-mailovou adresu a heslo pro přihlášení se do vašeho účtu na http://myaccount.bitdefender.com.

Poznámka

Heslo musí obsahovat alespoň čtyři znaky.

Pro úspěšné vytvoření účtu musíte nejprve aktivovat vaši e-mailovou adresu. Zkontrolujte vaši e-mailovou adresu a následujte instrukce, které naleznete v přijaté zprávě, odeslané pomocí Bitdefender registrační služby.

Důležité

Před přechodem na další krok prosím aktivujte svůj účet.

Jestliže nechcete vytvořit Bitdefender účet, klikněte na **Přeskočit tento krok**. Přesunete se tak na další krok v průvodci.

Klikněte na **Další** pro pokračování nebo klikněte na **Zrušit** pro ukončení průvodce.

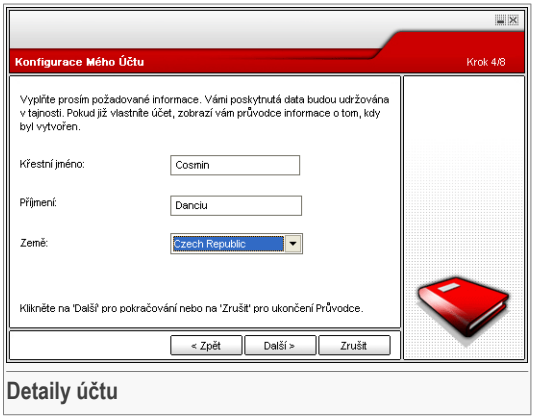
Již mám BitDefender účet

Pokud již máte aktivní účet, zadejte e-mailovou adresu a heslo vašeho účtu. Pokud zadáte neplatné heslo můžete jej opravit kliknutím na **Další**. Klikněte na **OK** pro znovuzadání hesla nebo na **Zrušit** pro ukončení průvodce.

Pokud jste zapomněli své heslo, klikněte na **Zapomněli jste heslo?** a následujte instrukce.

Klikněte na **Další** pro pokračování nebo klikněte na **Zrušit** pro ukončení průvodce.

2.3.4. Krok 4/8 - Zadání údajů účtu



Detaily účtu

Poznámka

Pokud jste zvolili **Přeskočit tento krok** ve třetím kroku průvodce, nemůžete do tohoto kroku průvodce vstoupit.

Vyplňte své křestní jméno a příjmení a zvolte zemi, ve které žijete.

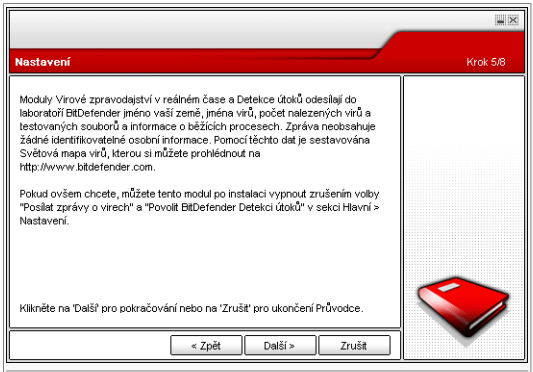
Pokud již máte účet, průvodce zobrazí informace, které jste v minulosti poskytli, jsou-li nějaké.

Důležité

Data, která zde poskytnete, zůstávají důvěrná.

Klikněte na **Další** pro pokračování nebo klikněte na **Zrušit** pro ukončení průvodce.

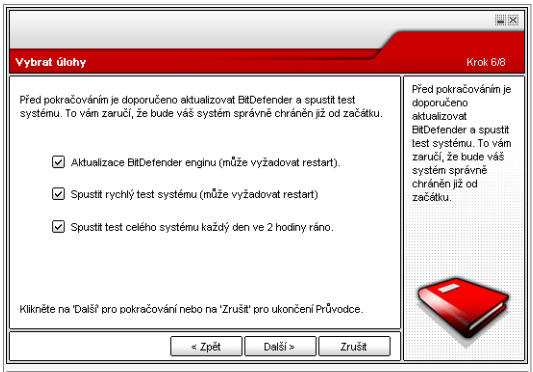
2.3.5. Krok 5/8 - O RTVR



RTVR informace

Klikněte na **Další** pro pokračování nebo klikněte na **Zrušit** pro ukončení průvodce.

2.3.6. Krok 6/8 - Volba úlohy ke spuštění



Výběr úlohy

Nastavte BitDefender Antivirus v10 na provádění důležitých úloh pro zajištění bezpečnosti vašeho systému.

Dostupné jsou následující volby:

- **Aktualizace BitDefender Antivirus v10 engine (může vyžadovat restart)** - během dalšího kroku bude aktualizován engine BitDefender Antiviru v10 a bude tak zajištěna ochrana vašeho počítače před posledními škodlivými kódy.
- **Spustit rychlý test systému (může vyžadovat restart)** - během dalšího kroku bude spuštěn rychlý test systému, který dovolí BitDefender Antiviru v10 zkontrolovat, zda-li nejsou soubory ve složkách `Windows` a `Program Files` nakaženy.
- **Spustit test celého systému každý den ve 2 hodiny ráno** - spustí test celého systému každý den ve 2 hodiny ráno.

Důležité

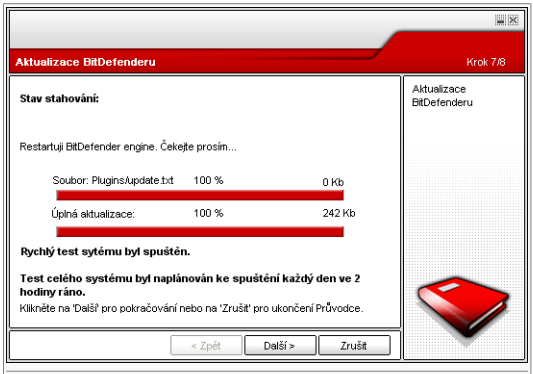
Před pokračováním k dalšímu kroku doporučujeme pro zajištění bezpečnosti vašeho systému tuto volbu povolit.

Zvolili jste pouze poslední volbu nebo žádnou z nabízených voleb, tento krok bude přeskočen.

Návratem na předchozí krok můžete provést jakékoli změny (klikněte na **Zpět**). Upozorňujeme, že je tento proces nevratný: pokud budete pokračovat, nebude již možné se na předchozí krok vrátit.

Klikněte na **Další** pro pokračování nebo klikněte na **Zrušit** pro ukončení průvodce.

2.3.7. Krok 7/8 - Čekání na dokončení úloh

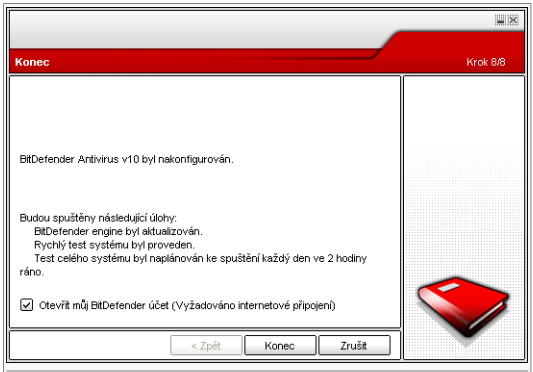


Stav úloh

Počkejte na dokončení úloh. Vidět můžete stav úloh vybraných v předchozím kroku.

Klikněte na **Další** pro pokračování nebo klikněte na **Zrušit** pro ukončení průvodce.

2.3.8. Krok 8/8 - Zobrazení souhrnu



Konec

Toto je poslední krok průvodce konfigurací.

Pro vstup do svého BitDefender účtu zvolte **Otevřít můj BitDefender účet**. Je vyžadováno připojení na Internet.

Pro ukončení průvodce a pokračování v instalaci klikněte na **Konec**.

2.4. Aktualizace

Aktualizační procedura může být provedena jedním z následujících způsobů:

- **Instalace bez odstranění předchozí verze - pro v8 a vyšší, kromě Internet Security**

  Spusťte soubor setup a následujte průvodce popsaného v části „*Instalační kroky*“ (str. 7).

  Důležité

  Během instalačního procesu se objeví chybové hlášení způsobené službou `Filespy service`. Pro pokračování instalace klikněte na **OK**.

- **Odinstalujte vaši předchozí verzi a nainstalujte novou - pro všechny verze BitDefenderu**

  Nejprve musíte odstranit vaši předchozí verzi, restartovat počítač a nainstalovat verzi novou, jak je popsáno v sekci „*Instalační kroky*“ (str. 7).

Důležité

Pokud provádíte aktualizaci z BitDefenderu v8 nebo vyšší, doporučujeme vám uložit si Nastavení BitDefenderu. Po dokončení procesu aktualizace si je můžete znovu načíst.

2.5. Odstranění, oprava nebo modifikace částí BitDefenderu

Chcete-li změnit, opravit, nebo odstranit **BitDefender Antivirus v10**, postupujte touto cestou ze Start menu ve Windows: **Start → Programy → BitDefender 10 → Změnit, Opravit nebo Odinstalovat**.

Budete požádáni o potvrzení Vaší volby kliknutím na **Další**. Objeví se nové okno, v němž si můžete vybrat:

- **Změnit** - vybrat nové programové komponenty pro přidání, nebo vybrat již instalované komponenty k odstranění.

  Poznámka

  Jak kompletně dokončit instalaci se dozvíte v šestém kroku sekce *„Instalační kroky“* (str. 7).

- **Opravit** - znovu nainstalovat veškeré programové komponenty, které byly instalovány v předchozí instalaci.

  Důležité

  Před opravami produktu doporučujeme, abyste si uložili Nastavení BitDefenderu. Po dokončení procesu oprav si je můžete znovu načíst.

- **Odstranit** - odstranit veškeré nainstalované komponenty.

  Pokud zvolíte odstranění BitDefenderu, nebudete již déle chráněni proti virům, spyware a hackerům. pokud chcete, aby byly po odinstalaci BitDefenderu povoleny Windows Firewall a Windows Defender, zvolte odpovídající zatrhávací políčko v dalším kroku průvodce.

  Prosíme Vás, abyste věnovali trochu svého času a řekli nám, proč jste se rozhodli odinstalovat BitDefender. Zvolte zatrhávací políčko **Zaslat odpověď** a vyplňte online formulář pro zaslání nám vašich postřehů.

Pro pokračování instalace, vyberte jednu ze tří možností uvedených výše. Volbu **Odstranit** doporučujeme pro čistou reinstalaci. Poté co je dokončen proces odinstalování, doporučujeme Vám vymazat složku `Softwin` z `Program Files`.

Popis a vlastnosti

3. BitDefender Antivirus v10

Antivirové a antispywarové řešení pro váš počítač!

BitDefender Antivirus v10 je silný antivirový a antispywarový nástroj s vlastnostmi, které nejlépe uspokojí vaše požadavky na bezpečnost systému. Snadnost použití a automatická aktualizace dělají z **BitDefender Antiviru** produkt 'Nainstaluj a zapomeň'.

3.1. Antivirus

Úkolem modulu Antivirus je odhalit a odstranit všechny přítomné viry. BitDefender Antivirus používá robustní skenovací nástroje, certifikované ICSA Labs, Virus Bulletin, Checkmark, Checkvir a TÜV.

Proaktivní detekce. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) emuluje virtuální počítač uvnitř počítače, kde se spouští jednotlivé programy za účelem testovaní potenciálně nebezpečného chování. Tato BitDefenderem patentovaná technologie reprezentuje novou bezpečnostní vrstvu, která udržuje operační systém v bezpečí před neznámými viry odhalováním záludných kódů, pro které ještě nebyly vydány podpisy.

Permanentní antivirová a antispywarová ochrana. Nové a zdokonalené skenovací nástroje BitDefenderu prohlédnou a léčí nakažené soubory na vstupu, ztráta dat je přitom minimalizována. Infikované dokumenty mohou být nyní obnoveny, namísto toho, aby byly smazány.

Detekce a odstranění rootkitů. Nový BitDefender modul vyhledává rootkity (podvodné skryté programy vytvořené pro kontrolu počítačů svých obětí) a po detekci je okamžitě odstraní.

Webové testování. Internetový provoz je nyní filtrován v reálném čase a to dokonce dříve, než dosáhne prohlížeče. Máte tak zajištěnu bezpečnost a příjemné zážitky na Internetu.

Ochrana Peer-2-Peer a IM aplikací. Filtruje viry, které se rozšířily prostřednictvím zasílání zpráv a softwarovými aplikacemi na sdílení souborů.

Plná ochrana e-mailů. BitDefender funguje na POP3/SMTP úrovni protokolu, filtruje příchozí a odchozí e-mailové zprávy, bez ohledu na používaného e-mailového klienta (Outlook™, Outlook Express™ / Windows Mail™, The Bat!™, Netscape®, atd.) bez další dodatečné konfigurace.

3.2. Antispyware

BitDefender v reálném čase monitoruje a předchází potenciálním hrozbám spyware dříve, než mohou váš systém poškodit. Díky komplexní databázi spywarových signatur zůstane váš počítač vždy bezpečný.

Antispywarová ochrana. BitDefender sleduje tucty potenciálních "aktivních bodů" ve vašem systému, kde by se mohl vyskytnout spyware, a také kontroluje jakékoliv změny systému a softwaru. Známé spywarové hrozby jsou zablokovány ihned.

Testování a odstranění spyware. BitDefender může testovat celý váš systém nebo jeho část, a zjišťuje přítomnost spyware. Využívá pravidelně aktualizovanou databázi spywarových signatur.

Ochrana soukromí. Ochránce soukromí monitoruje HTTP (webová) a SMTP (poštovní) data odesílaná z vašeho počítače, zda-li neobsahují osobní informace - jako čísla kreditních karet, čísa sociálního pojištění a ostatní uživatelská data (jako např. kódy a hesla).

Anti-Dialer. Konfigurovatený anti-dialer brání nebezpečným aplikacím v připojení k internetu a nárůstu vašeho telefonního účtu.

Kontrola cookies. Antispyware filtruje příchozí a odchozí soubory typu cookies a při surfování po internetu udržuje vaši identitu a nastavení v utajení.

Kontrola aktivního obsahu. Proaktivně blokuje veškeré potenciálně nebezpečné aplikace, jako jsou Java Aplety nebo Java Skritpy.

3.3. Další vlastnosti

Ovládání a použití. Průvodce nastavením se spustí ihned po instalaci a pomůže uživateli se zvolením nejvhodnějšího nastavení aktualizací, plánovače testování a provede uživatele registrací a aktivací produktu.

Uživatelské rozhraní. BitDefender přebudoval uživatelské rozhraní s důrazem na pohodlí a uspořádání ovládání. Výsledkem je množství modulů BitDefenderu v10 vyžadujících mnohem méně uživatelovi pozornosti, a to díky skvělému použití automatického a strojového učení.

Časté aktualizace. Vaše kopie BitDefenderu bude aktualizována 24 krát za den přes Internet, přímo nebo přes Proxy server. V nutném případě je produkt schopný se sám opravit stažením poškozených nebo chybějících souborů ze serverů BitDefender.

Podpora 24 hodin/7 dnů. Zajištěná kvalifikovanými zástupci a on-line databází s odpověďmi na často kladené otázky.

Záchranný disk. **BitDefender Antivirus v10** je dodáván na bootovacím CD. Toto CD může být použito k analýze, opravě nebo vyléčení poškozeného systému, který nemůže být spuštěn.

4. Moduly BitDefenderu

BitDefender Antivirus v10 obsahuje moduly: **Hlavní**, **Antivirus**, **Antispyware**, **Aktualizace**.

4.1. Hlavní modul

BitDefender je plně konfigurovaný pro maximální bezpečnost.

Základní informace o veškerých modulech BitDefenderu jsou zobrazeny v Hlavním modulu. Zde můžete zaregistrovat váš produkt a nastavit celkové chování Bitdefenderu.

4.2. Modul Antivirus

BitDefender vás chrání před viry, spyware a ostatními záludnými kódy, které vnikají do vašeho systému, tím, že skenuje vaše soubory, e-maily, stahované soubory a ostatní obsah při vstupu do vašeho systému.

Protivirová Bitdefender ochrana je rozdělena do dvou kategorií:

- Testování při přístupu - zabraňuje novým virům, spyware a ostatním záludným kódům vniknout do vašeho systému. Rovněž se jí také říká antivirový štít – soubory jsou testovány, když k nim uživatel přistoupí. BitDefender bude například testovat dokument vytvořený ve Wordu až když jej otevřete a e-mailovou zprávu, až když ji dostanete. BitDefender soubory testuje až "když je použijete" – tedy při přístupu k nim.
- Testování na požádání - odhaluje viry, spyware a ostatní záludné kódy již ve vašem systému usídlené. Je to klasické protivirové testování – testování iniciované uživatelem – vyberete disk, složku nebo soubor, který má BitDefender testovat – BitDefender tedy testuje na požádání.

4.3. Modul Antispyware

BitDefender sleduje tucty potenciálních "aktivních bodů" ve vašem systému, kde by se mohl vyskytnout spyware, a také kontroluje jakékoliv změny systému a softwaru. Známé spywarové hrozby jsou zablokovány ihned. To je velice efektivní při blokování trojských koní a dalších nástrojů instalovaných počítačovými hackery, kteří se pokoušejí proniknout do vašeho soukromí a odeslat vaše osobní informace, jako např. čísla kreditních karet, z vašeho počítače k hackerovi.

4.4. Modul Aktualizace

Každý den jsou identifikovány nové viry. To je důvod, proč udržovat BitDefender aktualizovaný novými virovými signaturami. Ve výchozím nastavení si BitDefender kontroluje nové aktualizace každou hodinu.

Aktualizace probíhá následujícími způsoby:

- **Aktualizace antivirových nástrojů** - jakmile se objeví nová hrozba, soubory, které obsahují virové signatury, musí být aktualizovány, aby byla zajištěna permanentně aktuální ochrana proti nim. Tato aktualizace je rovněž známa pod názvem **Aktualizace virových definic**.
- **Aktualizace antispywarových nástrojů** - do databáze budou přidány nové spywarové signatury. Tato aktualizace je rovněž známa pod názvem **Aktualizace Antispyware**.
- **Aktualizace produktu** - jakmile je vydána nová verze produktu, dojde k zavedení nových vlastností a skenovacích technik, které zlepší výkon produktu. Tato aktualizace je rovněž známa pod názvem **Aktualizace produktu**.

Dále, z pohledu intervencí uživatele, rozlišujeme:

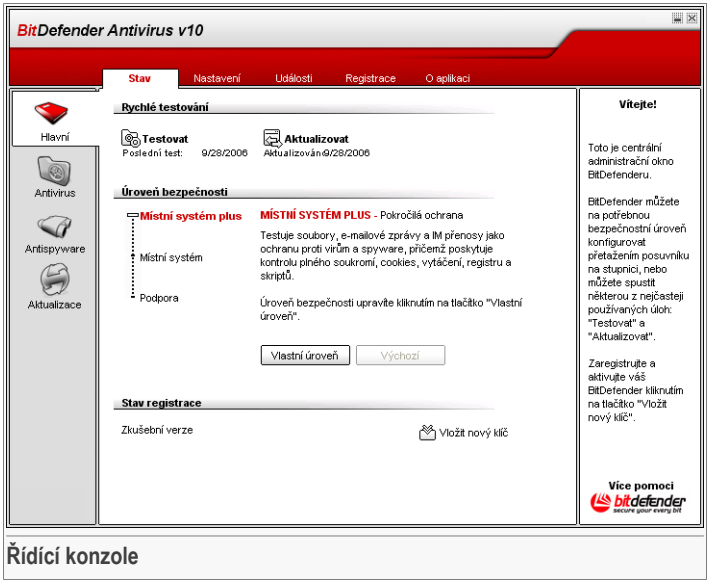
- Automatická aktualizace - BitDefenderu automaticky kontaktuje aktualizační server aby prověřil, zda byla zveřejněna nějaká aktualizace. Pokud ano, dojde k aktualizaci BitDefenderu automaticky. Automatická aktualizace může být provedena kdykoliv kliknutím na **Aktualizovat** v modulu Aktualizace.
- Ruční aktualizace - musíte stáhnout a nainstalovat poslední virové signatury ručně.

Řídící konzole

5. Přehled

BitDefender Antivirus v10 byl navržen s centralizovaným řídícím panelem, který umožňuje konfiguraci možností ochrany u všech modulů BitDefenderu. Jinými slovy, pro přístup ke všem modulům je dostačující otevřít řídící konzoli: **Antivirus**, **Antispyware** a **Aktualizace**.

Pro přístup k řídící konzoli použijte Start menu Windows a následně **Start** → **Programy** → **BitDefender 10** → **BitDefender Antivirus v10** nebo rychleji – stačí poklepat na **ikonu BitDefenderu** v systémové liště.



Řídící konzole

Na levé straně řídící konzole můžete vidět nabídku modulů:

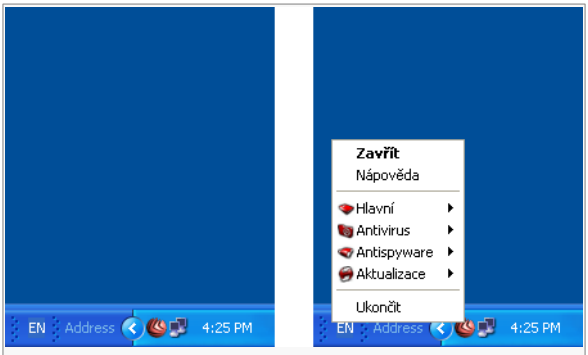
- Hlavní - pro přístup do sekce, kde uvidíte přehled veškerých hlavních nastavení v BitDefenderu, detaily produktu a kontaktní informace. Zde si můžete rovněž zaregistrovat produkt.
- Antivirus - v této sekci můžete nastavovat modul **Antivirus**.
- Antispyware - v této sekci můžete nastavovat modul **Antispyware**.
- Aktualizace - v této sekci můžete nastavovat modul **Aktualizace**.

Na pravé straně management konzole můžete uvidět informaci o tom, v jaké sekci se právě nacházíte. Volba **Více nápovědy**, umístěná dole vpravo, otevře soubor **Nápověda**.

5.1. Systémová lišta

Je-li konzole minimalizována, objeví se ikona v systémové liště.

