bitdefender 9

Internet Security

Uživatelská příručka

- Antivirus
- Firewall
- Antispam
- Antispyware
- Rodicovský kontrola

BitDefender 9 Internet Security

Uživatelská příručka

SOFTWIN

Vydáno 2006.01.13
Build 9.0.1

Právní oznámení


bitdefender
secure your every bit

Obsah

Licence a záruka

Tato Licenční smlouva je právní smlouvou mezi Vámi a SOFTWINem o použití výše jmenovaného softwarového produktu SOFTWINu, která zahrnuje počítačový software a může zahrnovat související media, tištěné materiály a “on-line” nebo elektronickou dokumentaci ("BitDefender"), přičemž všechny jeho části jsou chráněny americkými a mezinárodními copyrightovými právy a mezinárodní úmluvou o ochraně. Instalací, kopírování nebo jinými použitím BitDefenderu souhlasíte s tím, že jste vázáni s podmínkami této smlouvy. Pokud nesouhlasíte s podmínkami smouvy, neinstalujte ani nepoužívejte BitDefender, můžete jej nicméně vrátit v místě nákupu za plnou náhradu ceny do 30 dnů po zakoupení. Může být požadováno doložení Vašeho nákupu.

BitDefender je chráněn právy copyrightu a mezinárodními úmluvami o copyrightu, stejně jako ostatními zákony a úmluvami na ochranu duševního vlastnictví. BitDefender je licencovaný, nikoliv prodejný.

POSKYTNUTÍ LICENCE. SOFTWIN tímto Vám a pouze Vám poskytuje následující nevýhradní licenci na používání Bitdefenderu:

APLIKACE SOFTWARU. V témže operačním systému na jednom počítačovém terminálu můžete instalovat a používat jednu kopii BitDefenderu nebo jeho předcházející verzi. Primární uživatel počítače, na němž je BitDefender instalován může pořídit jednu dodatečnou (tj. druhou) kopii výlučně pro své použití na přenosném počítači.

POUŽITÍ V RÁMCI SÍTĚ. Kopii BitDefenderu můžete rovněž uložit nebo instalovat na paměťové zařízení, jakým je síťový server, používané pouze k instalaci nebo spouštění Bitdefenderu na Vaše ostatní počítače v rámci interní sítě ; musíte nicméně zakoupit a vyhradit separátní licenci pro každý jednotlivý počítačový terminál na němž je BitDefender instalován nebo spouštěn z paměťového zařízení. Licence na Bitdefender nesmí být sdílena nebo používána souběžně na různých počítačích nebo počítačových terminálech. Pokud požadujete multilicenci pro vícenásobné použití na počítačích nebo počítačových terminálech musíte zakoupit licenční balík.

LICENČNÍ BALÍKY. Pokud jste si zakoupili Licenční balík a získali Licenční smlouvu na multilicenci BitDefenderu, můžete pořídit několik dodatečných kopiií počítačového softwaru BitDefenderu, označovaných jako ”licencované kopie”. Jste rovněž oprávněni pořídit

odpovídající počet druhých kopií pro využití na přenosném počítači, tak jak je uvedeno výše v odstavci “Aplikace softwaru”.

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 SOFTWINu. BitDefender je chráněn autorskými právy 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 copyrightové dokumenty musíte vytvářet a přikládat v původní formě ke všem kopiiím vytvořeným bez ohledu na medium 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 medium, 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 medium proti stvrzence za poškozené medium, nebo refundovat peníze, které jste za BitDefender zaplatili. SOFTWIN nezaručuje nepřetržitost či bezchybnost BitDefenderu, nebo že chyby budou opraveny. SOFTWIN nezaručuje, že BitDefender splní Vaše požadavky. SOFTWIN TÍMTO ODMÍTÁ VEŠKERÉ DALŠÍ ZÁRUKY ZA BITDEFENDER, AŤ JIŽ VÝSLOVNÉ NEBO KONKLUDENTNÍ. TATO ZÁRUKA JE EXLUSIVNÍ A „IN LIEU” PRO VŠECHNY OSTATNÍ ZÁRUKY, AŤ JIŽ VÝSLOVNÉ NEBO KONKLUDENTNÍ, VČETNĚ KONKLUDENTNÍCH ZÁRUK MERKANTABILITY,

ZPŮSOBILOSTI KE ZVLÁŠTNÍMU ÚČELU NEBO NEPORUŠENÍ. 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 žádné situaci 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. 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.