Pokud na tuto ikonu poklepete, otevře se řídící konzole. Pokud ovšem na ikonu kliknete pravým tlačítkem myši, vyvolá se kontextové menu. Takto můžete BitDefender rychleji ovládat:



Ikona BitDefenderu v systémové liště

- **Zobrazit/Zavřít** - otevře řídící konzoli nebo ji minimalizuje do systémové lišty.
- **Nápověda** - otevře elektronickou dokumentaci.
- **Hlavní** - otevře Hlavní modul.
  - **Vložit nový klíč** - spustí průvodce registrací, který vás provede registračním procesem.
  - **Upravit účet** - spustí průvodce, který vás provede vytvořením BitDefender účtu.
- **Antivirus** - ovládání modulu Antivirus.
  - **virový štít je zapnutý/vypnutý** - zobrazuje stav virového štítu (zapnutý/vypnutý). Klikněte na tuto volbu pro zapnutí nebo vypnutí virového štítu.
  - **Test** - otevře podmenu, ze kterého si můžete vybrat ke spuštění jednu z testovacích úloh dostupných v sekci Test.
- **Antispyware** - ovládání modulu Antispyware.
  - **Antispyware je zapnutý / vypnutý** - zobrazuje stav antispywarové ochrany (zapnutá / vypnutá). Klikněte na tuto volbu pro vypnutí nebo zapnutí antispywarové ochrany.
  - **Pokročilá nastavení** - zde můžete nakonfigurovat ovládáni Antispywaru.
- **Aktualizace** - ovládání modulu Aktualizace.
  - **Aktualizovat** - provede okamžitou aktualizaci.

- **Automatická aktualizace je zapnutá / vypnutá** - zobrazuje stav automatické aktualizace (zapnutá / vypnutá). Klikněte na tuto volbu pro vypnutí nebo zapnutí automatické aktualizace.

- **Ukončit** - vypne aplikaci. Volbou této možnosti zmizí ikona ze systémové lišty a pro přístup do řídící konzole musíte aplikaci spustit znovu z menu Start.

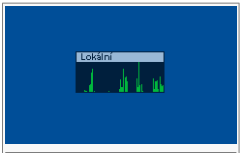
Poznámka

Pokud vypnete jeden nebo více modulů BitDefenderu, ikona se změní na černou. Tak budete vědět, že jsou některé moduly vypnuté i bez otevření řídící konzole.
Pokud je dostupná nová aktualizace, bude ikona blikat.

5.2. Panel aktivity testování

Panel aktivity testování je grafická vizualizace testování vašeho systému.

Zelené sloupce (**Lokální**) zobrazují počet testovaných souborů za vteřinu na stupnici 0 do 50.



Panel aktivity

Poznámka

Panel aktivity testování upozorní na vypnutý virový štít červeným křížem v příslušném poli (**Lokální**). Tak stále víte, zda jste chránění i bez otevření řídící konzole.

Pokud již nechcete vidět grafickou vizualizaci, klikněte na ni pravým tlačítkem a vyberte **Schovat**.

Poznámka

Pro úplné skrytí tohoto okna, odstraňte zatržítko v políčku **Zapnout monitor aktivity testování** (v modulu **Hlavní** v sekci Nastavení).

6. Hlavní modul

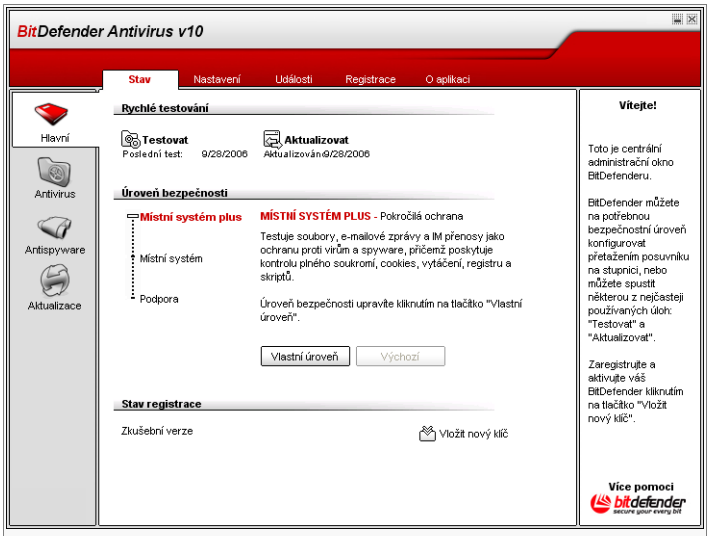
Sekce **Hlavní** této uživatelské příručky obsahuje následující témata:

- Všeobecné informace
- Nastavení řídící konzole
- Události
- Registrace produktu
- O BitDefenderu

Poznámka

Podrobnější informace týkající se **Hlavního** modulu najdete v kapitole *„Hlavní modul“* (str. 25).

6.1. Všeobecné informace



Všeobecné informace

V této sekci můžete nastavit úroveň celkové bezpečnosti. Můžete zde také produkt zaregistrovat a vidět datum expirace licence.

6.1.1. Rychlé úlohy

BitDefender dovoluje rychlý přístup k základním bezpečnostním úlohám. Užíváním těchto úloh můžete udržet váš BitDefender vždy aktualizovaný, testovat váš systém nebo blokovat síťový provoz.

Pro testování celého systému stačí kliknout na **Testovat**. Otevře se okno testu a bude proveden test celého systému.

Důležité

Důrazně doporučujeme, abyste test celého systému spustili alespoň jednou týdně. Pro více informací o testovacích úlohách a procesu testování si prohlédnětě sekci Testování na požádání v uživatelské příručce.

Před testováním vašeho systému doporučujeme Bitdefender aktualizovat, aby byl schopen detekovat i nejnovější hrozby. Pro aktualizaci BitDefenderu stačí kliknout na **Aktualizovat**. Počkejte pár vteřin, než se proces aktualizace dokončí, nebo, lépe, zkontrolujte sekci Aktualizace pro kontrolu stavu aktualizace.

Poznámka

Pro více informací o procesu aktualizace si přečtěte sekci Automatická aktualizace v uživatelské příručce.

6.1.2. Úroveň bezpečnosti

Můžete si zvolit úroveň bezpečnoti podle toho, jakou ochranu potřebujete. Přesunutím posuvníku na stupnici potřebnou úroveň nastavíte.

Jsou zde 3 typy úrovní bezpečnosti:

Úroveň bezpečnosti	Popis
Údržba	Neposkytuje žádnou ochranu. Zapnutá je pouze **Automatická aktualizace**. Pouze aktualizuje BitDefender. Ačkoli tato bezpečností úroveň neposkytuje žádnou ochranu, může být vhodná pro systémové administrátory.
Lokální systém	Poskytuje antivirovou ochranu. Doporučováno hlavně pro počítače bez přístupu k internetu nebo do sítě. Spotřeba systémových zdrojů je velmi nízká. Soubory budou při přístupu testovány na viry.

Úroveň bezpečnosti	Popis
Lokální systém Plus	Poskytuje antivirovou&antispywarovou ochranu. Doporučováno hlavně pro počítače bez přístupu k internetu nebo do sítě. Spotřeba systémových zdrojů je velmi nízká. Soubory budou při přístupu testovány na viry a spyware.

BitDefender Antivirus v10 je doporučován pro počítače bez přístupu k internetu nebo do sítě.

Upravovat úroveň bezpečnosti můžete kliknutím na **Vlastní úroveň**. V zobrazeném okně zvolte možnosti, které chcete povolit a klikněte na **OK**.

Pro nastavení posuvníku na výchozí hodnotu klikněte na **Výchozí**.

6.1.3. Stav registrace

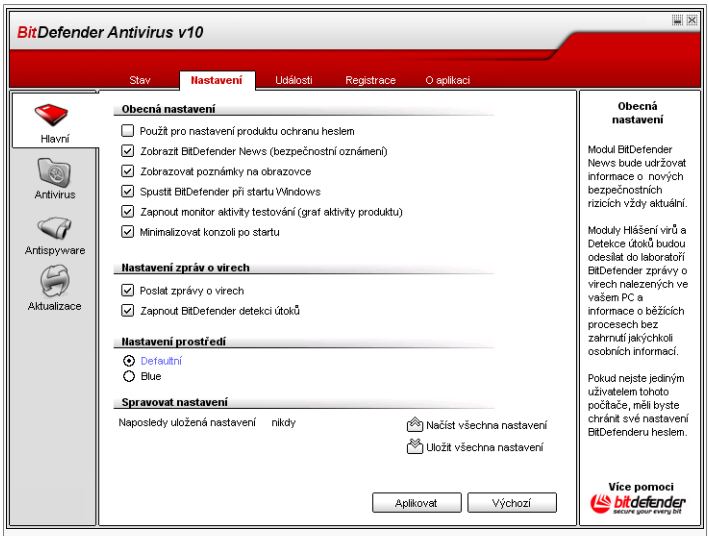
Zde můžete vidět informace o stavu vaší Bitdefender licence. Dále je zde uvedeno datum jejího vypršení a můžete si zde produkt zaregistrovat.

Pro vložení nového klíče klikněte na **Vložit nový klíč**. Pro úspěšnou registraci BitDefenderu dokončete průvodce registrací.

Poznámka

Pro více informací o procesu registrace si přečtěte sekci Registrace produktu v uživatelské příručce.

6.2. Nastavení řídící konzole



Nastavení řídící konzole

Zde si můžete nastavit základní parametry chování BitDefenderu. Ve výchozím nastavení je BitDefender načten při startu a pak minimalizován do systémové lišty.

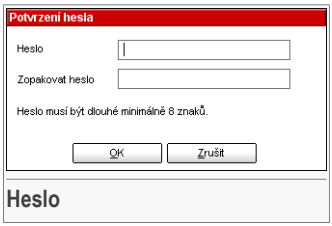
6.2.1. Obecná nastavení

- **Použit ochranu heslem** - umožní nastavení hesla za účelem ochrany konfigurace řídící konzole BitDefenderu.

  Poznámka

  Pokud nejste jedinou osobou používající tento počítač, je doporučeno ochránit vaše nastavení Bitdefenderu heslem.

  Pokud zvolíte tuto možnost, zobrazí se následující okno:



Heslo

Zadejte heslo do pole **Heslo**, potvrďte jej znovu do pole **Zopakovat heslo** a stiskněte **OK**.

Od tohoto okamžiku budete při pokusu o provedení změn v konfiguraci BitDefenderu požádáni o heslo.

Důležité

Pokud zapomenete heslo, je třeba opravit produkt.

- **Přijímat bezpečnostní oznámení** - přijímat občasná bezpečnostní sdělení o výskytu virových epidemií, zasílané serverem Bitdefender.
- **Zobrazovat poznámky na obrazovce** - zobrazovat vyskakovací okna s poznámkami o stavu produktu.
- **Spustit BitDefender při startu Windows** - automaticky spustí BitDefender při startu systému.

Poznámka

Doporučujeme ponechat tuto možnost zatrženu.

- **Zapnout monitor aktivity testování** - zapne/vypne Monitor aktivity testování.
- **Minimalizovat konzoli po spustění** - minimalizuje řídící konzoli BitDefenderu poté, co je načten při startu systému. V systémové liště se zobrazí pouze ikona BitDefenderu.

6.2.2. Nastavení zpráv o virech

- **Poslat zprávy o virech** - odešle hlášení o virech identifikovaných ve vašem počítači do laboratoře BitDefenderu. Umožní nám sledovat virové útoky.

  Zprávy nebudou obsahovat žádné tajné informace jako vaše jméno, IP adresa apod., a nebudou použity pro komerční účely. Dodaná informace bude obsahovat pouze jméno viru a bude využita výhradně pro tvorbu statistických hlášení.

- **Zapnout BitDefender detekci útoků** - odešle hlášení o virech identifikovaných ve vašem počítači do laboratoře BitDefenderu. Umožní nám sledovat virové útoky.

  Hlášení nebudou obsahovat žádné tajné informace jako vaše jméno, IP adresa apod., a nebudou použity pro komerční účely. Dodaná informace bude obsahovat pouze jméno viru a bude využita výhradně pro tvorbu statistických hlášení.

6.2.3. Nastavení prostředí

Umožňuje vybrat barvu řídící konzole. Skin představuje vzhled pozadí rozhraní. Pro změnu barvy pozadí klikněte na požadovanou barvu.

6.2.4. Správa nastavení

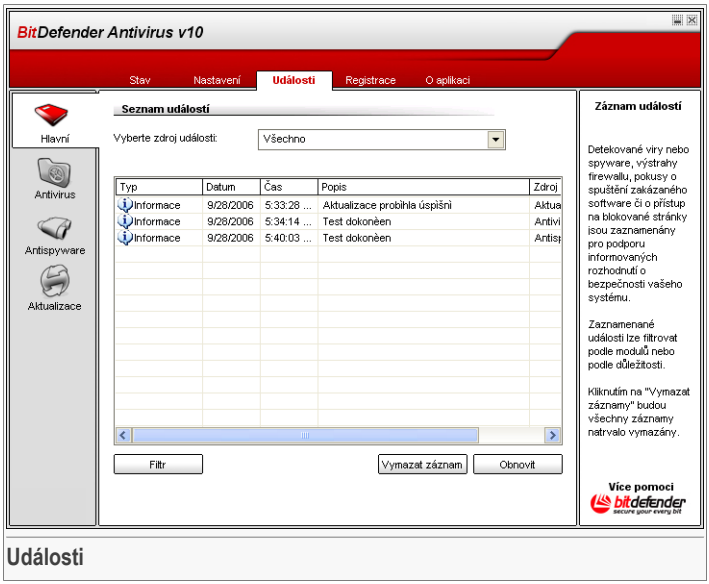
Použijte tlačítka **Uložit všechna nastavení** / **Načíst všechna nastavení** pro uložení/načtení všech nastavení, které jste v BitDefenderu provedli. Tak můžete používat stejná nastavení, pokud reinstalujete nebo opravujete BitDefender.

Důležité

Uložit a načíst nastavení mohou pouze uživatelé s administrátorskými právy.

Pro nahrání původních nastavení klikněte na **Obnovit původní nastavení**.

6.3. Události



Události

V této části jsou zobrazeny všechny události vygenerované BitDefenderem.

Najdete zde 3 typy událostí: **Informace**, **Varování** a **Kritický**.

Příklady událostí:

- **Informace** - kdy byl e-mail testovaný;
- **Varování** - kdy byl nalezen podezřelý soubor;
- **Kritický** - kdy byl nalezen infikovaný soubor.

Pro každou událost jsou k dispozici následující informace: datum a čas, kdy k události došlo, jednoduchý popis a její zdroj (**Antivirus**, **Firewall**, **Antispyware** or **Aktualizace**). Poklikejte na událost pro zobrazení jejích podrobností.

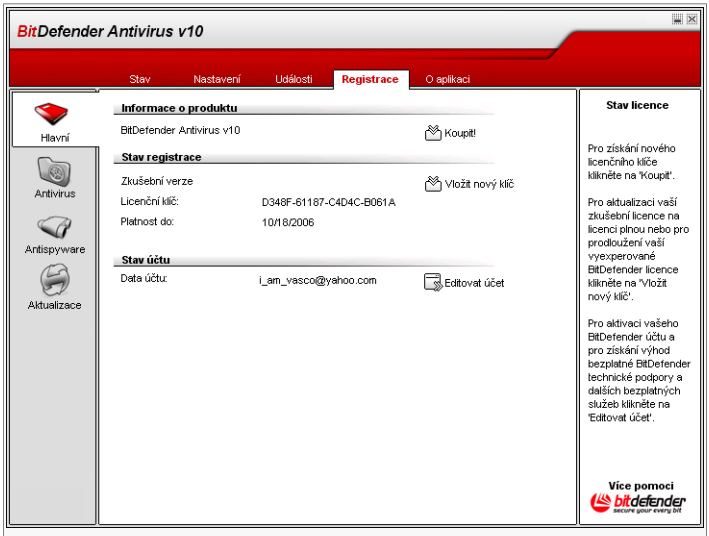
Můžete seřadit tyto události dvěma způsoby (podle data nebo podle zdroje):

- Kliknutím na **Filtrovat** vyberte, jaké typy událostí chcete zobrazit.
- Z menu vyberte zdroj události.

Jestli-že je řídící konzole otevřena v záložce **Události** a ve stejnou dobu nastane událost, musíte kliknout na **Obnovit**, abyste událost viděli.

Pro vymazání všech událostí ze seznamu klikněte na **Vymazat záznam** a poté na **Ano** pro potvrzení vaší volby.

6.4. Registrace produktu



Registrace produktu

Tato sekce obsahuje informace o stavu vašeho Bitdefender produktu (stav registrace, ID produktu, datum expirace) a BitDefender účet. Zde si můžete produkt zaregistrovat a upravovat svůj BitDefender účet.

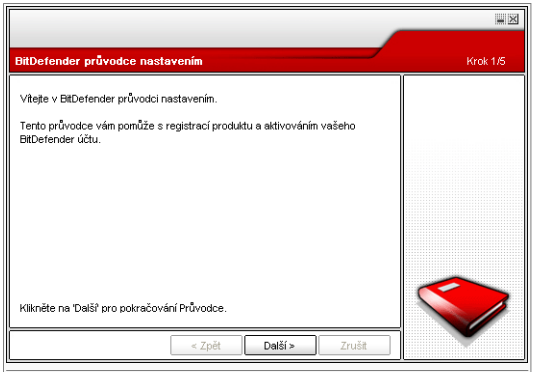
Pro získání nového licenčního klíče z BitDefender online obchodu, klikněte na tlačítko **Koupit**.

Kliknutím na **Vložit nový klíč** můžete zaregistrovat produkt, upravit registrační klíč nebo detaily účtu. Pro nastavení vašeho BitDefender účtu klikněte na **Upravit účet**. V obou případech bude spuštěn průvodce registrací.

6.4.1. Průvodce registrací

Průvodce nastavením má 5 kroků.

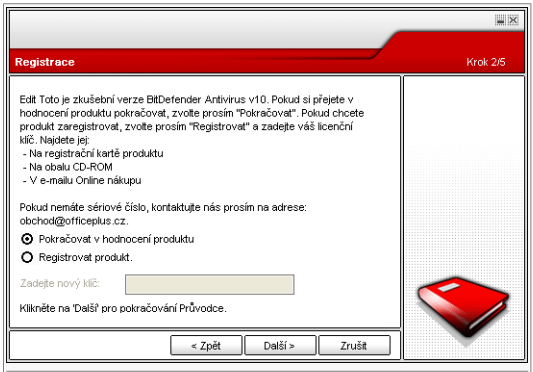
Krok 1/5 - Vítejte v BitDefender Průvodci registrací



Uvítací okno

Klikněte na **Další**.

Krok 2/5 - Registrace BitDefenderu



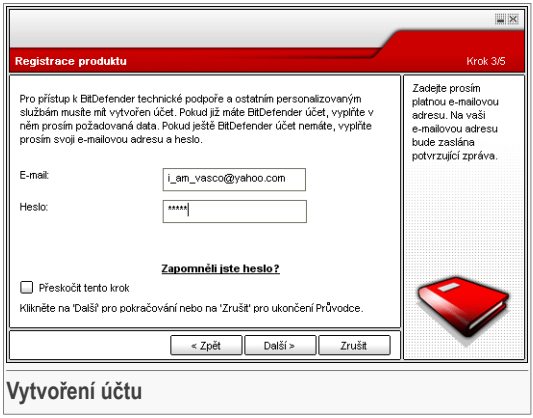
Registrace

Zvolte **Registrovat produkt** pro registraci **BitDefender Antiviru v10**. Licenční klíč zadejte v poli **Vložit nový klíč**.

Pro pokračování v hodnocení produktu zvolte **Pokračovat v hodnocení produktu**.

Klikněte na **Další**.

Krok 3/5 - Vytvoření BitDefender účtu



Nemám BitDefender účet

Pro získání bezplatné BitDefender technické podpory a dalších zdarma dostupných služeb musíte mít vytvořen účet.

Do pole **E-mail** zadejte platnou e-mailovou adresu. Zvolte si heslo a zadejte jej do pole **Heslo**. Heslo potvrďte přepsáním do pole **Zopakovat heslo**. Použijte tuto e-mailovou adresu a heslo pro přihlášení se do vašeho účtu na http://myaccount.bitdefender.com.

Poznámka

Heslo musí obsahovat alespoň čtyři znaky.

Pro úspěšné vytvoření účtu musíte nejprve aktivovat vaši e-mailovou adresu. Zkontrolujte vaši e-mailovou adresu a následujte instrukce, které naleznete v přijaté zprávě, odeslané pomocí Bitdefender registrační služby.

Důležité

Před přechodem na další krok prosím aktivujte svůj účet.

Jestliže nechcete vytvořit Bitdefender účet, klikněte na **Přeskočit tento krok**. Přesunete se tak na další krok v průvodci.

Pro pokračování klikněte na **Další**.

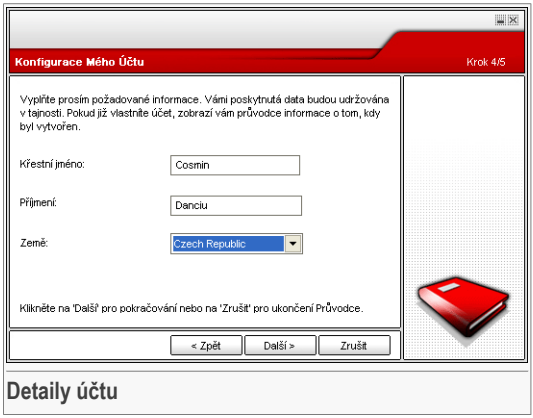
Již mám BitDefender účet

Pokud již máte aktivní účet, zadejte e-mailovou adresu a heslo vašeho účtu. Pokud zadáte neplatné heslo můžete jej opravit kliknutím na **Další**. Klikněte na **OK** pro znovuzadání hesla nebo na **Zrušit** pro ukončení průvodce.

Pokud jste zapomněli své heslo, klikněte na **Zapomněli jste heslo?** a následujte instrukce.

Pro pokračování klikněte na **Další**.

Krok 4/5 - Zadání detailů účtu



Detaily účtu

Poznámka

Pokud jste zvolili **Přeskočit tento krok** ve třetím kroku průvodce, nemůžete do tohoto kroku průvodce vstoupit.

Vyplňte své křestní jméno a příjmení a vyberte svoji zemi.