VLÁDOU OMEZENÁ PRÁVA. Použití, duplikace nebo vyzrazení je podle vlády předmětem restrikcí dle odstavce (c)(1)(ii) klauzule o Právu v Technických datech a počítačovém software v DFARS 252.227-7013 nebo pododstavcích (c)(1) a (2) klauzule o Omezení práva u komerčního počítačového software, tam kde je použitelné. Kontakt: SOFTWIN, at Fabrica de Glucoza St., No 5, 72322-Sect.2, Bucharest, Romania, nebo na tel. čísle : 40-21-2330780 či faxu: 40-21-2330763.

OBECNĚ. Tato smlouva se bude řídit rumunskými zákony a mezinárodní regulací a úmluvami o copyrightu. Tato smlouva může být modifikována pouze Licenčním dodatkem, který je součástí této smlouvy nebo písemným dokumentem podepsaným jak vámi, tak SOFTWINem. Tato smlouva byla napsána jen v anglickém jazyce a nemá být přeložena nebo vykládána v jiném jazyce. Ceny, náklady a poplatky za použití BitDefenderu mohou být změněny bez předchozího oznámení Vaší straně. 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 SOFTWINu. Microsoft, Windows, Excel, Word, logoWindows, Windows NT, Windows

2000 jsou registrované obchodní značky Společnosti Microsoft. Všechny ostatní ochranné známky jsou ve vlastnictví příslušných majitelů.

Předmluva

Tato Uživatelská příručka je určena všem uživatelům, kteří zvolili **BitDefender 9 Internet Security** 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 s Windows.

Tato kniha vám podrobně popíše produkt **BitDefender 9 Internet Security**, společnost a tým, jenž program vymyslel, vás provedou instalačním procesem a naučí vás, jak jej správně nakonfigurovat. Najdete zde informace o tom, jak používat **BitDefender 9 Internet Security**, jak ho aktualizovat, vyzkoušet a přizpůsobit svým představám. Naučíte se i, jak dostat to nejlepší z BitDefender.

Přejeme vám příjemnou a užitečnou lekci.

1. Konvence použité v této knize

1.1. Typografické konvence

Několik textových stylů bylo použito v knize pro zlepšení čitelnosti. Jejich aspekt' a význam jsou uvedeny v následující tabulce.

Vzhed	Popis
`příklad syntaxe`	Syntaxe je psán písmem se `stejnou roztečí`.
http://www.bitdefender.com	Webové stránky jsou umístěné na http nebo ftp serverech.
`<support@bitdefender.com>`	E - mailové zprávy jsou vložené v textu pro přehled o kontaktních informacích.

Vzhled	Popis
„Předmluva“ (str. xv)	Toto je odkaz směřující na nějaké místo v dokumentu.
`název souboru`	Soubory a adresáře jsou psány písmem se `stejnou roztečí`.
nastavení	Všechna nastavení jsou zvýrazněna **tučným** písmem.
`ukázka psaní kódu`	Části kódů jsou psány písmem se `stejnou roztečí`.

1.2. Poznámky k textu

Poznámky jsou v textu graficky značené, nabízejí vám dodatečné informace k stávajícímu odstavci.

Poznámka

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

Důležité

Toto vyžaduje vaši pozornost a je určeno k přečtení. 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 měli přečíst a porozumět mu, jelikož popisuje něco velice choulostivého.

2. Uspořádání knihy

Kniha se skládá z pěti částí, obsahuje hlavní témata: Instalace, Popis a vlastnosti, Nastavení, Použití a Nápovědu. Navíc obsahuje významový slovník a dodatky, které pomáhají objasnit různé aspekty BitDefenderu, jež by mohly způsobovat technické problémy.

Instalace. Instrukce vás krok za krokem provedou instalací BitDefenderu na počítači. Je zde komplexní průvodce instalací **BitDefender 9 Internet Security**. Počínaje nezbytnými předpoklady pro úspěšnou instalaci jste stále vedeni v průběhu celého instalačního procesu. V případě, že byste potřebovali odinstalovat BitDefender, je na konci uveden proces odinstalovaní.

Popis a vlastnosti. Krátké představení BitDefenderu. V této části je popsáno, co je BitDefender, SOFTWIN a oddělení pro ochranu dat. Je vám prezentován **BitDefender 9 Internet Security**, jeho rysy a moduly.

Řídící konzole. Popis základní administrativy a údržby BitDefenderu. V kapitolách jsou podrobně popsána všechna nastavení **BitDefender 9 Internet Security, dále je zde vysvětleno**, jak zaregistrovat produkt, jak otestovat váš počítač, jak nakonfigurovat antispam, jak nastavit FIrewall a jak vykonávat aktualizace.

Doporučený postup. Následujte kroky popsané v této sekci, abyste zamezili případnému ohrožení vašeho počítače virya spamy.

Odborná pomoc. Místo, kam byste se měli podívat, pokud nefunguje vše podle předpokladů. Je zde také sekce nejčastěji kladených otázek

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, ale může se stát, že narazíte na nějaký problém (či že jsme se dopustili chyby). Prosíme, napište nám o všech vadách, které naleznete v této knize, nebo jak byste ji zlepšily, abyste nám pomohli pro vás vytvořit co možná nejlepší dokumentaci.

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

Instalace produktu

Kapitola 1. Instalace BitDefender 9 Internet Security

Sekce **Instalace BitDefender 9 Internet Security** této uživatelské příručky obsahuje následující témata:

- Systémové požadavky
- Instalační kroky
- Aktualizace
- Odstranění, oprava nebo modifikace charakteristik BitDefenderu

1.1. Systémové požadavky

Pro zajištění správného fungování produktu před instalací ověřte, že jsou splněny následující požadavky systému:

- **Minimální processor** - Pentium MMX 200 MHz
- **Minimální místo na hard disku** - 40MB
- **Minimální paměť RAM** - 64MB (doporučeno 128MB)
- **Operační system** - Windows 2000/XP; Internet Explorer 5.5 (+)