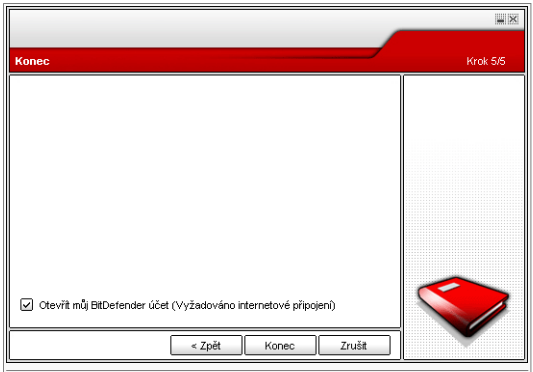
Pokud již máte účet, průvodce zobrazí informace, které jste v minulosti poskytli, jsou-li nějaké. Můžete zde také, pokud chcete, tyto informace upravovat.

Důležité

Data, která zde poskytnete, zůstávají důvěrná.

Klikněte na **Další**.

Krok 5/5 - Souhrn



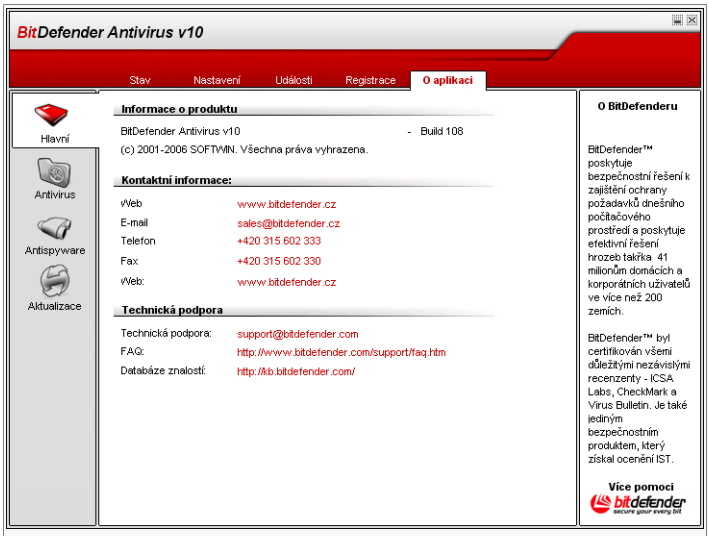
Konec

Toto je závěrečný krok průvodce konfigurací. Návratem na libovolný předchozí krok můžete provádět jakékoliv změny (klikněte na **Zpět**).

Jestliže nechcete provádět žádné změny, klikněte na **Konec** pro ukončení průvodce.

Pro vstup do svého BitDefender účtu zvolte **Otevřít můj BitDefender účet**. Je vyžadováno připojení na Internet.

6.5. O BitDefenderu



Všeobecné informace

Zde můžete najít kontaktní informace a informace o produktu.

BitDefender je vedoucí světový poskytovatel bezpečnostních řešení, které vyhovují dnešnímu počítačovému prostředí. Společnost nabízí jednu z nejrychlejší a nejefektivnjší řady bezbečnostního software, určujícího nové standardy prevence hrozeb, včasné detekce a ochrany. BitDefender poskytuje své produkty a služby více než 41 miliónům domácnostem a společnostem v takřka 180 zemích světa.

BitDefender™ je certifikovaný hlavními nezávislými recenzenty - **ICSA Labs**, **CheckMark** a **Virus Bulletin** a je to jediný bezpečnostní produkt, který obdržel **cenu IST**.

Podrobnější informace o BitDefenderu můžete získat na stránkách: http://www.bitdefender.com.

7. Modul Antivirus

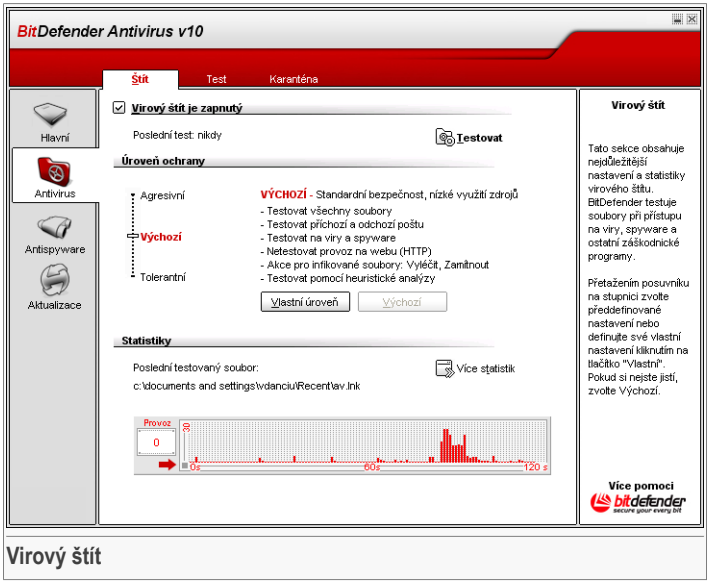
Sekce **Antivirus** této uživatelské příručky obsahuje následující témata:

- Testování při přístupu
- Testování na požádání
- Karanténa

Poznámka

Pro více detailů týkajících se modulu **Antiviru** si prohlédněte popis u *„Modul Antivirus“* (str. 25).

7.1. Testování při přístupu



Virový štít

V této sekci můžete konfigurovat **Virový štít** a sledovat informace o jeho aktivitách. **Virový štít** chrání váš počítač testováním e-mailů, stahovaných souborů a všech souborů k nimž přistupujete.

Důležité
Abyste ochránili váš počítač před infikací viry, mějte aktivovaný **Virový štít**.

V dolní části sekce je možné vidět statistiky **Virového štítu** o testovaných souborech a e-mailech. Chcete-li vidět podrobnější okno se statistikami, klikněte na **Více statistik**.

7.1.1. Úroveň ochrany

Můžete si vybrat úroveň ochrany jakou potřebujete. Pro nastavení požadované úrovně přesuňte posuvník na stupnici.

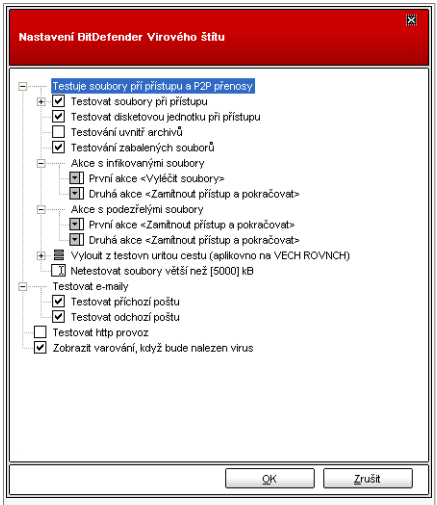
Existují 3 úrovně ochrany:

Úroveň ochrany	Popis
Tolerantní	Poskytuje základní ochranu. Spotřeba systémových zdrojů je velmi nízká. Programy a příchozí zprávy jsou testovány pouze na viry. Kromě klasického testování signatur je také použita heuristická analýza. Akce vykonané s infikovanými soubory jsou: smazat soubor/zakázat přístup.
Výchozí	Poskytuje základní ochranu. Spotřeba systémových zdrojů je velmi nízká. Všechny soubory a příchozí&odchozí e-mailové zprávy jsou testovány na viry a spyware. Kromě klasického testu signatur je také použita heuristická analýza. Akce vykonané s infikovanými soubory jsou: smazat soubor/zakázat přístup.
Agresivní	Poskytuje vysokou ochranu. Spotřeba systémových zdrojů je průměrná. Všechny soubory, příchozí&odchozí e-mailové zprávy a síťový provoz jsou testovány na viry a spyware. Kromě klasického testu signatur je také použita heuristická analýza. Akce vykonané s infikovanými soubory jsou: smazat soubor/zakázat přístup.

Pokud se chcete vrátit k výchozí úrovni ochrany, klikněte na **Výchozí**.

Pokročilí uživatelé mají v BitDefenderu možnost vlastního nastavení testování. Skener může být nastaven tak, aby přeskakoval přípony, adresáře či archivy, o nichž víte, že jsou neškodné. Tím můžete významně ušetřit čas a zlepšit citlivost počítače v průběhu testování.

Přizpůsobit **Virový štít** si můžete kliknutím na **Vlastní úroveň**. Otevře se náledující okno:



Nastavení štítu

Možnosti testování jsou uspořádány v rozbalovacím menu, podobně jako tomu bývá ve Windows.

Klikněte na "+" pro otevření dalších nastavení a na "–" pro jejich zavření.

Může se stát, že některé možnosti pro testování, přestože znaménko "+" svítí, nemohou být otevřeny. Důvodem je, že tyto možnosti ještě nebyly vybrány. Jakmile je vyberete, otevřou se.

- **Testovat soubory při přístupu a P2P přenosy** - testuje soubory při přístupu a spojení prostřednictvím komunikačních softwarových aplikací (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Dále vyberte typ souborů, který mají být testovány.

Možnost		Popis
Testovat soubory při přístupu	**Testovat všechny soubory**	Budou testovány všechny otevírané soubory, bez ohledu na jejich druh.
	Testovat jen programové soubory	Budou testovány pouze programové soubory. To znamená, pouze soubory s následujícími příponami: .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;

Možnost		Popis
		.chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml a .nws.
	Testovat uživatelem definované přípony	Budou testovány pouze soubory s příponami, které určí uživatel. Přípony musí být odděleny středníkem ";".
	Vyloučit z testování přípony: [ ]	Soubory s příponami určenými uživatelem NEBUDOU testovány. Přípony musí být odděleny středníkem ";".
	Testovat na rizikové programy	Testování na přítomnost rizikových programů. S nalezenými soubory bude zacházeno jako s infikovanými soubory. Software, který obsahuje adware komponenty, může přestat fungovat, pokud bude tato možnost zvolena. Pokud chcete z testování vynechat tyto typy souborů, vyberte možnost **Vynechat z testování dialery a aplikace**.
Testovat diskety při přístupu		Testování disketové machaniky při přístupu.
Testování uvnitř archivů		Budou testovány otevírané archivy. Výběr této možnosti vede ke zpomalení počítače.
Testování zabalených souborů		Budou testovány veškeré zabalené soubory.
První akce		Z rozbalovací nabídky si zvolte první akci vykonanou s infikovanými a podezřelými soubory.
	Odepřít přístup a pokračovat	V případě, že je zjištěn infikovaný soubor, přístup k němu bude odepřen.
	Vyléčit soubor	Vyléčí nakažený soubor.
	Smazat soubor	Okamžitě smaže infikované soubory, bez výstrahy.
	Přesunout do karantény	Infikované soubory jsou přesunuty do karantény.
Druhá akce		Z rozbalovacího menu zvolte druhou akci s infikovanými soubory, pro případ, že první akce selže.

Možnost		Popis
	Odepřít přístup a pokračovat	V případě, že je zjištěn infikovaný soubor, přístup k němu bude odepřen.
	Smazat soubor	Okamžitě smaže infikované soubory, bez výstrahy.
	Přesunout do karantény	Infikované soubory jsou přesunuty do karantény.
Netestovat soubory větší než [x] Kb		Uveďte maximální velikost souborů, které mají být testovány. Pokud je velikost 0 kB, budou testovány všechny soubory.
Vyloučit z testování určitou cestu (aplikováno na VŠECH ÚROVNÍCH)		Klikněte na "+" u zvolené možnosti pokud si přejete vynechat z testování nějakou složku. Otevře se nová volba `Nový záznam`. Zaškrtněte odpovídající políčko a v okně vyberte složku, kterou si přejete z testování vyloučit. Objekty zde vybrané budou vynechány z testování bez ohledu na zvolenou úroveň ochrany (nejen pro **Vlastní úroveň**).

- **Testovat e-maily** - testuje všechny příchozí i odchozí zprávy.

  Dostupné jsou následující volby:

Možnost	Popis
Testovat příchozí poštu	Testuje všechny příchozí e-mailové zprávy.
Testovat odchozí poštu	Testuje všechny odchozí zprávy.

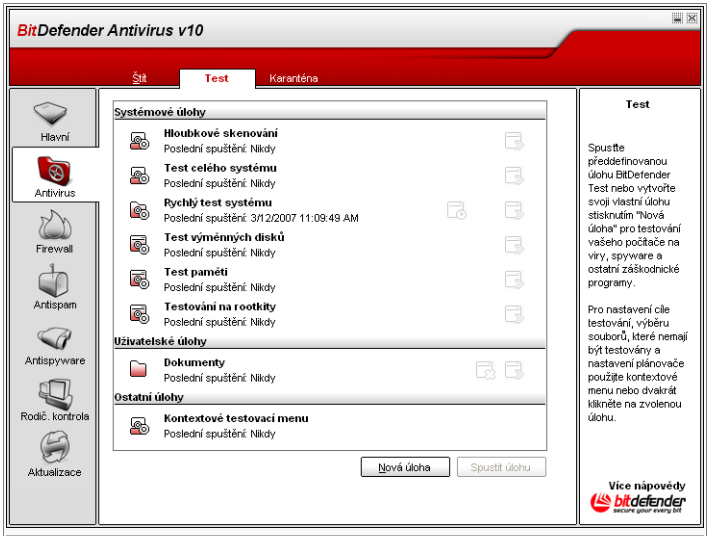
- **Testovat HTTP provoz** - testuje HTTP provoz.
- **Zobrazit varování při nalezení viru** - je-li v e-mailu nebo souboru nalezen vir, zobrazí se výstražné okno.

  V případě infikovaného souboru bude výstražné okno obsahovat jméno viru a cestu k němu, v případě infikovaného e-mailu bude okno obsahovat informaci o odesilateli, příjemci a jméno viru.

  Při nalezení podezřelého souboru můžete z výstražného okna spustit Průvodce, který vám pomůže odeslat soubor do laboratoří BitDefender k další analýze. Můžete zadat také vaši e-mailovou adresu, abyste mohli obdržet zpětnou informaci.

Klikněte na **OK** pro uložení změn a uzavření okna.

7.2. Testování na požádání



Testovací úlohy

V této sekci můžete nastavit BitDefender k testování vašeho počítače.

Hlavním úkolem BitDefenderu je udržovat váš počítač čistý – bez virů. BitDefender postupuje především tak, že drží nové viry mimo váš počítač a testuje e-mailové zprávy a nové soubory, stažené nebo kopírované do vašeho systému.

Existuje nicméně riziko, že virus byl již do vašeho systému zavlečený před tím, než jste instalovali BitDefender. Proto je dobré, jakmile nainstalujete BitDefender, ihned váš počítač testovat na přítomné viry. Rovněž doporučujeme, abyste testování vašeho počítače prováděli pravidelně.

7.2.1. Testovací úlohy

Testování na požádání je založeno na testovacích úlohách. Uživatel může počítač testovat s použitím výchozích úloh nebo úloh vlastních (uživatelsky definované úlohy).

Existují 3 kategorie testovacích úloh:

- **Systémové úlohy** - obsahuje seznam výchozích systémových úloh. Dostupné jsou následující úlohy:

Výchozí úloha	Popis
Hloukový test	Skenuje celý systém, včetně archivů, na viry a spyware.
Test celého systému	Skenuje celý systém, kromě archivů, na viry a spyware.
Rychlý test systému	Testuje všechny programy na viry a spyware.
Test výměnných disků	Testuje výměnné disky na viry a spyware.
Testovat paměť	Testuje paměť na známé spywarové hrozby.
Testování na rootkity	Testuje paměť na skryté záludné programy.

- **Uživatelské úlohy** - obsahuje uživatelsky definované úlohy.

`Dokumenty`. Použijte tuto úlohu pro testování vašich dokumentů ve složce `Dokumenty`.

- **Ostatní úlohy** - obsahuje seznam ostatních testovacích úloh. Tyto testovací úlohy se týkají alternativních testování, které nemohou být spuštěny v okně. Můžete pouze upravit jejich nastavení nebo si prohlédnout záznamy z testování.

U každé úlohy jsou napravo dostupná tři tlačítka:

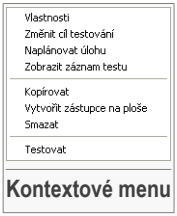
- **Plánovač úloh** - indikuje pozdější naplánování zvolených úloh. Pokud chcete tato nastavení změnit, klikněte v sekci Plánovač na tlačítko **Vlastnosti**.
- **Smazat** - odstraní zvolenou úlohu.

Poznámka

Pro systémové úlohy toto není dostupné. Nemůžete smazat systémovou úlohu.

- **Testovat** - spustí zvolenou úlohu a vyvolá okamžité testování.

7.2.2. Kontextové menu



Kontextové menu

Kontextové menu je dostupné pro každou úlohu. Kliknutím pravým tlačítkem myši na zvolenou úlohu se otevře.

Z kontextového menu jsou dostupné následující příkazy:

- **Vlastnosti** - otevře okno **Vlastnosti** na záložce **Přehled**, kde můžete změnit nastavení zvolené úlohy;
- **Změnit cíl testu** - otevře okno **Vlastnosti** na záložce **Cesta**, kde můžete změnit cíl testu zvolené úlohy;
- **Plánování** - otevře okno **Vlastnosti** na záložce **Plánovač**, kde můžete naplánovat zvolenou úlohu;
- **Zobrazit záznamy** - otevře okno **Vlastnosti** na záložce **Záznamy**, kde můžete vidět zprávy vygenerované po spuštění zvolené úlohy;
- **Kopírovat** - zkopíruje vybranou úlohu;

Poznámka

Toto můžete používat při vytváření nových úloh, stejně jako při úpravách jejich nastavení či jejich kopírování.

- **Vytvořit zástupce na ploše** - vytvoří na ploše zástupce zvolené úlohy;
- **Smazat** - smaže vybranou úlohu.

Poznámka

Pro systémové úlohy toto není dostupné. Nemůžete smazat systémovou úlohu.

- **Testovat** - okamžitě spustí vybranou úlohu.

Důležité

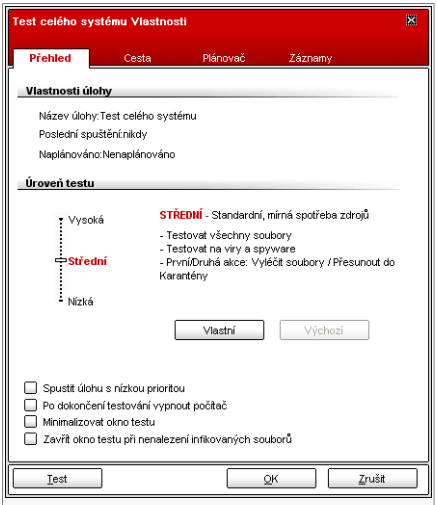
Díky podobným vlastnostem jsou v kategorii **Ostatní úlohy** dostupné pouze volby **Vlastnosti** a **Zobrazit záznam**.

7.2.3. Vlastnosti testovacích úloh

Každá testovací úloha má své vlastní okno **Vlastnosti**, kde je možné nastavit vlastnoti testování, cíle testování, naplánovat úlohu nebo si prohlédnout záznamy. Pro vstup do tohoto okna zvolte úlohu a klikněte na **Vlastnosti** (nebo na úlohu klikněte pravým tlačítkem myši a poté zvolte **Vlastnosti**).

Nastavení testu

Zde můžete vidět informace o úloze (název, poslední spuštění a stav naplánování) a nastavit vlastnosti testu.



Nastavení testu

Úroveň testu

Nejdříve musíte vybrat úroveň testu. Přesunutím posuvníku na stupnici zvolíte požadovanou úroveň.

Existují 3 úrovně testu:

Úroveň ochrany	Popis
Nízká	Poskytuje přijatelnou účinnost detekcí. Spotřeba systémových zdrojů je velmi nízká. Na viry budou testovány pouze soubory. Kromě klasického testu signatur bude použita i heuristická analýza. Akce vykonané s infikovanými soubory jsou: smazat soubor/přesunout do karantény.
Střední	Poskytuje středně vysokou účinnost detekcí. Spotřeba systémových zdrojů je průměrná. Na viry a spyware budou testovány všechny soubory. Kromě klasického testu signatur bude použita i heuristická analýza. Akce vykonané s infikovanými soubory jsou: smazat soubor/přesunout do karantény.
Vysoká	Poskytuje vysokou účinnost detekcí. Spotřeba systémových zdrojů je vysoká.

Úroveň ochrany	Popis
	Na viry a spyware budou testovány všechny soubory a archivy. Kromě klasického testu signatur bude použita i heuristická analýza. Akce vykonané s infikovanými soubory jsou: smazat soubor/přesunout do karantény.

Důležité

Úloha **Testování na rootkity** je dostupná se stejnými úrovněmi testování. Volby jsou následující:

- **Nízká** - Testovány budou pouze procesy. S detekovanými objekty nebude prováděna žádná akce.
- **Střední** - Soubory a procesy budou testovány na skryté objekty. S detekovanými objekty nebude prováděna žádná akce.
- **Vysoká** - Soubory a procesy budou testovány na skryté objekty. Detekované objekty budou přejmenovány.

Pokročilí uživatelé mají možnost vlastního nastavení testování v BitDefenderu. Skener může být nastaven tak, aby přeskakoval přípony, adresáře či archivy, o nichž víte, že jsou neškodné. Tím můžete významně ušetřit čas a zlepšit citlivost počítače v průběhu testování.

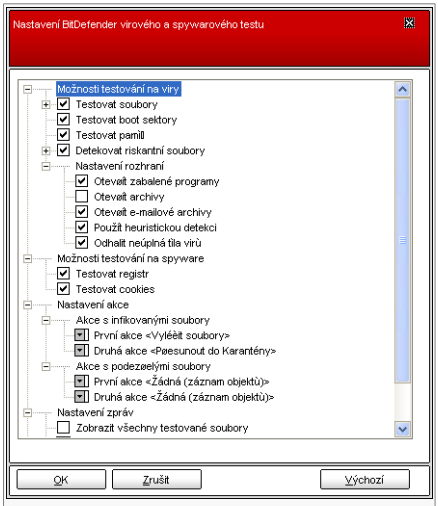
Klikněte na **Vlastní** pro nastavení svých vlastních možností testování. Otevře se nové okno.

Možnosti testování jsou uspořádány v rozbalovacím menu, podobně jako tomu bývá ve Windows.

Možnosti testování jsou seskupeny do 5 kategorií:

- **Možnosti testování na viry**
- **Možnosti testování na spyware**
- **Nastavení akce**
- **Nastavení zpráv**
- **Další nastavení**

Klikněte na "+" pro otevření dalších nastavení a na "–" pro jejich zavření.



Nastavení testu

Důležité

Pro úlohu **Testování na rootkity** jsou dostupné pouze tři kategorie: **Nastavení testování na rootkity**, **Nastavení zpráv** a **Další nastavení**. V první kategorii si můžete zvolit co chcete testovat (soubory, paměť nebo obojí) a můžete nastavit akce, které se provedou při detekování infikovaných objektů (**Nic (záznam objektů)/Přejmenovat objekty**). Poslední dvě kategorie jsou identické s těmi popsanými níže.

- Specifikujte typy objektů, které mají být testovány (archivy, e-mailové zprávy apod.) a další možnosti. To lze provést zaškrtnutím požadované možnosti v kategorii **Možnosti testování na viry**.

Možnost		Popis
Testovat soubory	**Testovat všechny soubory**	Budou testovány všechny otevírané soubory, bez ohledu na jejich druh.
	Testovat jen programové soubory	Testovány na viry budou pouze programové soubory. Tzn. pouze soubory s těmito příponami: `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` a `nws`.

Možnost		Popis
	Testovat uživatelem definované přípony	Budou testovány pouze soubory s příponami, které určí uživatel. Přípony musí být odděleny středníkem ";".
	Vyřadit uživatelem definované přípony	Soubory s příponami určenými uživatelem NEBUDOU testovány. Přípony musí být odděleny středníkem ";".
Testovat boot sektory		Testuje zaváděcí sektor systému.
Testovat paměť		Testuje paměť na viry a ostatní záludné programy.
Detekovat riskantní soubory		Testování na jiné hrozby než jsou viry, jako např. dialery a adware. S nalezenými soubory bude zacházeno jako s infikovanými soubory. Software, který obsahuje adware komponenty může přestat fungovat, pokud bude tato možnost zvolena. Zvolte **Vynechat aplikace a dialery**, pokud chcete některé z těchto souborů z testování vynechat.
Pokročilé možnosti testování	**Otevřít zabalené programy**	Testuje zabalené soubory.
	Otevřít archivy	Testuje uvnitř archivů.
	Otevřít e-mailové archivy	Testuje uvnitř e-mailových archivů.
	Použít heuristickou detekci	Použije heuristické testování souborů. Cílem heuristického testování je identifikovat nové viry na bázi určitých šablon (vzorů) a algoritmů, předtím než je nalezena nová definice viru. Mohou se objevit falešné poplašné zprávy. Pokud je takový soubor objeven, je označen jako podezřelý. V takovém případě vám doporučujeme zaslat daný soubor do laboratoře BitDefenderu na analýzu.
	Odhalit neúplná těla virů	Zjistí i nekompletní viry (viry s nekompletním tělem).

- Specifikování spywarového cíle (registr, paměť). To lze provést zaškrtnutím požadované možnosti v kategorii **Možnosti testování na spyware**.

Možnost	Popis
Test registru	Testuje zápisy do registru.
Test cookies	Testuje soubory cookies.

- Specifikujte akci, která se má provést při nalezení infikovaných a podezřelých souborů. Otevřete **Nastavení akce** a zvolte požadované akce.

  Zvolte akce, které mají být provedeny, pokud je detekován infikovaný nebo podezřelý soubor. Můžete zvolit různé akce pro infikované a pro podezřelé soubory. Můžete take zvolit druhou akci, pokud by první selhala.

Akce	Popis
Žádná (záznam souborů)	S infikovanými soubory nebude provedena žádná akce. Tyto soubory se objeví v souboru zpráv.
Dotázat se na akci uživatele	Jakmile je objeven infikovaný soubor, objeví se okno vyzývající uživatele k výběru akce pro tento soubor. Podle významu souboru se můžete rozhodnout jej vyléčit, izolovat v karanténě nebo jej smazat.
Vyléčit soubory	Vyléčí nakažený soubor.
Smazat soubory	Okamžitě smaže infikované soubory, bez výstrahy.
Přesunout do karantény	Přesune infikované soubory do karantény.
Přejmenovat soubory	Změní příponu infikovaných souborů. Nová přípona infikovaných souborů bude `.vir`. Přejmenováním infikovaných souborů je nebezpečí rozvoje viru a tedy i rozšíření infekce zabráněno. Současně mohou být tyto soubory uloženy pro další prozkoumání a analýzy.

Důležité

Přejmenovat soubory má podobný efekt i u skrytých souborů (rootkitů). Nová přípona infikovaných souborů bude `.vir`. Přejmenováním infikovaných souborů je nebezpečí rozvoje viru a tedy i rozšíření infekce zabráněno. Současně mohou být tyto soubory uloženy pro další prozkoumání a analýzy.

- Specifikujte možnosti pro soubor zpráv. Otevřete **Nastavení zpráv** pro výběr vhodných možností.

Možnost	Popis
Zobrazit všechny testované soubory	Zobrazí všechny testované soubory a jejich stav (infikovaný nebo ne). Výběr této možnosti vede ke zpomalení počítače.
Smazat záznamy starší než [x] dní	V tomto poli můžete specifikovat, jak dlouho mají být zprávy v sekci Záznamy testování uchovávány. Zvolte tuto volbu a napiště nový časový interval. výchozí časový interval je 180 dní.

Poznámka
Soubor se zprávou může být zobrazen v okně **Vlastnosti** v sekci Záznamy testování.

- Specifikujte další možnosti. Otevřete kategorii **Další nastavení**, kde můžete vybrat následující možnosti:

Možnost	Popis
Odeslat podezřelé soubory do laboratoří BitDefender	Po ukončení testování budete moci odeslat všechny podezřelé soubory do laboratoří BitDefender k analýze.

Jestli-že kliknete na **Výchozí**, načte se výchozí nastavení.

Klikněte na **OK** pro uložení změn a uzavření okna.

Další nastavení

Další obecná nastavení testovacího procesu jsou:

Možnost	Popis
Spustit test s nízkou prioritou	Sníží prioritu testovacího procesu, tím se umožní ostatním programům pracovat rychleji. Zvýší se však doba testovacího procesu.
Po dokončení testování vypnout počítač	Vypne počítač po ukončení testovacího procesu.
Odeslat podezřelé soubory do laboratoří BitDefender	Po ukončení testování budete moci odeslat všechny podezřelé soubory do laboratoří BitDefender k analýze.

Možnost	Popis
Minimalizovat okno testování do systray	Minimalizuje testovací okno do systémové lišty, dvojklikem na ikonu BitDefender opět otevřete.

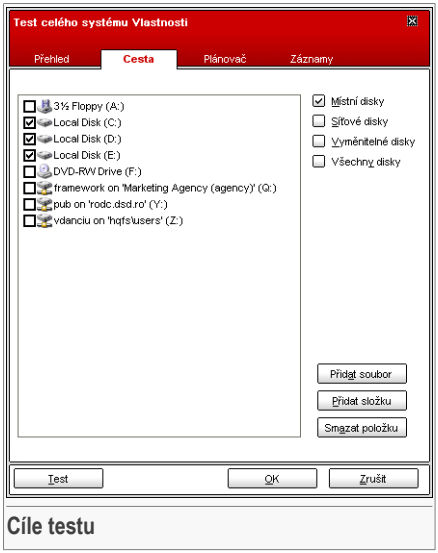
Klikněte na **OK** pro uložení změn a uzavření okna. Pro spuštění testu klikněte na **Test**.

Cíle testu

Pro vstup do této sekce zvolte úlohu, klikněte na **Vlastnosti** a poté klikněte na **Cesta**.

Zde můžete nastavit cíl testování.

Sekce obsahuje tato tlačítka:



Cíle testu

- **Přidat soubor** - otevře okno Procházet, kde si můžete vybrat soubor(y), které chcete testovat.
- **Přidat složku** - v okně Procházet si vyberete složku (složky), které chcete testovat.

Poznámka

Použijte uchopit&přenést pro přidání souborů/složek do seznamu.

- **Smazat položku** - ze seznamu objektů pro testování odstraní ty soubory/složky, které jste na seznam zařadili.

Poznámka

Odstraněny mohou být jen ty soubory/složky, které byly přidány na seznam dodatečně. Nikoli tedy ty, které automaticky "vidí" BitDefender.

Kromě tlačítek popsaných výše existují další možnosti pro rychlou volbu místa testování.

- **Místní disky** - testuje místní disky.
- **Síťové disky** - testuje všechny síťové disky.
- **Vyměnitelné disky** - testuje vyměnitelné disky (CD-ROM, disketovou jednotku).
- **Všechny položky** - testuje všechny disky, místní, síťové či vyměnitelné.

Poznámka

Pokud chcete testovat celý počítač na viry, zaškrtněte volbu **Všechny položky**.

Klikněte na **OK** pro uložení změn a uzavření okna. Pro spuštění testu klikněte na **Test**.

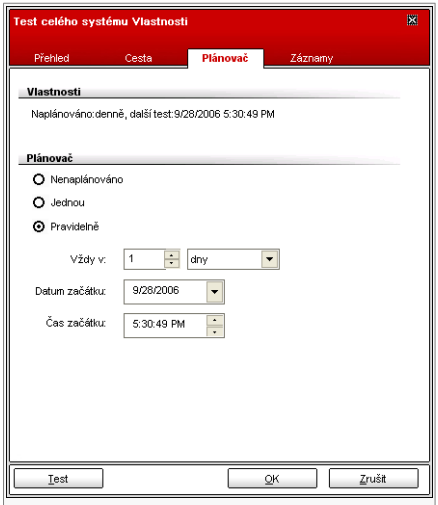
Plánovač

Pro vstup do této sekce zvolte úlohu, klikněte na **Vlastnosti** a poté klikněte na **Plánovač**.

Zde můžete vidět, zda je úloha naplánovaná či ne a upravit její vlastnosti.

Důležité

Jelikož testování zabere určitý čas a funguje nejlépe, když máte zavřené všechny ostatní programy, je pro vás nejlepší naplánovat testování na dobu, kdy nepoužíváte počítač a počítač je v klidovém stavu.



Plánovač

Když plánujete úlohu, musíte zvolit jednu z následujících voleb:

- **Nenaplánováno** - spustí úlohu pouze na vyžádání uživatele.
- **Jednou** - spustí testování jen jednou, v určený okamžik. Upravit datum a čas testu můžete v poli **Datum/Čas spuštění**
- **Pravidelně** - spustí testování opakovaně v určitých časových intervalech (hodiny, dny, týdny, měsíce, roky) počínaje zadaným datem.

  Pokud chcete, aby se testování opakovalo v určitých intervalech, zvolte **Pravidelně** a do polí **Vždy v** vyplňte příslušné číslo dne, měsíce, datum startu a čas opakování procesu testování. Také musíte definovat datum a čas spuštění testu.

Klikněte na **OK** pro uložení změn a uzavření okna. Pro spuštění testu klikněte na **Test**.

Záznamy testování

Pro vstup do této sekce zvolte úlohu, klikněte na **Vlastnosti** a poté klikněte na **Záznamy**.

Zde můžete vidět soubory zpráv vygenerované vždy, když je úloha spuštěna. Ke každému souboru je přiložena informace o jeho stavu (čistý/infikovaný), datum a čas testu a shrnutí (dokončeného testu).

Dostupná jsou dvě tlačítka:

- **Zobrazit záznam** - otevře vybraný soubor se zprávou;
- **Smazat záznam** - smaže vybraný soubor se zprávou.

Prohlédnout či smazat soubor můžete také kliknutím pravým tlačítkem myši na soubor a výběrem odpovídající volby z kontextového menu.

Klikněte na **OK** pro uložení změn a uzavření okna. Pro spuštění testu klikněte na **Test**.

Záznamy testování

7.2.4. Typy testů na požádání

BitDefender nabízí 3 druhy testů na požádání:

- Okamžité testování - spustí testovací úlohu ze systémových/uživatelských úloh;
- Kontextové testování - klikněte pravým tlačítkem myši na soubor nebo složku a vyberte BitDefender Antivirus v10;
- Testování Uchopit&Přenést - uchopte a pusťte daný soubor nebo složku do Grafu průběhu testování;

Okamžité testování

Pro testování vašeho počítače nebo jeho části můžete použít výchozí testovací úlohy, nebo si můžete vytvořit své vlastní úlohy. Zde jsou dvě metody vytvoření testovacích úloh:

- Klikněte na Kopírovat již vytvořenou úlohu, přejmenujte ji a proveďte potřebné změny v okně Vlatnosti;
- Klikněte na **Nová úloha** a nakonfigurujte ji.

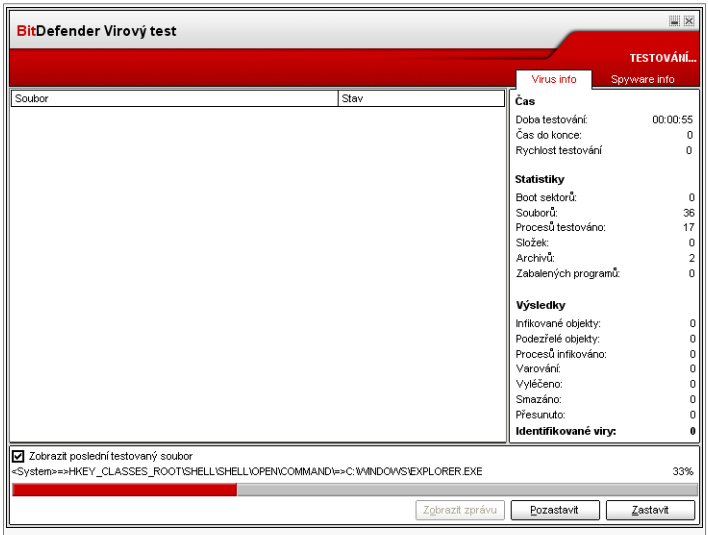
Aby mohl BitDefender provést kompletní testování, musíte zavřít všechny otevřené programy. Zejména je důležité zavřít vašeho e-mailového klienta (tj. Outlook, Outlook Express nebo Eudora).

Předtím, než necháte BitDefender testovat váš počítač, byste si měli ověřit, že je BitDefender aktualizován s virovými signaturami, protože nové viry se objevují denně. Ve spodní části modulu Aktualizace na řídící konzoli BitDefenderu si můžete ověřit, kdy byla provedena poslední aktualizace.

Pro spuštění testování použijte jednu z následujících metod:

- poklepejte na požadovanou úlohu ze seznamu.
- klikněte na tlačítko **Testovat** u požadované úlohy.
- vyberte úlohu a klikněte na **Spustit úlohu**.

Objeví se okno testování.



Okno testu

Pokud běží proces testování, na systémové liště se zobrazí ikona.

Během testování vám BitDefender ukáže jak postupuje a ukáže vám, zda jsou nalezeny nějaké hrozby. Vpravo můžete vidět statistiky týkající se testovacího procesu. V závislosti na testovaném cíli jsou k dispozici informace o spyware a/nebo informace o virech. Pokud je obojí dostupné, klikněte na odpovídající záložku, abyste se o hrozbách dozvěděli více.

Zaškrtnete-li volbu **Zobrazit poslední testovaný soubor**, zobrazí se pouze informace o posledních testovaných souborech.

Poznámka

Testování může trvat delší dobu, v závislosti na velikosti vašeho pevného disku.

Jsou dostupná tři tlačítka:

- **Stop** - objeví se nové okno, v němž můžete testování ukončit. Pro ukončení okna testu klikněte na **Ano**&**Zavřít**.

  Poznámka

  Poklud jsou během testování detekovány podezřelé soubory, budete požádáni o jejich zaslání do laboratoří BitDefender.

- **Pauza** - testování se dočasně zastaví - pro pokračování stiskněte tlačítko **Pokračovat**.
- **Zobrazit zprávu** - otevře se zpráva o testování.

Poznámka

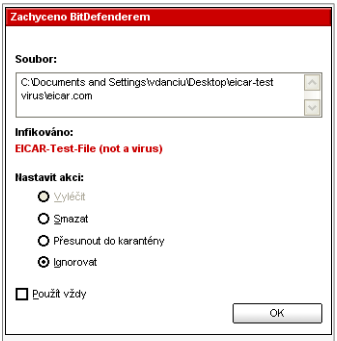
Pokud na spuštěnou úlohu kliknete pravým tlačítkem myši, otevře se kontextové menu, ve kterém budete moci testování ovládat. Volby (**Pauza/ Pokračovat**, **Stop** a **Stop&Zavřít**) mají stejnou funkci jako tlačítka v okně testu.

Pokud je v okně Vlastnosti zatržena volba **Dotázat se na akci uživatele**a bude detekován infikovaný soubor, otevře se výstražné okno s dotazem, jaká akce má být s infikovaným souborem vykonána.

V okně uvidíte název souboru a jméno viru.

Můžete si vybrat jednu z následujících akcí pro infikovaný soubor:

- **Vyléčit** - vyléčí nakažené soubory;
- **Smazat** - smaže infikované soubory;
- **Přesunout do karantény** - přesune infikovaný soubor do karantény;
- **Ignorovat** - ignoruje infekci. U infikovaného souboru nebude provedena žádná akce.



Výběr akce

testujete-li složku a přejete-li si, aby akce byla pro všechny infikované soubory stejná, vyberte možnost **Použit pro všechny**.

Poznámka

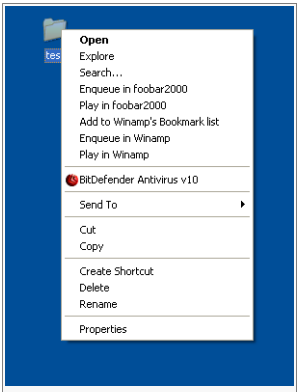
Není-li zpřístupněna možnost **Vyléčit**, znamená to, že soubor nemůže být vyléčen. Nejlepším řešením je buď izolovat daný soubor do karantény a odeslat nám jej na analýzu, nebo jej vymazat.

Klikněte na **OK**.

Poznámka

Soubor s reportem je automaticky uložen do sekce záznamy testování v okně **Vlatnosti** dané úlohy.

Kontextové testování



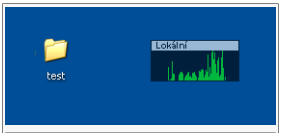
Kontextový test

Pravým tlačítkem myši klikněte na soubor nebo složku, kterou chcete testovat a vyberte možnost **BitDefender Antivirus v10**.

Upravovat nastavení testu a prohlížet si soubory se zprávami můžete v okně Vlastnosti úlohy **Kontextový test**.

Testování Uchopit&Pustit

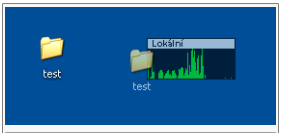
Uchopte soubor nebo složku, kterou chcete testovat a přeneste ji do **Grafu průběhu testování**, tak jak ukazuje obrázek níže.



Uchopte soubor

Pokud je detekován infikovaný soubor, objeví se výstražné okno s dotazem, jaká akce má být s infikovaným souborem provedena.

V obou případech testování (kontextové i uchopit&pustit) se objeví okno testu.



Pusťte soubor

7.2.5. Testování na rootkity

BitDefender přichází vyřešit ty nejnovější bezpečnostní hrozby a představuje rootkit detektor spolu s jeho účinným antivirovým&antispywarovým enginem. Bitdefender je

nyní schopný detekovat rootkity vyhledáváním skrytých souborů, složek a procesů. Navíc je schopen ochránit váš systém přejmenováním záludných programů využívajících rootkity.

Pro testování vašeho počítače na rootkity spusťte úlohu **Testování na rootkity**. Spustí se okno testu.

Důležité

Když testujete na rootkity, je doporučeno nastavit BitDefender aby se skrytými soubory neprováděl žádné akce.

Na konci testování si můžete prohlédnout výsledky. Pokud jsou detekován nějaké skryté soubory, opatrně je zkontrolujte: existence skrytých suborů může znamenat možnou hrozbu.

Pokud si jste jistí, že detekované soubory patří k nebezpečnému programu, doporučujeme nastavit akci **Přejmenovat soubory** a znovu spustit úlohu **Testování na rootkity**. Tímto způsobem bude skrytý soubor zablokován.

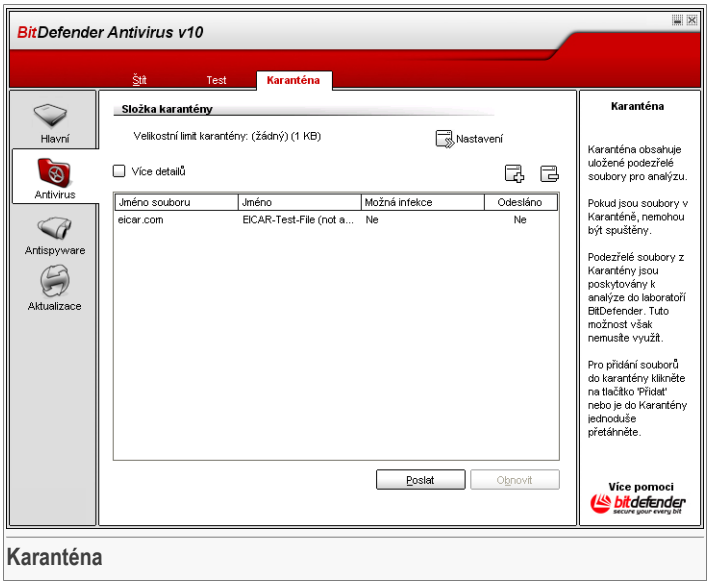
Varování

NE VŠECHNY SKRYTÉ SOUBORY JSOU ŠKODLIVÉ! Před přejmenováním skrytých souborů si musíte být jistí, že nepatří k žádné platné systémové aplikaci. Přejmenováním těchto souborů můžete docílit poškození vašeho systému.

Důležité

Pokud je váš systém napaden, je jedinou bezpečnou cestou čisté přeinstalování systému.

7.3. Karanténa



Karanténa

BitDefender umožňuje izolovat infikované či podezřelé soubory do zabezpečené oblasti, nazvané karanténa. Izolací těchto souborů v karanténě zaniká riziko infikace počítače a současně máte možnost zaslat tyto soubory na následnou analýzu do laboratoře BitDefender.

Modul **Karanténa** slouží pro administraci izolovaných souborů. Tento modul byl vybaven funkcí pro automatické zasílání infikovaných souborů do laboratoře BitDefender.

Sekce **Karanténa** obsahuje seznam všech souborů, které byly dosud izolovány. U každého souboru je uveden jeho název, velikost, datum izolace a datum odeslání. Pro více informací o jednotlivých souborech v karanténě klikněte na **Více detailů**.

Poznámka

Virus v karanténě nemůže způsobit žádnou škodu, protože nemůže být spuštěn nebo přečten.