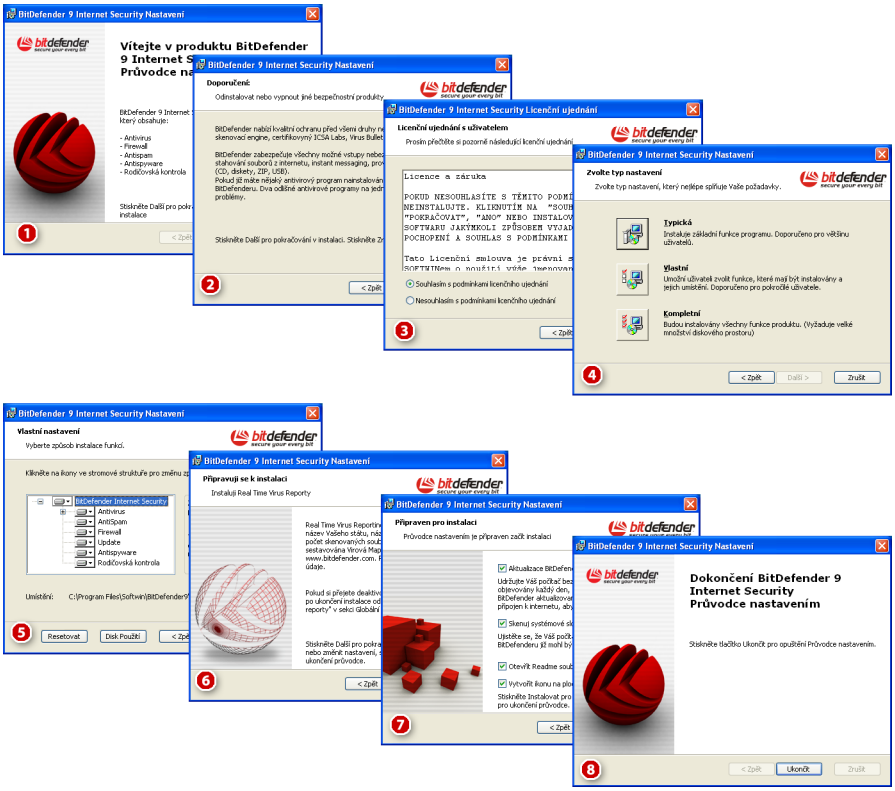
Varování

BitDefender 9 Internet Security nemůže být instalován na Windows NT 4.0 Server, Windows 2000 Server nebo Windows 2003 server. Pro tyto platformy doporučujeme korporátní produkty pro fileservery, gatewaye a poštovní servery.

1.2. Instalační kroky

Lokalizujte instalační soubor a klikněte na něj dvakrát myší. Tím bude spuštěn instalační průvodce, který vás bude provázet instalačním procesem:

Instalační kroky:



Obrázek 1.1. Instalační kroky

1. Klikněte **Další** pro pokračování nebo klikněte **Zrušit** pokud chcete ukončit instalaci.
2. Klikněte **Další** pro pokračování nebo klikněte **Zpět** pro návrat do prvního kroku.
3. Přečtěte si Licenční ujednání, vyberte **Souhlasím s podmínkami Licenčního ujednání** a klikněte **Další**. Pokud nesouhlasíte s těmito podmínkami klikněte na **Zrušit**. Instalační process bude opuštěn a ukončíte instalaci.
4. Můžete si zvolit jednu z verzí instalace: typickou, zákaznickou, 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** - zajistí plnou instalaci produktu. Všechny moduly BitDefenderu budou nainstalovány.

  Pokud si zvolíte instalaci **Typická** nebo **Kompletní**, krok 5 přeskočte.

5. Pokud jste si vybrali **Vlastní**, objeví se nové okno obsahující všechny komponenty BitDefenderu a můžete si 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 hard disku). Kliknete-li na ikonu, zobrazí se okno, kde můžete zvolit, zda chcete vybraný modul nainstalovat neb one.

   Můžete si zvolit složku, do níž chcete produkt instalovat. Výchozí složka je: `C:\Program Files\Softwin\BitDefender 9`.

   Pro jinou složku klikněte **Procházet** a v okně, které se otevře, vyberte složku, do níž má být BitDefender nainstalován. Klikněte **Další**.

6. Klikněte **Další**.

7. Defaultně jsou nastaveny tyto volby:

   - **Aktualizace BitDefenderu** - po ukončení instalace proběhne aktualizace BitDefenderu. Váš system musí být připojen k internetu.
   - **Skenuj sistémové složky Windows** - na konci instalace se spustí skenování virů v celém počítači.
   - **Otevřít soubor readme** - na konci instalace se otevře soubor readme.
   - **Vytvořít ikonu na plochu** - pro umístění zástupce BitDefenderu na plochu na konci instalace.

   Pro započetí instalace klikněte **Instalovat**.

8. Klikněte **Ukončit** pro dokončení instalace produktu. Pokud jste si zvolili výchozí nastavení instalační cesty, bude v `Softwin` vytvořena nová složka pojmenovaná `Program Files`, která obsahuje podsložku `BitDefender 9`.

Poznámka

Možná budete požádáni, abyste restartovali systém, tak aby mohl být dokončen instalační process.

1.3. Aktualizace

Aktualizační procedura může být provedena jedním z následujících způsobů:

- Instalace bez odstranění předchozí verze - pouze pro verze v8 a v9

  Spusťte soubor setup a následujte Průvodce popsaného v části „*Instalační kroky*“ (str. 3).