Pro přidání souboru do karantény klikněte na tlačítko **Přidat**. Otevře se okno, ve kterém vyberete umístění souboru na disku. Tímto způsobem bude soubor do

karantény zkopírován. Pokud chcete soubor do karantény přesunout, musíte zatrhnout pole **Odstranit z původního umístění**. Rychůlejší metodat přidání podezřelých souborů do karantény je uchopit&pustit do seznamu karantény.

Pro odstranění zvoleného souboru z karantény klikněte na tlačítko **Odstranit**. Pokud chcete smazaný soubor obnovit do původního umístění, klikněte na **Obnovit**.

Jakýkoli soubor z karantény můžete odeslat do laboratoře BitDefender kliknutím na **Poslat**.

Důležité

Před odesláním souborů musíte specifikovat některé informace – klikněte na **Nastavení** a vyplňte pole v sekci **Nastavení odesílání**, jak je popsáno níže.

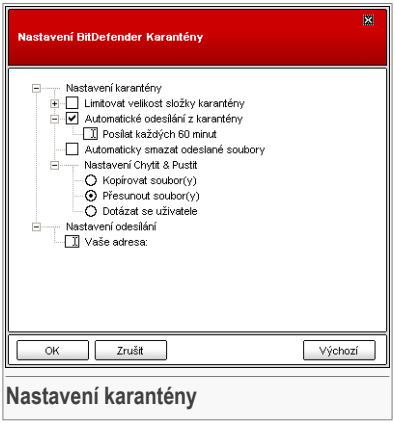
Klikněte **Nastavení** pro otevření pokročilých nastavení karantény. Otevře se nové okno.

Možnosti karantény jsou seskupeny do dvou kategorií:

- **Nastavení karantény**
- **Nastavení odesílání**

Poznámka

Klikněte na "+" pro otevření dalších nastavení a na "–" pro jejich zavření.



Nastavení karantény

Nastavení karantény

- **Limit velikosti složky karantény** - dovoluje mít pod kontrolou velikost celé karantény. Základní velikost je 12000 kB. Pokud chcete tuto hodnotu změnit, napište novou hodnotu do odpovídajícího pole.

  Jestliže vyberete volbu **Automaticky smazat staré soubory**, tak když bude karanténa plná a vy přidáte další soubory, nejstarší soubory v karanténě budou automaticky vymazány za účelem uvolnění místa pro nově přidané soubory.

Poznámka

Ve výchozím nastavení nemá složka karantény žádný velikostní limit.

- **Automatické odesílání** - automaticky odesílá soubory z karantény do laboratoří BitDefender pro další analýzu. V poli **Odeslat každých x minut** můžete nastavit časové rozmezí mezi dvěma odesláními v minutách.
- **Automaticky smazat odeslané soubory** - automaticky vymaže soubory z karantény, poté co byly odeslány do laboratoře BitDefenderu na analýzu.
- **Nastavení Chytit&Pustit** - používáte-li metodu chytit&pustit pro přidávání souborů do karantény, můžete zde specifikovat akci: kopírovat, přesunout nebo dotázat se uživatele.

Nastavení odesílání

- **Váše adresa** - uveďte vaši e-mailovou adresu, pokud si přejete obdržet od našich expertů e-mail o podezřelých souborech odeslaných na analýzu.

Klikněte na **OK** pro uložení změn nebo klikněte na **Výchozí** pro načtení výchozího nastavení.

8. Modul Antispyware

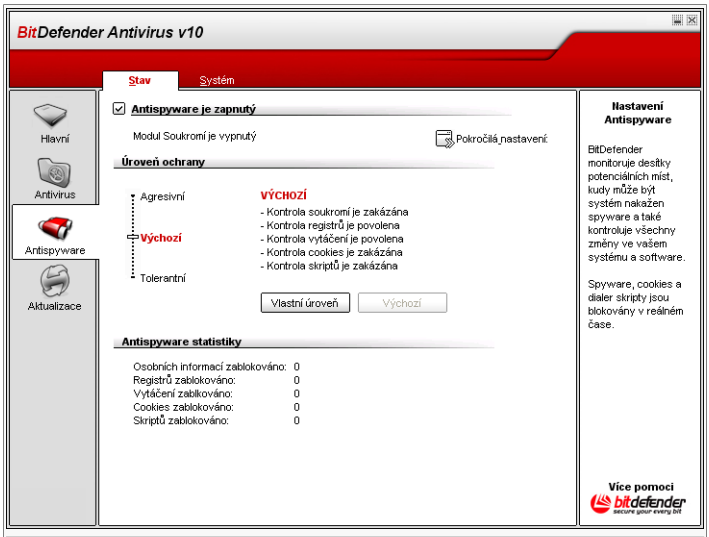
Sekce **Antispyware** této uživatelské příručky obsahuje následující témata:

- Stav Antispywaru
- Pokročilá nastavení - Ochrana soukromí
- Pokročilá nastavení - Kontrola registru
- Pokročilá nastavení - Kontrola vytáčení
- Pokročilá nastavení - Kontrola cookies
- Pokročilá nastavení - Kontrola skriptů
- Systémové informace

Poznámka

Pro více detailů týkajících se modulu **Antispyware** si prohlédněte „*Modul Antispyware*“ (str. 25).

8.1. Stav Antispywaru



Stav Antispywaru

V této sekci můžete konfigurovat modul **Antispyware** a zobrazit informace, které se této aktivity týkají.

Důležité

Abyste ochránili svůj počítač před spywarem, musíte mít zapnutý **Antispyware**.

Ve spodní části této sekce můžete vidět **Statistiky Antispywaru**.

Antispyware chrání váš počítač proti spywaru pomocí 5 důležitých ochranných kontrol:

- Ochrana soukromí - chrání vaše osobní data filtrováním odchozích HTTP a SMTP přenosů podle pravidel vytvořených v sekci Soukromí.
- Kontrola registru - budete upozorněni, kdykoliv se program pokusí modifikovat vstup do registru – následně bude vyřazen ze startovací fáze Windows.
- Kontrola vytáčení - budete upozorněni, kdykoliv se program pokusí přistoupit k počítačovému modemu.

- Zde tedy pomůže právě Kontrola cookies - budete upozorněni vždy když se nová stránka pokouší vytvořit cookie.
- S Kontrola skriptů - budete upozorněni, kdykoliv se webová stránka pokusí aktivovat skript nebo jiný aktivní obsah.

Pro upravení nstavení těchto kontrol klikněte na Pokročilá nastavení.

8.1.1. Úroveň ochrany

Můžete si vybrat úroveň ochrany jakou potřebujete. Pro nastavení požadované úrovně přesuňte posuvník na stupnici.

Existují 3 úrovně ochrany:

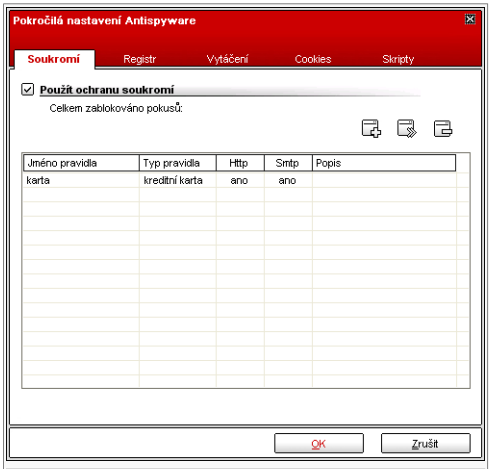
Úroveň ochrany	Popis
Tolerantní	**Kontrola registru**
Výchozí	**Kontrola registru** a **Kontrola vytáčení** jsou zapnuté.
Agresivní	**Kontrola registru**, **Kontrola vytáčení** a **Kontola soukromí** jsou zapnuté.

Upravovat úroveň bezpečnosti můžete kliknutím na **Vlastní úroveň**. V zobrazeném okně zvolte možnosti, které chcete povolit a klikněte na **OK**.

Jestliže stiskněte tlačítko **Výchozí** vrátí se posuvník do standardní polohy.

8.2. Pokročilá nastavení - Kontrola soukromí

Pro vstup do této sekce klikněte na tlačítko **Pokročilá nastavení** z modulu **Antispyware** v sekci Stav.



Kontrola soukromí

Zabezpečení důvěrných dat je tím nejdůležitějším co ná v současnosti trápí. Krádeže dat drží rychlost s vývojem internetové komunikace a stává se tak novou metodou okrádání lidí získáváním jejich důvěrných informací.

Dostane-li se váš e-mail nebo dokonce kreditní karta do špatných rukou, mohou být tyto informace zneužity a můžete se doslova topit ve spamových zprávách nebo můžete být překvapeni přístupem na váš prázdný účet.

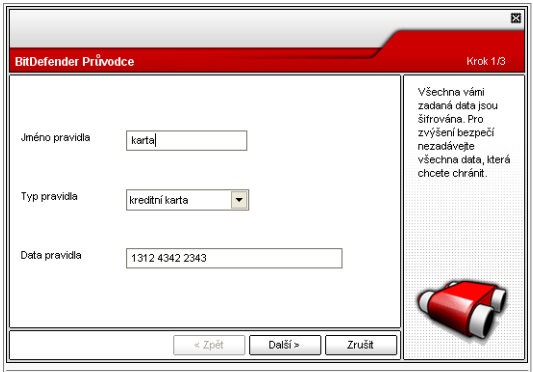
Kontrola soukromí vám pomůže uchovat důvěrná data v bezpečí. Hlídá HTTP a SMTP provoz a hledá určitá slova, která jste definovali. Pokud je takové nalezeno, jsou tyto webové stránky či e-maily zablokovány.

Pravidla mohou být přidána ručně (kliknutím na tlačítko **Přidat** a vybráním parametrů pro toto pravidlo). Bude spuštěn průvodce nastavením.

8.2.1. Průvodce nastavením

Průvodce nastavením má 3 kroky.

Krok 1/3 - Vložení typu a dat pravidla



Vložení typu a dat pravidla

Zadejte do pole jméno pravidla.

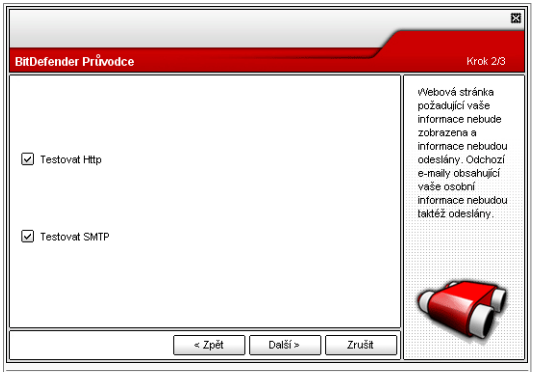
Musíte nastavit následující parametry:

- **Typ pravidla** - zvolte typ pravidla (adresa, jméno, kreditní karta, PIN atd.).
- **Data pravidla** - zadejte data pravidla.

Všechna vámi zadaná data jsou šifrována. Pro vaši bezpečnost ale nezadávejte všechna data, která chcete chránit.

Klikněte na **Další**.

Krok 2/3 - Volba provozu



Volba provozu

Zvolte síťový provoz, který chcete testovat. The following options are available:

- **Testovat HTTP** - testuje HTTP (webový) provoz a blokuje odchozí data odpovídající pravidlům.
- **Testovat SMTP** - testuje SMTP (e-mailový) provoz a blokuje odchozí e-mailové zprávy obsahující data uvedená v previdlech.

Klikněte na **Další**.

Krok 3/3 - Popis pravidla

Popis pravidla

Do pole zadejte krátký popis pravidla.

Klikněte na **Konec**.

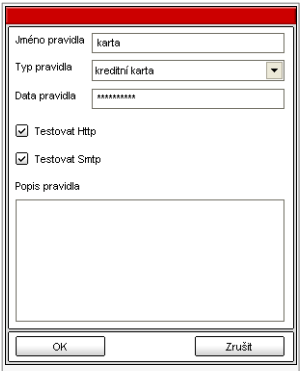
8.2.2. Správa pravidel

Zde můžete v tabulce vidět seznam pravidel.

Pro odstranění pravidla jej vyberte a klikněte na tlačítko **Smazat**. Pro dočasnou deaktivaci pravidla bez jeho odstranění, odškrtněte odpovídající pole.

Pro editaci pravidla na klikněte na tlačítko **Editovat** nebo na něj poklepejte. Otevře se nové okno.

Zde můžete změnit jméno, popis a parametry pravidla (typ, data a provoz). Pro uložení změn klikněte na **OK**.

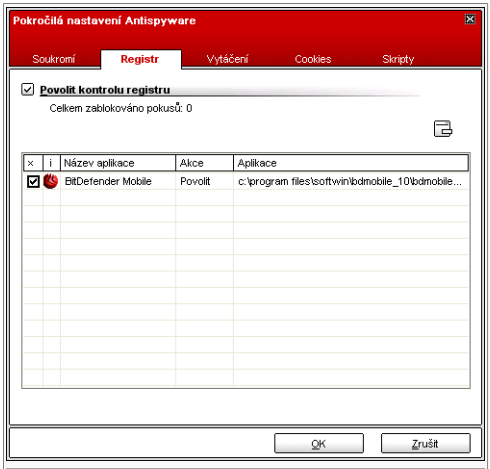


Editace pravidla

Klikněte na **OK** pro uložení změn a uzavření okna.

8.3. Pokročilá nastavení - Kontrola registru

Pro přístup do této sekce otevřete okno **Pokročilá Antispyware nastavení** (přejděte do modulu **Antispyware** do sekce, Stav, klikněte na **Pokročilá nastavení**) a klikněte na záložku **Registr**.



Kontrola registru

Velmi důležitou částí operačního systém Windows je **Registr**. Je to místo, kde Windows uchovávají svoje nastavení, instalované programy, uživatelské informace atd.

Registr slouží i pro definici programů, které mají být spouštěny automaticky při startu Windows. Toho obvykle využívají viry, tak aby byly automaticky spuštěny pokaždé, kdy uživatel restartuje svůj počítač.

Kontrola registru dohlíží nad registrem Windows – důležitá pro odhalování Trojských koní. Budete upozorněni, kdykoliv se program pokusí modifikovat vstup do registru – následně bude vyřazen ze startovací fáze Windows.

Výstraha registru

Tuto modifikaci můžete zamítnout kliknutím na **Ne** nebo povolit kliknutím na **Ano**.

Chcete-li, aby si BitDefender zapamatoval vaši odpověď, zaškrtněte: **Zapamatovat si tuto odpověď'**.

Poznámka

Vaše odpovědi se stanou součástí seznamu pravidel.

Pro smazání položky v registru, nejprve tuto položku vyberte a pak klikněte na tlačítko **Smazat**. Pro dočasné deaktivování zápisu do registru bez mazání odškrtněte odpovídající volbu.

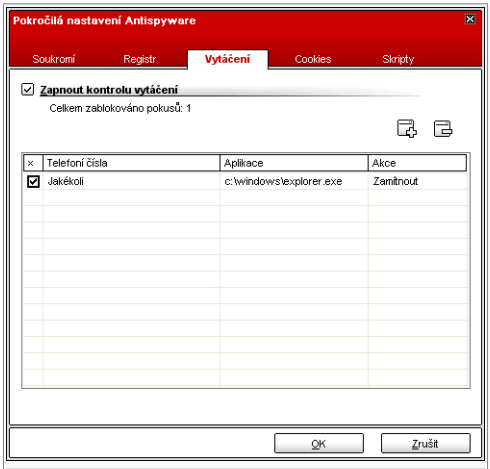
Poznámka

BitDefender vás při instalaci nových programů obvykle upozorní, že je potřeba jej spustit při příštím startu vašeho počítače. Ve většině případů jsou tyto programy důvěryhodné.

Klikněte na **OK** pro uzavření tohoto okna.

8.4. Pokročilá nastavení - Kontrola vytáčení

Pro vstup do této sekce otebřete okno **Pokročilá Antispywarová nastavení** (jděte do nodulu **Antispyware**, sekce Stav, klikněte na **Pokročilá nastavení**) a klikněte na záložku **Vytáčení**.



Kontrola vytáčení

Dialery (voliče telefonních čísel) jsou aplikace, které využívají modemy počítačů tak, aby vytáčely nejrůznější telefonní čísla. Obvykle jsou dialery používány pro vstup do různých umístění s vytáčením velmi drahých telefonních čísel.

S **Kontrolou vytáčení** můžete určovat, která telefonní spojení budou povolena a která blokována. Tato funkce monitoruje všechny dialery pokoušející se o vstup do počítačového modemu, okamžitě varuje uživatele a vyzve jej k rozhodnutí mezi blokací či souhlasem s takovými operacemi:

Výstraha vytáčení

Zde vidíte názvy aplikací a telefonní čísla.

Zaškrtněte volbu **Zapamatovat si tuto odpověď**, pak klikněte na **Ano** nebo na **Ne** a pravidlo bude vytvořeno, aplikováno a zobrazeno v tabulce pravidel. Kdykoliv se bude aplikace pokoušet o vytočení stejného čísla, upozorněni již nebudete.

Do každého pravidla, které jste doporučili, aby si systém zapamatoval, můžete vstoupit v sekci **Vytáčení** a dále jej vyladit.

Důležité

Pravidla jsou seřazena podle priority seshora, první pravidlo má nejvyšší prioritu. Pravidlo můžete chytit a přesunout a tím změnit jeho prioritu.

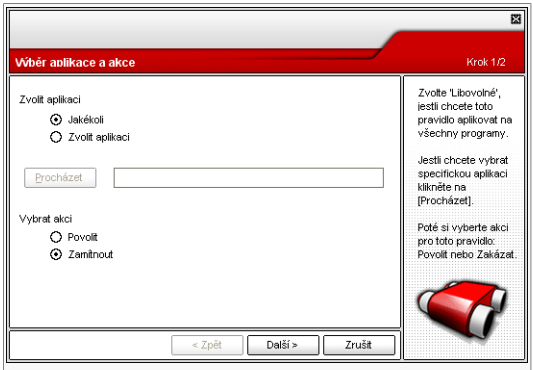
Pro smazání pravidla, je potřeba jej nejprve vybrat a poté kliknout na tlačítko **Smazat**. Pro modifikaci atributů pravidla na ně klikněte dvakrát. Pro dočasnou deaktivaci pravidla bez jeho smazání odškrtněte odpovídající volbu.

Pravidla mohou být přidána automaticky (skrz okno výstrahy) nebo ručně (kliknutím na tlačítko **Přidat** a vybráním parametrů pro toto pravidlo). Bude spuštěn průvodce nastavením.

8.4.1. Průvodce nastavením

Průvodce nastavením má 2 kroky.

Krok 1/2 - Výběr aplikace a akce



Výberte aplikaci a akci

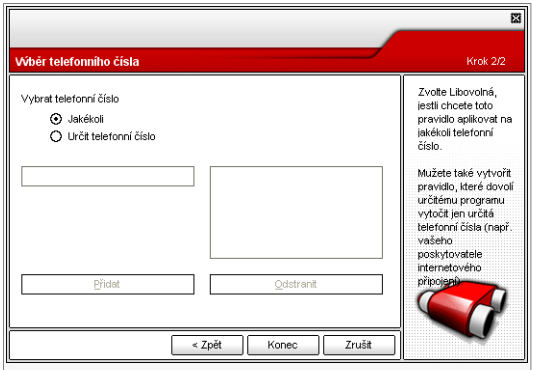
Můžete nastavit parametry:

- **Aplikace** - vyberte aplikaci pro pravidlo. Můžete vybrat buďto jen jednu aplikaci (klikněte na **Zvolit aplikaci**, potom na **Procházet** a vyberte aplikaci), nebo všechny aplikace (klikněte na **Jakékoli**).
- **Akce** - zvolte akci pro pravidlo.

Akce	Popis
Povolit	Akce bude povolena.
Zakázat	Akce bude zakázána.

Klikněte na **Další**.

Krok 2/2 - Výběr telefonního čísla



Vyberte telefonní číslo

Zaškrtněte **Určit telefonní číslo**, pak napište telefonní čísla, pro která chcete vytvořit pravidlo a klikněte **Přidat**.

Poznámka

Můžete použít zástupné znaky na seznamu zakázaných telefonních čísel, např. 1900* znamená, že budou blokována všechna čísla začínající na 1900.

Zaškrtněte **Jakékoli** pokud chcete toto pravidlo aplikovat na všechna telefonní čísla. Chcete-li číslo vymazat, vyberte jej a klikněte na **Odstranit**.

Poznámka

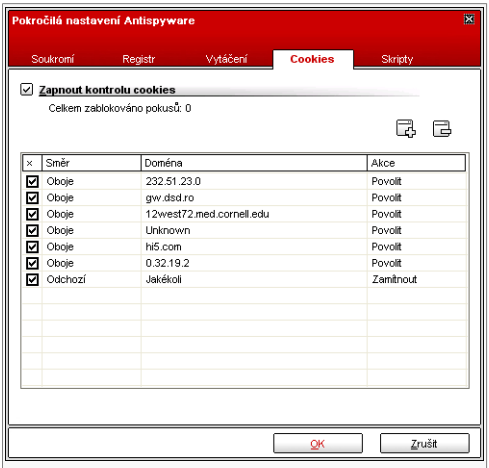
Můžete rovněž vytvořit pravidlo, které povolí určitému programu vytáčet jen určitá čísla (např. číslo vašeho poskytovatele internetu nebo fax news servis).

Klikněte na **Konec**.

Klikněte na **OK** pro uložení změn a uzavření okna.

8.5. Pokročilá nastavení - Kontrola cookies

Pro vstup do této sekce otevřete okno **Pokročilá antispywarová nastavení** (jděte do modulu **Antispyware** sekce, Stav , klikněte na **Pokročilá nastavení**) a klikněte na záložku **Cookies**.



Kontrola cookies

Cookies se na internetu vyskytují zcela běžně. Jsou to malé soubory uložené ve vašem počítači. Webové stránky vytvářejí tyto cookies proto, aby mohli o vás vystopovat určitou informaci.

Obecně jsou cookies dělány proto, aby Vám zjednodušili život. Na příklad pomáhají webové stránce zapamatovat si vaše jméno a preference, takže je nemusíte zadávat každou návštěvu znovu.

Ale cookies mohou být rovněž zneužity ke kompromitaci vašeho soukromí, tím že jsou stopovány vaše surfovací návyky.