Důležité

Během instalačního procesu se objeví chybové hlášení způsobené `službou Filespy`. Klikněte na **OK** pro pokračování instalace.

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

  Nejprve musíte odstranit vaši předchozí verzi, restartovat počítač a nainstalovat novou, jak je popsáno v sekci „*Instalační kroky*“ (str. 3).

Důležité

Jestliže aktualizujete z v8 na v9, doporučujeme Vám uložit si nastavení BitDefenderu , Seznam přátel a Seznam Spammerů. Po skončení aktualizačního procesu je můžete opět nahrát.

1.4. Odstranění, oprava nebo modifikace charakteristik BitDefenderu

Chcete-li modifikovat, opravit, nebo odstranit **BitDefender 9 Internet Security**, postupujte touto cestou ze Start menu ve Windows: **Start** -> **Programs** -> **BitDefender 9** -> **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;
- **Opravit** - znovu nainstalovat veškeré programové komponenty, které byly instalovány v předchozí instalaci;

Důležité

Před opravami produktu doporučujeme, abyste si uložili: Seznam přátel a Seznam spamerů. Můžete si uložit Nastavení BitDefenderu a Bayesianské database. Po dokončení procesu oprav si je můžete znovu načíst.

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

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

Kapitola 2. Přehled

BitDefender nabízí bezpečnostní řešení požadavků na ochranu v dnešním počítačovém prostředí a dodává toto efektivní řízení hrozeb 41 milionům domácnostem a firemním uživatelům ve více než 100 zemích.

BitDefender je navržený k tomu, aby poskytl plnou ochranu pro podnikové sítě a systémy. Vedle antivirové ochrany zahrnuje antispam, firewall a řešení bezpečnostní správy. BitDefender se také specializuje na poskytování pomoci s navrhováním a realizací zabezpečovacích systémů pro podnikové sítě.

BitDefender Professional byl třetí produkt svého druhu na světě, který získal certifikaci ICSA pro Windows XP a jako první získal ocenění za inovaci od Evropských komisí a akademií. BitDefender Antivirusantivirus je oceněný všemi významnějšími recenzenty na antivirovém poli - ICSA Labs, CheckMark, CheckVir, TÜV a Virus Bulletin.

BitDefender má sídlo v Bukurešti, Rumunsku a má kanceláře v Tettnangu, Německu, Barceloně, Španělsku a Floridě, US. Webové stránky: http://www.bitdefender.com

2.1. 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 reprezentuje nejlepší evropské inovace v oblasti informační technologie.

Komplexní. Pokryje každý jednotlivý bod vaší sítě, poskytuje kompletní ochranu. Bezpečnostní řešení BitDefender pro podnikatelské prostředí uspokojí ochranné požadavky z dnešního obchodního prostředí. Umožňuje zvládat všechny komplexní hrozby, jež mohou ohrozit síť, od malých lokálních oblastí až po velké multiservery, multi-platform 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:

- Útoku Wormů (Červů)
- Ztráta spojení díky infikovaným e-mailům
- E - mailové selhání
- Čištění a obnova systému
- Ztráta produktivity koncových uživatelů, protože systémy nejsou dosažitelné
- Hackerství a neoprávněný přístup, který může způsobit velké škody

Některé současně vývojové trendy a výhody mohou být splněny použitím BitDefender bezpečnostní soupravy:

- Zvětšit síťovou dostupnost zastavením šíření záludných kódových útoků (např. Nimda, trojští koně, DDoS).
- Chránit vzdálené uživatele od útoků.
- Efektivním snížením nákladů na administrativu a prostor s BitDefender Enterprise hospodářskou správou.
- Zastavením šíření škodlivých programů přes e-mail používáním BitDefender e-mailové ochrany v síťových serverech.