Zde tedy pomůže právě **Kontrola cookies**. Pokud je aktivována, požádá vás **Kontrola cookies** o souhlas, vždy když se nová stránka pokouší vytvořit cookie:

Výstraha cookie

Zde vidíte název aplikace, která se pokouší zaslat soubor cookie.

Zaškrtněte volbu **Zapamatovat si tuto odpověď**, pak klikněte na **Ano** nebo na **Ne** a pravidlo bude vytvořeno, aplikováno a zobrazeno v tabulce pravidel. Kdykoliv se v budoucnu připojíte na stenou stránku, upozorněni již nebudete.

Toto vám pomůže rozhodnout se, kterým webovým stránkám věřit a kterým nikoliv.

Poznámka

Z důvodu obrovského množství cookies používaných v dnešní době na internetu je zahájení procesu **Kontroly cookies** zpočátku velmi pracné. Nejprve obdržíte spoustu otázek ohledně stránek, které se pokouší umístit cookies na váš počítač. Jakmile doplníte vaše řádné stránky do seznamu pravidel, stane se surfování tak snadným jako dříve.

Do každého pravidla, které jste doporučili, aby si systém zapamatoval, můžete vstoupit v sekci **Cookies** a dále jej doladit.

Důležité

Pravidla jsou seřazena podle priority seshora, první pravidlo má nejvyšší prioritu. Pravidlo můžete chytit a přesunout a tím změnit jeho prioritu.

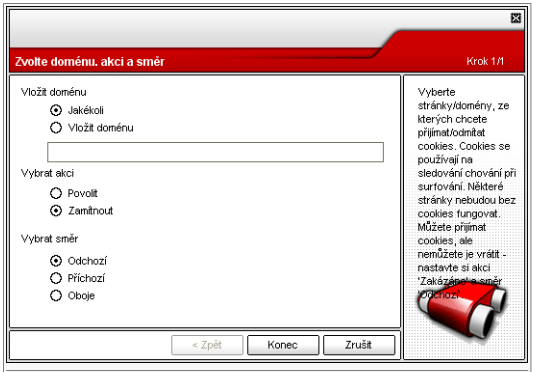
Pro smazání pravidla, je potřeba jej nejprve vybrat a poté kliknout na tlačítko **Smazat**. Pro modifikaci atributů pravidla na ně klikněte dvakrát. Pro dočasnou deaktivaci pravidla bez jeho smazání odškrtněte odpovídající volbu.

Pravidla mohou být přidána automaticky (skrz okno výstrahy) nebo ručně (kliknutím na tlačítko **Přidat** a vybráním parametrů pro toto pravidlo). Bude spuštěn průvodce nastavením.

8.5.1. Průvodce nastavením

Průvodce nastavením má 1 krok.

Krok 1/1 - Zvolte adresu, akci a směr



Vyberte adresu, akci a příkaz

Můžete nastavit parametry:

- **Adresa domény** - napište doménu, na níž má být pravidlo aplikováno.
- **Akce** - zvolte akci pro pravidlo.

Akce	Popis
Povolit	Cookies z této domény budou provedeny.
Zakázat	Cookies z této domény nebudou provedeny.

- **Směr** - vyberte směr spojení.

Typ	Popis
Odchozí	Pravidlo bude aplikováno pouze pro cookies, které jsou odeslány zpět na připojenou stránku.
Příchozí	Pravidlo bude aplikováno, pouze pro cookies, které jsou získané z připojené stránky.
Obojí	Pravidlo se použije pro oba směry.

Klikněte na **Konec**.

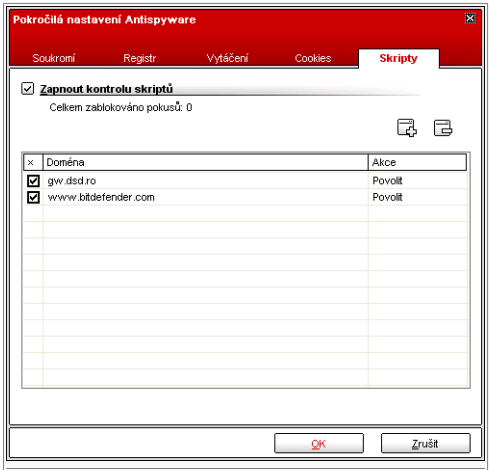
Poznámka

Můžete akceptovat cookies, ale nikdy je nevracet nastavením akce **Zakázat** a směru **Odchozí**.

Klikněte na **OK** pro uložení změn a uzavření okna.

8.6. Pokročilá nastavení - Kontrola skriptů

Pro vstup do této sekce otevřete okno **Pokročilá anitspywarová nastavení** (jděte do modulu **Antispyware**, sekce Stav, klikněte na **Pokročilá nastavení**) a klikněte na záložku **Skripty**.

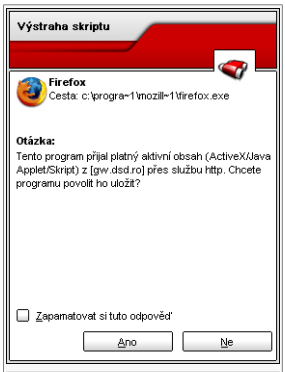


Kontrola skriptů

Skripty a ostatní kódy jako jsou ActiveX prvky a Java applety, které jsou používány při vytváření interaktivních webových stránek, mohou být naprogramovány tak, aby měly škodlivé účinky. Elementy Active X, mohou na příklad, dosáhnout úplného přístupu k vašim datům – mohou pak číst data z vašeho počítače, mazat informace, zachytit hesla a odchytávat zprávy, když jste on-line. Aktivní obsah byste měli akceptovat jen u těch stránek, které zcela znáte a důvěřujete jim.

BitDefender vám umožní spustit tyto prvky nebo je zablokovat.

S **kontrolou skriptu** můžete rozhodovat o stránkách, kterým důvěřujete a kterým ne. BitDefender vás požádá o souhlas, kdykoliv se webová stránka pokusí aktivovat skript nebo jiný aktivní obsah:



Výstraha skriptu

Zde vidíte název zdroje.

Zaškrtněte volbu **Zapamatovat si tuto odpověď**, pak klikněte na **Ano** nebo na **Ne** a pravidlo bude vytvořeno, aplikováno a zobrazeno v tabulce pravidel. Kdykoliv se v budoucnu stejna stranka pokusi o poslání aktivního obsahu, upozorněni již nebudete.

Do každého pravidla, které jste doporučili, aby si systém zapamatoval, můžete vstoupit v sekci **Skripty** a dále jej vyladit.

Důležité

Pravidla jsou seřazena podle priority seshora, první pravidlo má nejvyšší prioritu. Pravidlo můžete chytit a přesunout a tím změnit jeho prioritu.

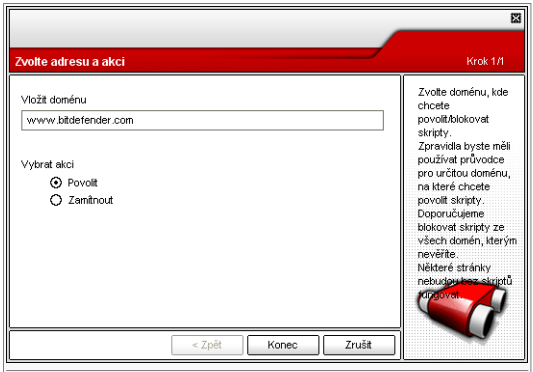
Pro smazání pravidla, je potřeba jej nejprve vybrat a poté kliknout na tlačítko **Smazat**. Pro modifikaci atributů pravidla na ně klikněte dvakrát. Pro dočasnou deaktivaci pravidla bez jeho smazání odškrtněte odpovídající volbu.

Pravidla mohou být přidána automaticky (skrz okno výstrahy) nebo ručně (kliknutím na tlačítko **Přidat** a vybráním parametrů pro toto pravidlo). Bude spuštěn průvodce nastavením.

8.6.1. Průvodce nastavením

Průvodce nastavením má 1 krok.

Krok 1/1 - Výběr aplikace a akce



Vyberte aplikaci a akci

Můžete nastavit parametry:

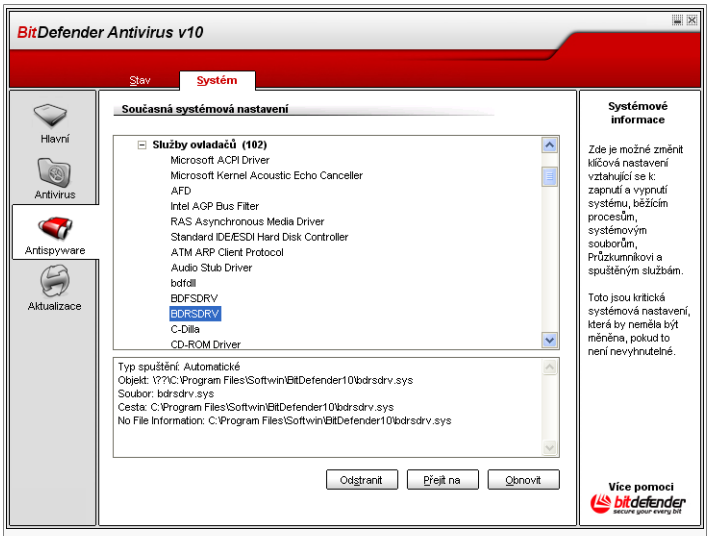
- **Adresa domény** - napište doménu, na níž má být pravidlo aplikováno.
- **Akce** - zvolte akci pro pravidlo.

Akce	Popis
Povolit	Skripty na doméně budou spuštěny.
Zakázat	Skripty na doméně nebudou spuštěny.

Klikněte na **Konec**.

Klikněte na **OK** pro uložení změn a uzavření okna.

8.7. Systémové informace



Systémové informace

Zde můžete vidět a měnit nastavení o informacích.

Seznam obsahuje všechny položky nahrané při startu systému právě tak jako položky nahrané různými aplikacemi.

Jsou dostupná tři tlačítka:

- **Odstranit** - vymaže vybranou položku.
- **Přejít na** - otevře okno s umístěním aktuální položky (například **Registr**).
- **Obnovit** - znovu otevře sekci **O systému**.

9. Modul Aktualizace

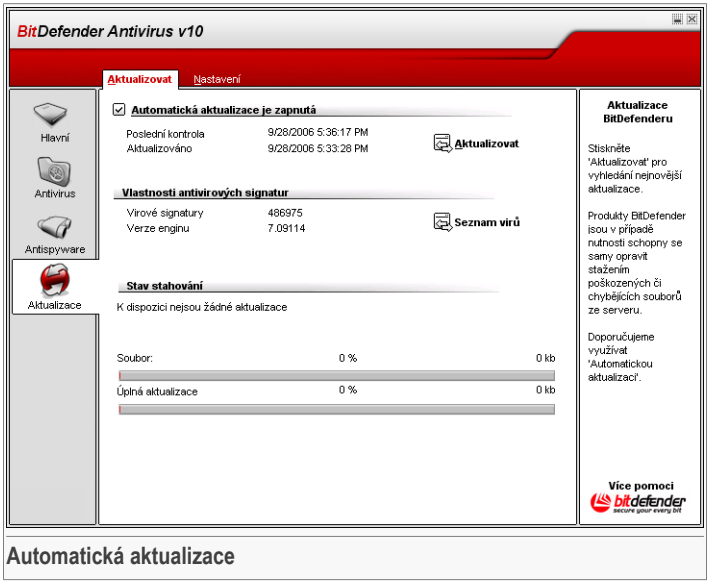
Aktualizační část této uživatelské příručky obsahuje následující témata:

- Automatická aktualizace
- Ruční aktualiazce
- Nastavení aktualizací

Poznámka

Podrobnější informace týkající se modulu **Aktualizace** najdete v kapitole *„Modul Aktualizace“* (str. 26).

9.1. Automatická aktualizace



Automatická aktualizace

V této sekci můžete vidět informace o aktualizaci a aktualizace spuštět.

Důležité

Pro zajištění trvalé ochrany před nejnovějšími hrozbami udržujte **Automatickou aktualizaci** zapnutou.

Jestliže jste připojeni k Internetu širokopásmovým nebo DSL připojením, pečuje o sebe BitDefender sám. Kontroluje nové virové podpisy po zapnutí vašeho počítače a každou následující **hodinu**.

Jestli byla objevena aktualizace v závislosti na volbách nastavených v části Možnosti automatické aktualizace, budete dotázáni k potvrzení aktualizačního procesu nebo bude aktualizace provedena automaticky.

Automatická aktualizace může být také provedena kdykoliv budete chtít kliknutím na **Aktualizovat**. Tato aktualizace je také známa jako **Aktualizace vyžádaná uživatelem**.

Aktualizační modul se připojí k aktualizačním serverům BitDefenderu a ověří, jestli je nějaká aktualizace k dispozici. Pakliže je nějaká aktualizace objevena v závislosti na volbách nastavených v Nastavení manuální aktualizace, buďto budete vyzváni k potvrzení aktualizace, nebo aktualizace proběhne automaticky.

Důležité

Po ukončení aktualizace může být nezbytné restartovat počítač. Doporučujeme tak učinit co nejdříve.

Poznámka

Jestliže jste připojení k Internetu vytáčenou linkou, doporučujeme zvyknout si provádět aktualizaci BitDefenderu ručně uživatelem.

Signatury záludných programů můžete získat kliknutím na **Seznam virů**. Bude vytvořen soubor HTML, který bude obsahovat všechny dostupné signatury. Pro prohlédnutí si tohoto seznamu klikněte znovu na **Seznam virů**. V databázi můžete vyhledávat specifickou signaturu nebo kliknout na **BitDefender seznam virů** pro přechod do online BitDefender databáze signatur.

9.2. Ruční aktualizace

Tato metoda dovolí instalaci nejnovějších virových definic. Pro instalaci nejnovějších aktualizací produktu použijte Automatickou aktualizaci.

Důležité

Užívejte ruční aktualizaci tehdy, když automatická aktualizace nemůže být vykonána nebo když počítač není připojený k Internetu.

Existují 2 cesty, jak vykonat ruční aktualizaci:

- `weekly.exe` soubor;
- `zip archivy`.

9.2.1. Ruční aktualizace pomocí `weekly.exe`

Aktualizační balíček `weekly.exe` je vydáván každý pátek a zahrnuje všechny virové definice a aktualizuje testovací rozhraní k danému datu dostupné.

Pro aktualizaci BitDefenderu pomocí `weekly.exe` dodržte následující kroky:

1. Stáhněte weekly.exe a uložte ho na vašem pevném disku.
2. Najděte stáhnutý soubor a poklepejte na něj, tím spustíte aktualizaci.
3. Klikněte na **Další**.
4. Zaškrtněte **I accept the terms in the License Agreement** a klikněte na **Next**.
5. Klikněte na **Install**.
6. Klikněte na **Konec**.

9.2.2. Ruční aktualizace pomocí `zip archivů`

Na aktualizačních serverech existují dva soubory obsahující aktualizace testovacího rozhraní a virové podpisy: `cumulative.zip` a `daily.zip`.

- `cumulative.zip` je aktualizován každý týden v pondělí a zahrnuje všechny do té doby známé virové definice a aktualizace testovacího rozhraní.
- `daily.zip` je aktualizován každý den a zahrnuje všechny do té doby známé virové definice a aktualizace testovacího rozhraní.

BitDefender používá architekturu založenou na službě. Proto se procedura nahrazení virových definic liší v závislosti na operačním systému:

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

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

Body, které musí být splněny:

1. **Stáhněte příslušnou aktualizaci.** Jestliže je pondělí, stahujte prosím cumulative.zip a uložte ho někde na vašem disku. Jinak prosím stahujte daily.zip a uložte ho někde na vašem disku. Jestli provádíte ruční aktualizaci poprvé, stáhněte prosím oba archivy.
2. **Vypněte BitDefender antivirovou ochranu.**

- **Vypněte BitDefender řídící konzoli.** Klikněte pravým tlačítkem na ikonku BitDefenderu v Systémové liště a vyberte **Ukončit**.
- **Otevřete služby.** Otevřete nabídku **Start**, vyberte **Ovládací panely**, klikněte na **Nástroje pro správu** a potom na **Služby**.
- **Zastavte službu BitDefender Virus Shield.** Vyberte **BitDefender Virus Shield** ze seznamu a klikněte na **Zastavit**.
- **Zastavte službu BitDefender Scan Server.** Vyberte **BitDefender Scan Server** ze seznamu a klikněte na **Zastavit**.

3. **Rozbalte obsah archivu.** Začněte s `cumulative.zip` pokud jsou k dispozici obě aktualizace. Rozbalte obsah do složky `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` a potvrďte přepsání stávajících souborů.
4. **Restartujte Antivirovou ochranu BitDefenderu.**
   - **Zapněte službu BitDefender Scan Server.** Vyberte **BitDefender Scan Server** ze seznamu a klikněte na **Spustit**.
   - **Zapněte službu BitDefender Virus Shield.** Vyberte **BitDefender Virus Shield** ze seznamu a klikněte na **Spustit**.
   - **Otevřete řídící konzoli BitDefenderu.**

Poznámka

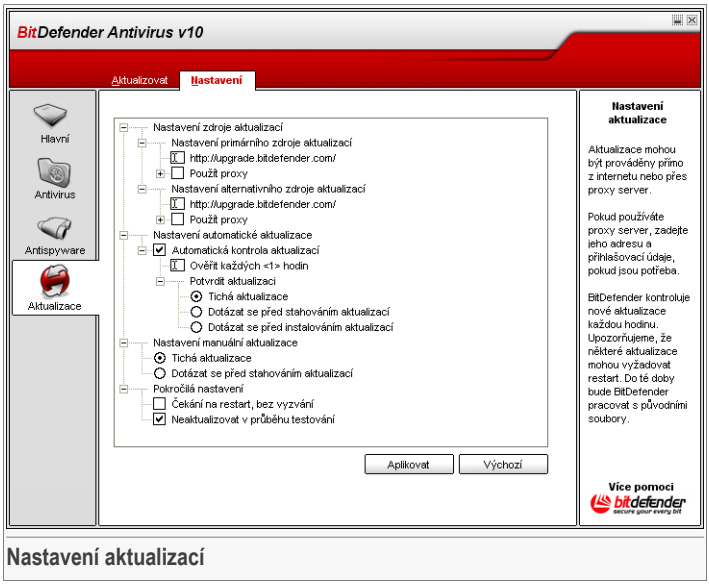
Pokud máte nainstalovány Windows Vista, budete požádáni o potvrzení většiny těchto akcí.

Windows 98, Windows Millennium

Body, které musí být splněny:

1. **Stáhněte příslušnou aktualizaci.** Jestliže je pondělí, stahujte prosím cumulative.zip a uložte ho někde na vašem disku. Jinak prosím stahujte daily.zip a uložte ho někde na vašem disku. Jestli provádíte ruční aktualizaci poprvé, stáhněte prosím oba archivy.
2. **Rozbalte obsah archivu.** Začněte s `cumulative.zip` pokud jsou k dispozici obě aktualizace. Rozbalte obsah do složky `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` a potvrďte přepsání stávajících souborů.
3. **Restartujte počítač.**

9.3. Nastavení aktualizací



Nastavení aktualizací

Aktualizace může být provedena z lokální sítě nebo z internetu přímo přes proxy server.

Okno s nastavením aktualizací obsahuje 4 kategorie možností (**Nastavení zdroje aktualizací**, **Nastavení automatické aktualizace**, **Nastavení manuální aktualizace** a **Pokročilá nastavení**) uspořádané v rozbalovacím menu, podobně jako ve Windows.

Poznámka

Klikněte na znaménko "+" pro otevření kategorie a na znaménko "–" pro zavření kategorie.

9.3.1. Nastavení aktualizací

Pro rychlejší aktualizace můžete nastavit dvě lokality: **Nastavení primárního zdroje aktualizací** a **Nastavení sekundárního zdroj aktualizací**. Pro obě lokality musíte nastavit následující:

- **Aktualizační lokalita** - Pokud jste připojeni do sítě, která používá BitDefender signatury lokálně, změňte toto nastavení. Výchozí hodnota je: http://upgrade.bitdefender.com.
- **Použít proxy** - v případě, že využíváte proxy server, zvolte tuto možnost. Musí být specifikováno následující:
  - **Nastavení proxy** - uveďte IP adresu nebo název proxy serveru a port, který BitDefender používá pro připojení k proxy serveru.

    Důležité
    Syntaxe: `název:port` nebo `ip:port`.

  - **Uživatel proxy** - uveďte uživatelské jméno, které používáte pro proxy.

    Důležité
    Syntaxe: `doména\uživatel`.

  - **Heslo proxy** - uveďte platné heslo pro výše uvedeného uživatele.

9.3.2. Možnosti automatické aktualizace

- **Automatická kontrola aktualizací** - BitDefender automaticky kontroluje, zda jsou na serverech dostupné nové aktualizace.
- **Ověřit každých x hodin** - Nastavení, jak často BitDefender kontroluje dostupnost aktualizací. Výchozí hodnota je 1 hodina.
- **Tichá aktualizace** - BitDefender automaticky stáhne a nahraje aktualizaci.
- **Dotázat se před stahováním aktualizací** - před stažením nové aktualizace budete dotázáni.
- **Dotázat se před instalováním aktualizací** - po stažení aktualizace budete dotázáni, zda má být provedena její instalace.

Důležité
Pokud zvolíte **Dotázat se před stahováním aktualizací** nebo **Dotázat se před instalováním aktualizací** a zvolíte ukončit a zavřít management konzoli, automatická aktualizace nebude provedena.

9.3.3. Nastavení manuální aktualizace

- **Tichá aktualizace** - manuální aktualizace bude provedena na pozadí.
- **Dotázat se před stahováním aktualizací** - při provádění manuální aktualizace budete pokaždé dotázáni před stažením nové aktualizace.

Důležité

Pokud zvolíte **Dotázat se před stahováním aktualizací** a zvolíte ukončit a zavřít management konzoli, aktualizace nebude provedena.

9.3.4. Pokročilá nastavení

- **Čekat na restart, bez vyzvání** - Pokud aktualizace vyžaduje restart, produkt bude nadále pracovat s původními soubory, dokud počítač nebude restartován. Uživatel nebude k restartu počítače vyzýván, takže jej aktualizace BitDefenderu nebude vyrušovat při práci.
- **Neprovádět aktualizaci v průběhu testování** - BitDefender se nebude aktualizovat, pokud běží testovací proces. Jedině tak nebude BitDefender aktualizační proces zasahovat do právě testovaných úkolů.