2.2. Data Security Division (Oddělení pro ochranu dat)

Od počátku oddělení pro ochranu dat společnosti SOFTWIN přiblížilo zabezpečení dat určitým způsobem, s první inteligentní aktualizací nevyžadující žádný uživatelský zásah,

s první vzdálenou antivirovou správou pomocí WAP technologie nebo prvním v antiviru integrovaným firewallem poskytujícím úplnou odpověď komplexní bezpečnostní hrozby.

BitDefender je schopen poskytnout plnou ochranu dat na všech kritických úrovních v dnešním obchodním prostředí. Oddělení pro ochranu dat se zaměřuje na zabezpečení ochrany systémů proti počítačovým virům, provádí antivirový výzkum, vyvíjí nové technologie pro monitorování všech možných cest, jak nakazit systém, a v neposlední řadě poskytuje vzdělávání IT&C veřejnosti o nebezpečí výpočetních virů.

Bezpečnostní řešení BitDefenderu uspokojuje ochranné požadavky dnešního obchodního prostředí, umožňuje zvládat všechny hrozby, které ohrožují síť - od malé lokální sítě po velké multiservery, multi-platform WANy.

2.3. SOFTWIN

V Bukurešti založený SOFTWIN je vůdčí dodavatel komplexních softwarových řešení a služeb v Rumunsku.

SOFTWIN se zaměřuje na poskytování softwarových řešení a služeb, jež umožňují rychle rostoucím společnostem vyřešit obchodní výzvy a získat nové obchodní příležitosti.

SOFTWIN umožňuje společnostem soustředit se na jejich hlavní obchod a expandovat k novým trhům.

SOFTWIN zaměstnává přes 500 vysoce kvalifikovaných profesionálů zkušených v rozvíjení řešení a služeb.

Od jeho založení v roce 1990 vzrost průměrný roční příjem SOFTWINu o +30%.

SOFTWIN má 4 oddělení, která také určují hlavní obchodní směry společnosti:

- CRM
- Business Information Solutions
- eContent Solutions
- Data Security Solutions

SOFTWIN poskytuje služby a řešení zákazníkům na celém světě. Přes 90% obratu společnosti je získáno z vývozu do USA a Evropské unie.

Používáním nejnovější technologie SOFTWIN úspěšně vyvinul přes 500 softwarových vývojových projektů, přes 3,500 strukturovaných projektů pro mezinárodní partnery zabezpečujících data více než 43 milionům uživatelů v 80 zemích světa a více než 1,500,000 klientských hovorů ročně vyřízených službou CRM.

Kapitola 3. BitDefender 9 Internet Security

BitDefender 9 Internet Security pokrývá všechny bezpečnostní požadavky rodiny, která využívá připojení k internetu. Poskytuje základní ochranu proti virům, spyware, spamu, podvrženým e-mailům a nevhodnému obsahu webu.

3.1. Antivirus

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

Heuristika ve Virtualním prostředí. Heuristika ve virtualním prostředí (HiVE) provádí emulaci virtuálního počítače 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.

Trvalá antivirová 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.

Ochrana Peer-2-Peer aplikací. Skenuje viry, které se rozšířily prostřednictvím zasílání zpráv a softwarovými aplikacemi se sdílenými soubory.

Plná ochrana e-mailů. Aplikace funguje na POP3 úrovni protokolu, blokuje veškeré infikované e-mailové zprávy, bez ohledu na používaného e-mailového klienta (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat,atd.) bez další dodatečné konfigurace.

3.2. Firewall

Modul Firewall kontroluje dobu přístupu aplikací a uživatelů k Internetu. V “tajném módu” bude počítač skrytý před útoky hackerů a před nebezpečnými kódy.

Kontrola internetového provozu. Lze přímo definovat, která příchozí a odchozí připojení povolit a která zakázat, dale umožňuje definovat specifická pravidla pro protokoly, porty aplikace a nebo vzdálené adresy.

Kontrola připojení. BitDefender umožňuje sledovat v reálném čase, které programy se připojily k síti. Jedním kliknutím myši lze nastavit, které programy se mohou připojovat a které ne.