Poznámka

Jestliže je BitDefender aktualizován v momentě, kdy probíhá testování, proces bude považován za nezdařený.

Klikněte na **Použít** pro uložení změn. Pokud kliknete na **Výchozí**, bude načteno výchozí nastavení.

Doporučený postup

10. Doporučený postup

Sekce **Doporučený postup** této uživatelské příručky obsahuje následující témata:

- Jak ochránit váš počítač před virovými útoky
- Jak nastavit testovací úlohu

10.1. Jak ochránit váš počítač před virovými útoky

Pro ochranu vašeho počítače před útoky virů, spyware a ostatních záludných programů následujte tyto kroky:

1. **Dokončení průvodce prvotním nastavením.** Během instalace bude spuštěn průvodce. Pomůže vám s registrací BitDefenderu a vytvořením BitDefender účtu, abyste mohli čerpat výhody bezplatné technické podpory. Také vám pomůže s nastavením BitDefenderu a důležitých bezpečnostních úloh.

   Důležité

   Máte-li záchranné CD BitDefenderu, otestuje před instalací BitDefenderu celý váš systém, aby byla vyloučena přítomnost škodlivých programů.

2. **Aktualizace BitDefenderu.** Pokud jste během instalace nedokončili průvodce prvotním nastavením, učiňte tak ručně (jděte do modulu **Aktualizace**, sekce Aktualizace a klikněte na **Aktualizovat**).

3. **Provedení testu celého systému.** Vstupte do modulu **Antivirus**, sekce Štít a klikněte na **Testovat**.

   Poznámka

   Spustit test celého systému můžete také v sekci Test. Zvolte **Test celého systému** a klikněte na **Spustit**.

4. **Prevence nákazy.** v sekci **Štít** mějte zapnutý Virový štít, abyste byli chráněni proti virům, spyware a ostatním škodlivým programům. Nastavte takovou úroveň ochrany, kterou potřebujete. Tuto můžete upravit kdykoli budete chtít, kliknutím na **Vlastní úroveň**.

   Důležité

   Nastavte váš BitDefender Antivirus v10, aby testoval váš systém nejméně jednou týdně, naplánováním úlohy **Test celého systému** v sekci Test.

5. **Aktualizace BitDefenderu.** V modulu **Aktualizace**, sekci Aktualizace, mějte zapnuto **Automatická aktualizace**, abyste byli chránění proti nejnovějším hrozbám.
6. **Naplánování testu celého systému.** Jděte do sekce **Test** a nastavte BitDefender k testování celého systému alespoň jednou týdně naplánováním úlohy **Test celého systému**.

10.2. Jak nastavit testovací úlohu

Pro vytvoření a konfiguraci testovací úlohy následujte tyto kroky:

1. **Vytvoření nové úlohy.** Jděte do sekce Test a klikněte na **Nová úloha**. Otevře se okno Vlastnosti.

   Poznámka

   Vytvořit novou úlohu můžete také zkopírováním jedné již vytvořené. Klikněte pravým tlačítkem myši na úlohu a v kontextovém menu zvolte **Zkopírovat**. Zvolte kopii a klikněte na **Vlastnosti** pro otevření okna **Vlastnosti**.

2. **Nastavení úrovně testování.** Pro nastavení úrovně testování jděte do sekce **Přehled**. Pokud chcete, můžete upravit nastavení testování kliknutím na **Vlastní**.
3. **Výběr cíle testování.** Jděte do sekce **Cesta testování** a vyberte objekty, které mají být testovány.
4. **Plánování úlohy.** Pokud je testovací úloha komplexní, můžete ji chtít naplánovat na později, až bude váš počítač v klidu. To pomůže BitDefenderu pečlivě otestovat váš systém. Jděte v sekci **Plánovač** na naplánovat úlohu.

Záchranné CD BitDefenderu

BitDefender Antivirus v10 přináší bootovatelné CD (Záchranné CD BitDefenderu založené na LinuxDefenderu) schopné testovat a léčit všechny existující pevné disky před startem operačního systému.

Měli byste použít Záchranné CD BitDefenderu, kdykoli váš operační systém nepracuje správně díky virové nákaze. Ta většinou nastane, pokud nepoužíváte Antivirový produkt.

Aktualizace virových podpisů je provedena automaticky bez uživatelského zásahu pokaždé, když nabootujete ze záchranného CD BitDefenderu.

LinuxDefender je BitDefenderem přepracovaná verze Knoppixu, která integruje nejnovější BitDefender Linuxové zabezpečení do GNU/Linux Knoppix CD nabízející okamžitou SMTP Antivirovou a Antispamovou ochranu a Antivirus,který je schopný testovat a léčit existující pevné disky (včetně Windows NTFS oddílů), vzdálené správy Samba/Windows nebo NFS přípojných bodů. Rozhraní na bázi internetového prohlížeče je v BitDefenderu také zahrnuté.

11. Přehled

Hlavní rysy

- Okamžitá emailová ochrana (Antivirus & Antispam)
- Antivirová ochrana pro váš pevný disk
- Podpora pro zápis NTFS (používá návrh Captive project)
- Vyléčení nakažených souborů z oddílů Windows XP

11.1. Co je KNOPPIX?

Citace z 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. Systémové požadavky

Před nabootováním LinuxDefenderu musíte prvně ověřit, zda váš systém splňuje následující požadavky.

Procesor

x86 kompatibilní, minimálně 166 MHz, ale v tomto případě neočekávejte příliš velký výkon. Řada procesorů i686 okolo 800MHz bude lepší volbou.

Paměť

Minimální přijatelná hodnota je 64MB, pro lepší výkon doporučujeme 128MB.

CD-ROM

LinuxDefender se spuští z CD, proto je potřeba vlastnit CD-ROM a BIOS schopný z něho bootovat.

Internetové připojení

Přestože LinuxDefender spustíte i bez internetového připojení, aktualizační procedury vyžadují aktivní HTTP adresy, dokonce i přes proxy server. Proto je pro aktualizovanou ochranu internetové připojení NUTNOSTÍ.

Grafické rozlišení

Pro internetovou správu je doporučeno grafické rozlišení minimálně 800x600.

11.3. Obsažený software

Záchranné CD BitDefenderu zahrnuje následující programové vybavení.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- BitDefender Vzdálená správa (internetové uspořádání)
- BitDefender Linux Edition (Antivirový skener) + GTK Rozhraní
- BitDefender Dokumentace (formát PDF & HTML)
- BitDefender Extra (Obrázky, Letáky)
- Linux-Kernel 2.6
- NTFS - zápis pomocí Captive project
- LUFS - Linux Userland systém souborů
- Nástroje pro obnovu dat a opravu systému, i pro jiné operační systémy
- Nástroje pro síťovou a zabezpečovací analýzu pro administrátory sítí
- Zálohovací systém Amanda
- THTTPD
- Analyzátor síťových spojení, IPTraf IP LAN monitorovací program
- Nessus program pro revizi síťové bezpečnosti
- Nástroj pro změnu, zálohu a obnovu Rozdělených, QTParted a partimage souborů
- Adobe Acrobat Reader
- Internetový prohlížeč Mozilla Firefox

11.4. BitDefender Linux bezpečnostní řešení

LinuxDefender CD zahrnuje BitDefender SMTP Proxy Antivirus/Antispam pro Linux, BitDefender Vzdálenou správu (internetové rozhraní pro konfiguraci BitDefenderu SMTP Proxy) a BitDefender Linuxové vydání pro testování virů.

11.4.1. BitDefender SMTP Proxy

BitDefender pro Linuxové poštovní servery - SMTP Proxy je bezpečné řešení kontroly obsahu, které poskytne antivirovou a antispamovou ochranu na úrovni brány tím, že testuje všechny e-mailové zprávy na známé a neznámé nebezpečné programy. Výsledkem jedinečné patentované technologie BitDefender pro poštovní servery je kompatibilní s většinou existujících e-mailových platforem a "RedHat Ready" úředně ověřený.

Toto Antivirové a Antispamové řešení testuje, léčí a filtruje e-maily stávajícího poštovního serveru bez ohledu na platformu a operační systém. BitDefender SMTP

Proxy je startován v čase bootování operačního systému a testuje všechny příchozí e-maily. Pro konfiguraci BitDefender SMTP Proxy použijte BitDefender Vzdálenou správu pomocí instrukcí popsaných dále.

11.4.2. BitDefender Vzdálená správa

Můžete konfigurovat a spravovat služby BitDefenderu vzdáleně (poté, co jste nastavili vaši síť) nebo lokálně pomocí následujících kroků:

1. Spusťte prohlížeč Firefox a spusťte BitDefender Vzdálenou správu URL: https://localhost:8139 (nebo poklikejte na ikonu BitDefender Vzdálené správy na vaší ploše)
2. Přihlaste se jako uživatel "bd" s heslem "bd"
3. Vyberte "SMTP Proxy" v nabídce na levé straně
4. Nastavte skutečný SMTP server a naslouchací port
5. Přidejte e-mailové domény k přenosu
6. Přidejte síťové domény k přenosu
7. Vyberte "AntiSpam" v nabídce nalevo ke konfiguraci schopností Antispamu
8. Vyberte "Antivirus" ke konfiguraci akcí BitDefender Antiviru (co dělat, pokud je nalezen vir,umístění karantény)
9. Dále můžete nastavit "poštovní oznámení" a přístupová práva ("Log")

11.4.3. BitDefender Linuxové vydání

Antivirový skener zahrnutý v LinuxDefenderu je integrovaný přímo do desktopu. Tato verze je charakteristická pro GTK+ grafické rozhraní.

Jen brouzdejte vašim pevným diskem (nebo vzdáleným namountovaným), klikněte pravým tlačítkem na nějaký soubor nebo složku a vybere "Testovat pomocí BitDefenderu". BitDefender Linuxové vydání bude testovat vybrané položky a zobrazi výslednou zprávu. Pro upřesňující nastavení se podívejte do dokumentace BitDefender Linuxové Vydání (ve složce BitDefender Dokumentace nebo v manuálových stránkách) a také na program **/opt/BitDefender/lib/bdc**.

12. LinuxDefender - Jak na to

12.1. Spuštění a ukončení

12.1.1. Spuštění LinuxDefenderu

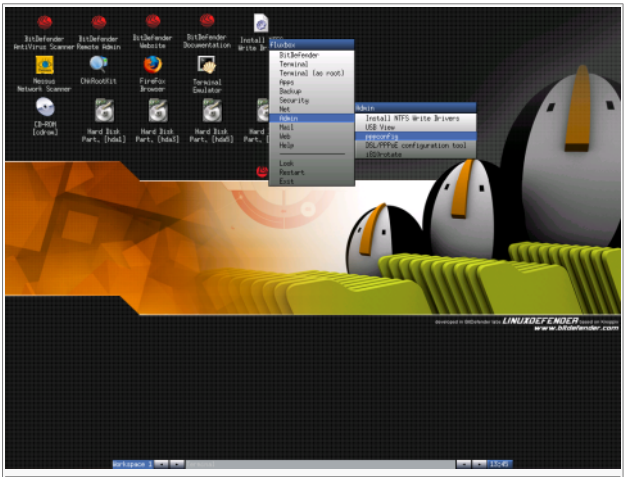
Ke spuštění CD nastavte BIOS vašeho počítače na bootování z CD, vložte CD do mechaniky a restartujte počítač. Ujistěte se, že váš počítač může bootovat z CD.

Počkejte, než se objeví následující obrazovka, abyste spustili LinuxDefender, následujte instrukce na obrazovce.

Bootovací obrazovka

Stiskněte `F2` pro detailní nastavení. Stiskněte `F3` pro detailní nastavení v němčině. Stiskněte `F4` pro detailní nastavení ve francouzštině. Stiskněte `F5` pro detailní nastavení ve španělštině. Pro rychlý start se standardním nastavením pouze stiskněte `ENTER`.

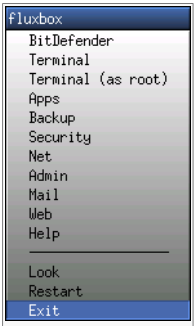
Poté, co je dokončen proces bootovaní, spatříte další obrazovku. Nyní můžete začít používat LinuxDefender.



Plocha

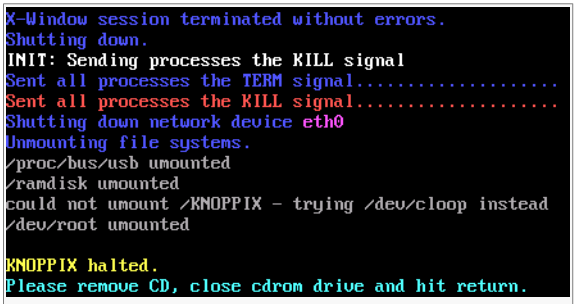
12.1.2. Ukončení LinuxDefenderu

Pro bezpečné ukončení LinuxDefenderu doporučujeme odebrat všechny namountované úseky použitím příkazu **umount** nebo kliknutím pravého tlačítka myši na ikonky úseků na ploše a vyberte **Unmount**. Pak vy můžete bezpečně vypnout váš počítač výbráním **Exit** nabídky LinuxDefenderu (klikněte pravým tlačítkem myši k jeho otevření) nebo zadáním příkazu **halt** do terminálu.



Volba "EXIT"

Poté, co LinuxDefender úspěšně ukončil všechny programy, objeví se obrazovka podobná té následující. Můžete odstranit CD, abyste mohli nabootovat z vašeho pevného disku. Nyní můžete bezpečně vypnout váš počítač nebo ho restartovat.



Čekání na zprávu, když se počítač vypíná

12.2. Nastavení internetového připojení

Jestliže jste v DHCP síti a máte Ethernetovou síťovou kartu, internetové připojení by již mělo být detekované a nastavené. Pro ruční nastavení následujte tyto kroky.

1. Otevřete nabídku LinuxDefenderu (kliknutím pravým tlačítkem myši) a vyberte **Terminal** k otevření terminálu.
2. Napište **netcardconfig** v otevřeném terminálu ke spuštění síťového konfiguračního nástroje.
3. Jestli vaše síť používá DHCP, vyberte **yes** (jestli si nejste jistí, zeptejte se vašeho síťového administrátora). Jinak viz níže.
4. Síťové připojení by mělo být nyní automaticky nastaveno. Můžete si prohlédnout vaši IP a nastavení síťové karty pomocí příkazu **ifconfig**.
5. Jestliže máte pevnou IP (nepoužíváte DHCP), vyberte **No** u DHCP otázky.
6. Následujte instrukce na vaší obrazovce. Jestli si nejste jisti co psát, kontaktujte vašeho systémového správce nebo správce sítě.

Jestliže je všechno v pořádku, můžete otestovat vaše internetové připojení "pingnutím" `bitdefender.com`.

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

Jestli používáte vytáčené připojení, vyberte **pppconfig** z Administrátorské nabídky LinuxDefenderu. Poté následujte instrukce na obrazovce k nastavení PPP internetového připojení.

12.3. Aktualizace

BitDefender pro LinuxDefender používá systémový ramdisk pro soubory, které lze aktualizovat. Tímto způsobem můžete aktualizovat všechny virové podpisy, testovací rozhraní nebo Antispam databáze, dokonce i když spouštíte systém z nezapisovatelného média jako např. LinuxDefender CD.

Ujistěte se, že máte funkční internetové připojení. Nejprve otevřete BitDefender Vzdálenou Správu a vybrate **Live! Update** z levé nabídky. Stiskněte **Update Now** ke kontrole dostupných aktualizací.

Jako alternativu můžete zadat následující příkaz do konzole.

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

Všechny aktualizační procesy jsou standartně zapisovány do BitDefender logu. Můžete si ho prohlédnout tímto příkazem.

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

Jestli pro odchozí spojení používáte proxy server, **nakonfigurujte** ho v nabídce **Live! Update**.

12.4. Hledání virů

12.4.1. Jak mohu zpřístupnit má Windows data?

Podpora pro zápis NTFS

Podpora pro zápis NTFS je k dispozici použitím metody Captive NTFS write project. Potřebujete dva soubory řadičů z vaší Windows instalace: `ntoskrnl.exe` and `ntfs.sys`. Momentálně jsou podporovány pouze řadiče Windows XP. Všimněte si, že je můžete použít i k zpřístupnění oddílů Windows 2000/NT/2003.

Instalace NTFS řadičů

Pro zpřístupnění vašich NTFS Windows oddílů a aby na ně mohly být zapisována data, musíte nejprve nainstalovat NTFS řadiče. Jestli ve vašem Windows nepoužíváte NTFS formát, ale FAT, a nebo potřebujete přístup pouze pro čtení vašich dat, můžete přímo namountovat disky a zpřístupnit Windows disky stejně jako jakýkoliv Linux disk.

Pro přidání podpory pro NTFS oddíly musíte nejprve nainstalovat NTFS řadiče z vašich pevných disků, ze vzdálených míst, USB disků nebo z Aktualizace Windows. Je doporučeno použít řadiče ze známého bezpečného umístění, protože lokální řadiče Windows mohou být nakaženy viry nebo poškozené.

Klikněte na ikonu **Install NTFS Write Drivers** pro zápis na vaší ploše ke spuštění **BitDefender Captive NTFS Installer**. Vyberte první možnost, chcete-li instalovat řadiče z místního pevného disku.

Jestliže jsou řadiče umístěny dafaultně, použijte **Quick search** pro jejich nalezení.

Můžete specifikovat umístění vašich řadičů nebo je můžete stáhnout z Windows aktualizace SP1.

Řadiče nejsou instalovány na pevný disk, ale jsou pouze dočasně používány LinuxDefenderem pro zpřístupnění Windows NTFS oddílů. Poté, co program nainstaluje NTFS řadiče, můžete kliknout na NTFS oddíly na vaší ploše a brouzdat jejich obsahem. Jako dobrého správce souborů používejte Midnight Commander z nabídky LinuxDefenderu (nebo napište **mc** do terminálu).

12.4.2. Jak spustím antivirový test?

Brouzdejte vašimi složkami, klikněte pravým tlačítkem myši na soubor nebo adresář a vyberte **Send to**. Pak vyberte **BitDefender Scanner**.

Nebo můžete jako root napsat z terminálu následující příkaz. **BitDefender Antivirus Scanner** začne testovat vybraný soubor nebo adresář.

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

Pak klikněte na **Start Scan**.

Jestli chcete nastavit Antivirus, zvolte **Configure Antivirus** z levého panelu programu.

12.5. Vytvoření okamžitého filtru pošty

Můžete použít LinuxDefender k vytvoření řešení pro kontrolu pošty bez instalace nějakého softwaru nebo modifikování poštovního serveru. Nápad spočívá v umístění systému LinuxDefenderu před váš poštovní server, a tím dovolit BitDefenderu hledat Spam a viry v celém SMTP spojení a předat je potom skutečnému poštovnímu serveru.

12.5.1. Nezbytné předpoklady

Budete pořebovat PC s Pentium 3 kompatibilním procesorem nebo novějším, přinejmenším 256MB RAM a CD/DVD mechaniku, ze které se dá bootovat. LinuxDefender bude muset přijímat SMTP spojení namísto skutečného poštovního serveru. Je zde několik cest jak toho docílit.

1. Změňte IP vašeho skutečného poštovního serveru a přiřaďte staré IP systému LinuxDefenderu
2. Měňte vaše DNS záznamy tak, že MX vstup pro vaše domény směřuje k systému LinuxDefenderu
3. Nastavte vaše emailové klienty, aby používali nový LinuxDefender systém jako SMTP server
4. Změnte nastavení vašeho Firewallu, aby přesměrovávalo všechna SMTP spojení na systém LinuxDefenderu namísto skutečného poštovního serveru

Nápověda LinuxDefenderu nepopisuje ani jednu z výše uvedených skutečností. Pro více informací se podívejte do Linux Networking guides a do dokumentace Netfilter.

12.5.2. Emailový obránce

Nabootujte z vašeho LinuxDefender CD a vyčkejte, než se načte a zprovozní systém X Windows.

Pro nastavení BitDefender SMTP Proxy poklikejte na ikonku **BitDefender Remote Admin** na vaší ploše. Objeví se následující okno. Použijte jako uživatele `bd` s heslem `bd` a přihlašte se do Vzdálené správy BitDefenderu.

Po úspěšném přihlášení budete schopni konfigurovat BitDefender SMTP Proxy.

Vyberte **SMTP Proxy** pro konfiguraci skutečného poštovního serveru, který chcete chránit před Spamy a viry.

Vyberte záložku **Email domains** a zadejte všechny emailové domény, pro které chcete přijímat e-maily.

Stiskněte **Add Email Domain** nebo **Add Bulk Domains** a následujte instrukce na obrazovce k nastavení provozu emailových domén.

Vyberte záložku **Net domains** a zadejte všechny sítě, pro které chcete přenášet emaily.

Stiskněte **Add Net Domain** nebo **Add Bulk Net Domains** a následujte instrukce na obrazovce, abyste nastavili přenos do síťových domén.

Vyberte **Antivirus** z nabídky vlevo, abyste určili, co dělat, když je nalezen virus, a abyste nakonfigurovali další nastavení Antiviru.

Nyní jsou všechna SMTP spojení testovaná a filtrovaná BitDefenderem. Standartně všechny zavirované zprávy jsou vyléčené nebo smazané a všechny objevené BitDefenderem jsou označené v předmětu slovem `[SPAM]`. Emailová hlavička (`X-BitDefender-Spam: Yes/No`) je přidána ke všem emailům, aby usnadnila orientaci uživatelům.

12.6. Provedení síťové bezpečnostní prověrky

Vedle schopností odstraňovat škodlivé programy, obnovovat data a kontrolovat poštu, LinuxDefender přichází s řadou nástrojů, které dovedou provést hloubkovou síťovou bezpečnostní prověrku. Analýzu ohroženého systému je také možné provést pomocí bezpečnostních nástrojů zahrnutých v LinuxDefenderu. Přečtěte si tuto malou nápovědu a naučte se, jak spustit bezpečnostní prověrku vaší sítě.

12.6.1. Kontrola rootkitů

Před tím, než začnete hledat bezpečnostní problémy na síťových počítačích, ujistěte se, že nebyl poškozen LinuxDefender. Můžete provést virový test instalovaných pevných disků, jak je popsáno v kapitole **Hledání virů**, nebo můžete otestovat systémové nástroje Unixu.