Tajný mód (stealth mode). Hackeři nebo nebezpečné programy ani nemusí zjistit, že Váš počítač vůbec existuje. Pokud bude Tajný mód zapnut, počítač nebude reagovat na žádné pokusy zvenčí, které mají zjistit otevřené porty apod.

3.3. Antispam

Jednoduše utvořený modul BitDefender Antispam řeší spamy, takže se tímto problémem nemusíte zabývat.

Anti-Phishing. Udržte si odstup od záludných e - mailových zpráv pokoušících se z vás vylákat informace o vašem bankovním účtu pomocí nového BitDefender phishing detektoru.

Samoučící se filtr. Pokročilý, samoučící se Bayesiánský filtr Vám jedním kliknutím umožní třídit zprávy na “Spamy” nebo “Nespamy”. Po několika málo iteracích se toto filtr naučí sám a časem tuto problematiku převezme zcela na sebe. Každé označkování které provedete, zvýší přesnost filtru. Jak citlivý filtr nastavíte, záleží jen na Vás.

Heuristický, URL, White List/Black List,Charset a Image fitry. Čtyři typy filtrů dále zajišťují vaši kontrolu nad e-maily. Heuristický filtr kontroluje poštu a hledá charakteristické rysy spamu. White list/Black list filtr odmítne poštu ze známých spam adres a nechá projít poštu od vašich přátel, URL filtr blokuje poštu obsahující podezřelé odkazy, zatímco charset filtr blokuje poštu obsahující "podivné" znaky. Image filtr rozhoduje, zda obrázky obsažené v e-mailech patří ke spamu.

Bez potíží. Budete informováni pouze o příchodu legitimních zpráv. Spam bude nerušeně ukládán do složky Spam, kde jej můžete prozkoumat či vyhodit.

Kompatibilita a integrace do Outlooku(tm). BitDefender antispam je kompatibilní se všemi e-mailovými klienty. BitDefender antispam lišta s nástroji v Microsoft Outlooku a Outlook Express umožňuje uživatelům filtrovat poštu a kontakty bez ukončení Outlooku.

3.4. Antispyware

Monitoruje a předchází potenciálním hrozbám spyware dříve, než mohou počítač napadnout. Díky komplexní databázi spywarových signatur zůstane Váš počítač vždy bezpečný.

Antispywarová ochrana v reálném čase. BitDefender monitoruje desítky potenciálních míst, kudy může spyware do počítače proniknout. Známý spyware je blokován v reálném čase.

Spyware skenování a odstranění. BitDefender skenuje celý system nebo jeho část a zjišťuje přítomnost spyware. Využívá komplexní databázi spywarových signature, která je průběžně aktualizována.

Kontrola aktivního obsahu. Proaktivně blokuje veškeré potenciálně nepřátelské aplikace , jako jsou Java Applets nebo kódy typu Java Scripts.

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

Kontrola cookie. Antispyware filtruje příchozí a odchozí soubory typu cookie a při surfování po internetu udržuje Vaši identitu a preference v utajení.

3.5. Rodičovská kontrola

Parental control modul neboli modul "rodičovské kontroly" umí blokovat přístup na webové stránky, které považujete za nevhodné, blokuje přístup k internetu v určitou denní dobu (např. v době vyučování), případně blokuje aplikace jako jsou hry, chat, programy sdílející soubory apod.

Kontrola webu. URL filtr umožňuje blokovat přístup na webové stránky s určitým obsahem. Seznam blokovaných webů a jejich částí je poskytována BitDefenderem a aktualizována v rámci pravidlených updatů. Je možné nastavit blokování take těch webů, které obsahují odkazy na zakázané stránky.

Časové omezení. Použitím Časového omezení je možné povolit nebo blokovat přístup k webu uživatelům nebo apllikacím v určité době.

Kontrola aplikací. Je možné blokovat spuštění libovolných aplikací. Touto cestnou jsou blokovány hry, messaging software a podobné aplikace. Aplikace zde definované, jsou chráněné proti změnám a nemohou být kopírovány ani přesunuty.