Nejprve namountujte všechny vaše pevné disky kliknutím na jejich ikonu na ploše nebo použitím příkazu **mount** v terminálu. Pak poklikejte na ikonu **ChkRootKit**, abyste zkontrolovali obsah CD ,nebo napište příkaz **chkrootkit** do terminálu, použitím parametru `-r NEWROOT` určíte nový / (root) adresář počítače

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

Jestli jsou nalezeny systémové nástroje, chkrootkit vypíše nalezené nástroje **VELKÝM TUČNÝM PÍSMEM**.

12.6.2. Nessus - síťový skener

> Nessus je nejpopulárnější open-source skener zranitelnosti, který využívá přes 75.000 organizací ve světě. Mnoho z těchto organizací významně uspořilo náklady používáním Nessusu při auditu zařízení a aplikací nepostradatelných pro jejich fungování.
>
> *—www.nessus.org*

Nessus může být užívaný pro vzdálené testování vašich síťových počítačů proti různé zranitelnosti. Také doporučuje některá opatření ke snížení bezpečnostních rizik a předejití bezpečnostních incidentů.

Klikněte na ikonu **Nessus Security Scanner** na vaší ploše nebo spusťte **startnessus** z terminálu. Počkejte, než se objeví následující okno. V závislosti na vašem hardwarovém vybavení to může trvat až 10 minut, než se Nessus načte, dohromady existuje něco přes 5000 pluginů obsahujících databáze zranitelnosti systému. Použijte uživatel `knoppix` a heslo `knoppix` pro přihlášení.

Klikněte na políčko **Target selection** a napište IP adresy nebo názvy počítačů, které chcete testovat na zranitelnost systému. Ujistěte se, že jste nastavily všechna nastavení v závislosti na vaší síti nebo nastavení systému, předtím než začnete test abyste ušetřily hromadu síťových prostředků a zdrojů a abyste měli přesnější výsledek testu. Nakonec klikněte na **Start the scan**.

Po skončení testovacího procesu zobrazí Nessus výsledky a doporučení. Můžete uložit zprávu do několika formátů, včetně HTML s koláčovými grafy a tabulkami. Uloženou zprávu můžete zobrazit vaším oblíbeným prohlížečem.

12.7. Kontrola operační paměti RAM

Obvykle, kdy má váš systém neočekávané chování (čas od času zamrzá nebo se sám resetuje), může se jednat o problém s pamětí. Můžete testovat vaše RAM jednotky pomocí programu **memtest**, popsaného níže.

Zapněte váš počítač a nabootujte z LinuxDefender CD. Napište **memtest** do terminálu a stiskněte klávesu Enter.

Program Memtest ihned začne a spustí několik testů kontroly stavu RAM. Můžete nastavit jaké testy se mají spustit a různá další nastavení Memtestu, stisknutím tlačítka `c`.

Kompletní Memtest může zabrat až 8 hodin, v závislosti na vaší systémové RAM kapacitě a rychlosti. Doporučujeme spustit všechny testy Memtestu pro úplnou kontrolu chyb RAM pamětí. Program můžete kdykoliv ukončit stisknutím `ESC`.

Jestliže jste rozhodnuti koupit si nový hardware (kompletní systém nebo pouze součásti) doporučujeme použít LinuxDefender a memtest ke kontrole chyb nebo problémů s kompatibilitou.

Odborná pomoc

13. Podpora

13.1. Odborná pomoc

Jako seriózní firma se SOFTWIN snaží poskytovat svým zákazníkům rychlou a přesnou podporu. Asistenční centrum (které můžete kontaktovat na níže uvedené adrese) je nepřetržitě informováno o nejnovějších hrozbách. Včas tak může reagovat na Vaše dotazy.

BitDefender poskytuje nejpokročilejší produkty za nejlepší ceny a šetří tak čas a peníze svých zákazníků. Myslíme si, že úspěšný obchod závisí na dobré komunikaci a smyslu pro dokonalou podporu zákazníka.

Pište nám kdykoliv o pomoc na e-mail <support@bitdefender.com> Pro rychlou odezvu, prosím uveďte ve vašem e-mailu co nejvíce detailů o BitDefenderu a vašem systému, popište váš problém co možná nejpřesněji.

13.2. On-line nápověda

13.2.1. BitDefender Knowledge Base (BitDefender - databáze poznatků)

BitDefender - databáze poznatků je online úschovna informací o produktech BitDefenderu. Ukládají se zde v snadno přístupných zprávách výsledky z pokračující technické podpory a chyb-opravujících aktivit vývojových týmů BitDefenderu, společně s dalšími hlavními články o virové prevenci, o managementu BitDefenderu a detailních vysvětlení, a mnoho jiných článků.

Databáze BitDefenderu je volně dostupná pro veřejnost. Toto množství informací je ještě další způsob jak poskytnout zákazníkům BitDefenderu technické poznatky a náhled, který potřebují. Všechny právoplatné dotazy nebo nahlášení chyb pocházejících od klientů BitDefender nakonec najdou svou cestu do databáze znalostí BitDefenderu, stejně tak jako zprávy, které opravují chyby nebo informační články doplňující nápovědu daného produktu.

BitDefender databáze znalostí je k dispozici kdykoli na http://kb.bitdefender.com.

13.3. Kontaktní informace

Schopná komunikace je klíčem k úspěšnému obchodu. Za posledních 10 let si SOFTWIN vybudoval skutečnou reputaci a nadmíru splnil všechna očekávání svých klientů a partnerů, tím že se s nimi nepřetržitě snaží vylepšit komunikaci. Prosím neváhejte nás kontaktovat s jakýmikoliv problémy nebo otázkami, které byste měli.

13.3.1. Webové adresy

Prodejní oddělení: <sales@bitdefender.cz>
Technická podpora: <support@bitdefender.com>
Dokumentace: <documentation@bitdefender.com>
Partner Program: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Mediální vztahy: <pr@bitdefender.com>
Pracovní příležitosti: <jobs@bitdefender.com>
Viry: <virus_submission@bitdefender.com>
Spam: <spam_submission@bitdefender.com>
Oznámení zneužívání produktu: <abuse@bitdefender.com>
Tvorba webových stránek: http://www.bitdefender.cz
Tvorba ftp archivů: ftp://ftp.bitdefender.com/pub
Lokální distributoři: http://www.bitdefender.com/partner_list
BitDefender databáze znalostí: http://kb.bitdefender.com

13.3.2. Pobočky

BitDefender je připravený odpovídat na libovolné dotazy týkající se činnosti v komerční nebo veřejné oblasti. Jejich příslušné adresy a kontakty jsou uvedeny níže.

Germany

Softwin GmbH
Centrála pro západní Evropu
Karlsdorferstrasse 56
88069 Tettnang
Germany
Telefon: 07542/94 44 44
Fax: 07542/94 44 99
Email: <info@bitdefender.com>
Obchod: <sales@bitdefender.com>
Web: http://www.bitdefender.com

Technická podpora: <support@bitdefender.com>

Velká Británie a Irsko

One Victoria Square
Birmingham
B1 1BD
Telefon: +34 932189615
Fax: +40 21 2330763
Email: <info@bitdefender.com>
Obchod: <sales@bitdefender.com>
Web: http://www.bitdefender.co.uk
Technická podpora: <support@bitdefender.com>

Španělsko

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Technická podpora: <soporte@bitdefender-es.com>
Obchod: <comercial@bitdefender-es.com>
Telefon: +34 932189615
Fax: +34 932179128
Web: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technická podpora: <support@bitdefender.com>
Zákaznický servis: 954-776-6262
Web: http://www.bitdefender.com

Rumunsko

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bukurešť
Technická podpora: <suport@bitdefender.ro>
Obchod: <sales@bitdefender.ro>
Telefon: +40 21 2330780

Fax: +40 21 2330763
Web: http://www.bitdefender.ro

Významový slovník

ActiveX

Active X je šablona pro psaní programů tak, aby je ostatní programy a operační systém mohly volat. Technologie Active X je používána Microsoft Internet Explorerem pro tvorbu interaktivních webových stránek, které vypadají a chovají se spíše jako počítačové programy, než statické stránky. Pomocí Active X mohou uživatelé klást otázky a odpovídat na ně, používat tlačítka a různými způsoby interaktivně komunikovat s webovými stránkami. Ovladače Active X jsou často psány ve Visual Basicu.

Active X se vyznačuje naprostým nedostatkem bezpečnostních kontrol; experti zabývající se bezpečností před jeho používáním na internetu zrazují.

Adware

Adware je často spojen s hostovanou aplikací, která je poskytována tak dlouho, dokud je akceptován adware. Protože je adware instalován většinou až po odsouhlasení licenčních podmínek, nejedná se o trestný čin.

Přesto např. pop-up okna a reklamy mohou obtěžovat a snižovat funkčnost systému. Také informace shromažďované některými aplikacemi mohou znamenat bezpečností riziko pro uživatele, kteří nejsou plně seznámeni s podmínkami licenční smlouvy.

Archiv

Disk, páska nebo adresář, který obsahuje soubory, které byly zálohovány.

Soubor, který obsahuje jeden nebo více souborů v komprimovaném formátu.

Backdoor (zadní vrátka)

Díra v bezpečnostním systému, kterou designeři úmyslně zanechali. Nemusí se vždy jednat o zlý úmysl; některé operační systémy, např. počítají s privilegovanými účty zamýšlenými pro používání terénními servisními techniky.

Boot sektor

Sektor na začátku každého disku, který rozpozná architekturu disku (velikost sektoru, velikost clusteru atd.) U startovacích disků obsahuje zaváděcí sektor rovněž program, který načítá operační systém.

Boot virus

Virus, který infikuje boot sektor pevného disku nebo diskety. Pokus o spuštění diskety infikované virem zaváděcího sektoru zapříčiní, že se virus v paměti aktivuje. Pokaždé, když zavedete systém z tohoto místa, budete mít aktivní virus v paměti.

Prohlížeč

Zkratka pro webový prohlížeč, aplikaci používanou pro nalezení a zobrazení webových stránek. Dva nejpopulárnější prohlížeče jsou Mozilla Firefox, Opera a Microsoft Internet Explorer. Oba jsou to grafické prohlížeče, což znamená, že umějí zobrazit grafiku i text. Navíc, většina nejmodernějších prohlížečů umí prezentovat multimediální informace, včetně zvuku a videa, ačkoliv pro některé formáty vyžadují plug-iny.

Příkazový řádek

V příkazovém řádku píše uživatel příkazy do řádku přímo na obrazovce.

Cookie

V internetovém světě jsou cookies popisovány jako malé soubory, obsahující informace o individuálních počítačích, které mohou být analyzovány a použity inzerenty pro vysledování Vašich internetových zálib a zájmů. V této oblasti se technologie cookie stále ještě rozvíjí se záměrem cílit reklamu přímo tam, kde jste prozradili, že jsou vaše zájmy. Na druhou stranu zahrnují ve skutečnosti sledování a stopování, kam chodíte a na co klikáte. Je pochopitelné, že to vyvolalo debatu o soukromí a mnoho lidí se cítí uraženo představou, že je na ně nazíráno jako na "SKU číslo" (určitě znáte čárový kód na zadní straně všech balíčků, které jsou skenovány v obchodě na pokladně). Jakkoliv se může zdát tato představa extrémní, v některých případech odpovídá realitě.

Disková mechanika

Disková mechanika je zařízení, které čte data a zapisuje je na disk.

Mechanika hard disku čte a zapisuje na hard disky.

Disketová mechanika slouží pro přístup k disketám.

Diskové mechaniky mohou být buď interní (umístněné uvnitř počítače), nebo externí (umístěné v oddělené krabici, která se připojuje k počítači).

Stahování

Znamená kopírování dat (obyčejně celého souboru) z hlavního zdroje na periférní zařízení. Tento termín je obvykle používán pro popis procesu kopírování souboru z online serveru na vlastní počítač. Stahování může často odkázat na kopírování souboru ze síťového souborového serveru na počítač v síti.

E-mail

Elektronická pošta; služba, která posílá zprávy na počítače prostřednictvím místních nebo globálních sítí.

Události

Akce nebo výskyty odhalené programem. Událostmi mohou být aktivity uživatele, jako např. klikání tlačítkem myši nebo stisk klávesy, nebo systémové události, jako např. vyčerpání paměti.

Chybná detekce

Objeví se, když skener identifikuje soubor jako infikovaný, ačkoliv ve skutečnosti není.

Přípona názvu souboru

Součást názvu souboru, nacházející se za tečkou, která indikuje druh dat uložených v souboru.

Mnohé operační systémy používají přípony názvů souborů, např. Unix, VMS a MS-DOS. Skládají se obvykle z 1-3 písmen (některé staré operační systémy nepodporují více než tři). Jako příklad poslouží “c” jako zdrojový kód C, “ps” jako PostSkript, “txt” pro libovolný text.

Heuristika

Na pravidlech založená metoda identifikace nových virů. Tato metoda skenování je nezávislá na specifických virových signaturách. Výhodou heuristického skenování je, že nedochází k “ohlupování” novou variantou existujících virů. Nicméně, občas se může stát, že ohlásí podezřelý kód u normálních programů – pak hovoříme o "chybné detekci".

IP

Internetový protokol - směr udávající protokol v soupravě TCP/IP protokolů, který je zodpovědný za adresování, směrování a fragmentaci a znovuseskupení IP paketů.

Java applet

Java program, který je vytvořený pro spouštění na webové stránce. Pro použití appletu na webové stránce byste museli specifikovat název appletu a velikost (délku a šířku - v pixelech), kterou applet může použít. Když je webová stránka zpřístupněna, prohlížeč stahuje ze serveru applet a spouští ho na uživatelském zařízení (klient). Applety se v jednotlivých aplikacích liší, a jsou regulovány přísným bezpečnostním protokolem.

Příklad: přestože jsou applety spouštěny u uživatele, nemohou přečíst nebo zapsat data z/na uživatelovo zařízení. Applety jsou dále omezovány, takže mohou číst a psát data pouze na té doméně, z níž jsou poskytovány.

Makro virus

Typ počítačového viru, který je zašifrovaný jako makro (vestavěný) do dokumentu. Mnohé aplikace, jako např. Microsoft Word a Excel podporují silné jazyky makro.

Tyto aplikace Vám umožní vestavět makro do dokumentu a nechat makro spustit pokaždé, když je dokument otevřen.

E-mailový klient

E-mailový klient je aplikace, která Vám umožňuje posílat a dostávat elektronickou poštu.

Paměť

Vnitřní skladové prostory v počítači. Termín paměť označuje datový sklad ve formě čipů, a slovo sklad je používán pro paměť, která existuje na páskách nebo discích. Každý počítač disponuje určitým množstvím fyzické paměti, obvykle označované jako hlavní paměť nebo RAM.

Ne-Heuristika

Tato metoda skenování je založena na specifických virových signaturách. Výhodou ne-heuristického skenování je to, že není “ohlupováno” něčím, co se pouze zdá jako virus a nezpůsobuje tedy falešný poplach.

Zabalené programy

Soubor v komprimovaném formátu. Mnoho operačních systémů a aplikací obsahuje příkazy, které Vám umožní zapakovat soubory tak, aby zabíraly méně paměti. Například předpokládejte, že máte textový soubor obsahující deset mezer za sebou. Normálně by takový soubor vyžadoval deset bajtů paměti.

Program, který pakuje soubory, nahradí mezery speciálním znakem pro sérii mezer a číslem udávajícím počet mezer, které byly nahrazeny. V tomto případě, deset mezer potřebuje pouze dva bajty. Tohle je pouze jedna pakovací technika, ale existuje jich více.

Cesta

Přesné nasměrování k souboru v počítači. Tato nasměrování bývají obvykle popisovány prostředky hierarchického souborového systému s vrchu dolů.

Cesta mezi dvěma body, jako je např. komunikační kanál mezi dvěma počítači.

Phishing

Jedná se o rozesílání podvržených zpráv, které se tváří jako legitimní, a to za tím účelem, aby uživatel poskytl soukromé informace, které budou následně zneužity. E-mail obvykle nasměruje uživatele na webovou stránku, kde má aktualizovat své osobní informace, hesla, číslo kreditní karty, čísla bankovních účtů apod. Webová stránka je však falešná.

Polymorfní virus

Virus, který mění svoji formu podle každého souboru, který infikuje. Jelikož takové viry nemají konzistentní binární vzorec, je těžké je identifikovat.

Port

Rozhraní v počítači, ke kterému můžete připojit zařízení. Osobní počítače mají celou řadu portů. Uvnitř je celá řada portů pro připojení diskových mechanik, displejů a klávesnic. Vně mají osobní počítače porty pro propojení modemů, tiskáren, myši, a ostatních periférních zařízení.

V sítích TCP/IP a UDP je to konečný bod logického propojení. Číslo portu udává, o jaký typ portu jde. Např. port 80 je používán pro provoz HTTP.

Soubor s reportem

Soubor, který obsahuje seznam akcí, které se uskutečnily. BitDefender vytváří soubor s reportem obsahujícím skenovanou cestu, složky, množství skenovaných archivů a souborů a dále počty, kolik infikovaných a podezřelých souborů bylo nalezeno.

Rootkit

Rootkit je soubor softwarových nástrojů, které nabízejí přístup k systému na úrovni administrátora. Rootkity byly poprvé použity v UNIXových operačních systémech a jsou využívány k získání administrátorských práv, dovolujících jim utajit svoji přítomnost i před samotnými systémovými administrátory.

Hlavní úlohou rootkitů je maskovat procesy, soubory, přihlašování a záznamy. Takto mohou také zachytit data z terminálů, síťových připojení nebo periferií, pokud se včlení do příslušného softwaru.

Rootkity nejsou ve skutečnosti nebezpečné. Například, systémy a dokonce některé aplikace skrývají kritické soubory používající rootkity. Nicméně jsou většinou používány ke skrývání zákeřného softwaru nebo maskování přítomnosti vetřelce v systému. V kombinaci se zákeřným softwarem se rootkity stávají velkou hrozbou pro integritu a bezpečnost systému. Mohou monitorovat síťový provoz, vytvořit zadní vrátka do systému, modifikovat soubory a záznamy a předcházet tak jejich detekci.

Skript

Jiný termín pro makro nebo pro dávkový /batch/ soubor; skript je seznam příkazů, které mohou být vykonány bez uživatelovy interakce.

Spam

Jedná se o hromadné rozesílání nevyžádaných e-mailů.

Spyware

Jakýkoli software, který tajně shromažďuje informace o uživateli přes internetové připojení bez jeho vědomí, obvykle pro reklamní účely. Spywarové aplikace jsou většinou skrytou součástí freewarových a sharewarových programů, volně přístupných na internetu; nicméně by u freeware a shareware programů mělo být napsáno, že neobsahují spyware. Pokud je spyware nainstalován, monitoruje uživatelovu aktivitu na internetu a odesílá informace někomu jinému. Spyware také dokáže shromažďovat informace o e-mailových adresách a dokonce i hesla a čísla kreditních karet.

Podobnost spywaru a Trojských koní tkví hlavně ve skutečnosti, že uživatelé instalují jeden produkt za druhým. Nejjednodušším způsobem, jak se stát obětí spyware je stahování a výměna dnes běžně dostupných peer-to-peer souborů.

Nehledě na otázku etiky a porušování soukromí, zabírá spyware také paměť a systémové zdroje počítače, zneužívá připojení k internetu pro odesílání nashromážděných informací a zpomaluje tak chod dalších aplikací. Protože spyware využívá paměť a další systémové zdroje, aplikace běžící na pozadí mohou vést až k nestabilitě a pádu systému.

Položky Po spuštění

Veškeré soubory uložené v této složce se po startu počítače spustí. Například, obrazovka při startu, zvukový soubor, který se přehraje, když je počítač poprvé spuštěn, kalendář s připomínkami, nebo různé programy. Obvykle je v této složce uložen jen odkaz na soubor, nikoliv soubor samotný.

Systémová lišta

Zavedená poprvé ve Windows 95; systémová lišta se nachází v úlohové liště Windows (obvykle dole, v blízkosti hodin) a obsahuje miniaturní ikony pro snadný přístup k systémovým funkcím jako je fax, tiskárna, modem, hlasitost atd. Klikněte dvakrát nebo klikněte pravým tlačítkem myši na ikonu pro zobrazení a přístup k detailům a ovládání.

TCP/IP

Protokol kontroly přenosu/Internetový protokol - sada síťových protokolů široce používaných na internetu, které poskytují komunikaci mezi provázanými sítěmi počítačů s různorodou hardwarovou architekturou a rozličnými operačními systémy. TCP/IP obsahuje standardy pro komunikaci počítačů a konvence o propojování sítí a směrovém přenosu.

Trojský kůň

Destruktivní program, který se maskuje jako neškodná aplikace. Narozdíl od virů, se Trojští koně nereplikují, ale přesto mohou být destruktivní. Jedním z nejzákeřnějších typů Trojského koně je program, který se domáhá vyčištění vašeho počítače od virů, ale namísto toho do počítače viry zavede.

Termín pochází z příběhu Homérovy Illiady, v němž Řekové darují gigantického dřevěného koně svému nepříteli, Trójanům, jako symbol míru. Ale jakmile Trójané dovlekli koně dovnitř městských hradeb, řečtí vojáci vylezli z dutých útrob dřevěného koně a otevřeli městské brány, aby tak umožnili svým krajanům nahrnout se dovnitř a zmocnit se Tróje.

Aktualizace

Nová verze softwarového nebo hardwarového produktu vyvinutá, aby nahradila starší verzi téhož produktu. Při instalaci aktualizací je často kontrolováno, zda je starší verze skutečně nainstalována na vašem počítači, a pokud ne, nemůžete aktualizace instalovat.

BitDefender má svůj vlastní modul pro aktualizaci, který vám umožňuje aktualizace produktu kontrolovat a provádět ručně, nebo automaticky.

Virus

Program, nebo kód, který je načten do Vašeho počítače bez Vašeho vědomí a pracuje proti Vaší vůli. Většina virů se může také replikovat. Všechny počítačové viry jsou dílem člověka. Je relativně jednoduché vyrobit vir, který se kopíruje stále a stále znovu. Dokonce i takový jednoduchý vir je nebezpečný, protože rychle využije veškerou využitelnou paměť a přivede systém ke kolapsu. Mnohem nebezpečnějšími typy viru jsou takové, které jsou schopné se přenášet po sítích a obcházet bezpečnostní systémy.

Definice viru

Binární vzorec viru, používaný antivirovým programem k odhalení a elminaci viru.

Červ

Program, který se šíří po síti svojí reprodukcí sebe samého. Neumí se připojit k jiným programům.