3.6. Další vlastnosti

Časté aktualizace. Vaše kopie BitDefenderu se aktualizuje 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. Majitelé BitDefender licence mohou zdarma čerpat výhod aktualizací virových definic a aktualizací produktu.

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

Záchranný disk. **BitDefender 9 Internet Security** je dodáván na bootovacím CD (založeným na LinuxDefenderu), které může být použito k opravě sytému bez jeho nastartování.

Kapitola 4. Moduly BitDefenderu

BitDefender 9 Internet Security obsahuje moduly: **Hlavní**, **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Rodičovský zámek** a **Aktualizace**.

4.1. Hlavní modul

BitDefender je plně konfigurovaný pro maximální bezpečnost.

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

4.2. Modul Antivirus

BitDefender Vás chrání před viry, které vstupují do Vašeho systému, tím že skenuje Vaše soubory, e-maily, stahovatelné soubory a ostatní obsah při vstupu do Vašeho systému. V modulu Antivirus mátte přístup ke všem nastavením a vlastnostem.

Protivirová ochrana se člení na dvě kategorie:

- Skenování při vstupu - zabraňuje novým virům vstoupit do vašeho systému. Rovněž se jí říká protivirový štít – soubory jsou skenovány, když do nich uživatel vstupuje. BitDefender například bude skenovat dokument vytvořený ve Wordu až když jej otevřete, a e-mailovou zprávu, až když ji dostanete. BitDefender skenuje “když je použijete” – tedy při vstupu do nich.
- Skenování na požádání - odhaluje viry již ve vašem systému usídlené. Je to klasické protivirové skenování – skenování iniciované uživatelem – vyberete disk, složku nebo soubor, který má BitDefender skenovat – tedy BitDefender skenuje na požádání.

4.3. Modul Firewall

Firewall chrání váš počítač před nepovolenými příchozími i odchozími pokusy o spojení. Má stejnou funkci jako stráž u brány - bude stále dohlížet na vaše internetové spojení a sledovat, komu povolí přístup k Internetu a koho zablokuje.

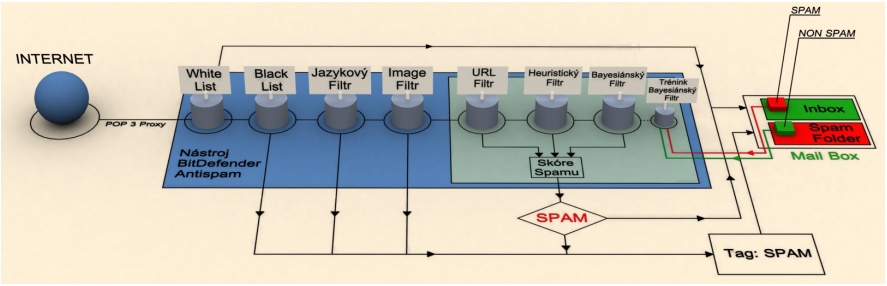
Firewall je základní, jestliže máte široké pásmo nebo DSL spojení.

4.4. Modul Antispam

Spam se stává stále závažnějším problémem pro jednotlivce i pro firmy. Není příjemný, nechcete, aby se dostal do rukou dětem, rozčiluje Vás (kvůli ztrátě času, nebo proto, že Vám chodí porno stránky do služebního e-mailu) a neumíte zabránit lidem aby ho posílali. To nejlepší, co se dá udělat je zřejmě zastavit jeho příjem. Bohužel, Spamy přicházejí v celé řadě forem a formátů a ve velkém množství.

4.4.1. Schéma

Níže uvedené schéma zobrazuje, jak BitDefender pracuje.



Obrázek 4.1. Antispam Filtry

Antispamové filtry z uvedeného schematu (White list, Black list, Jazykový (znaková sada) filtr, Image filtr, URL filtr, Heuristický filtr a Bayesiánský filtr) využívá modul Antispam v konjunkci, tak aby mohl určit, zda má daný e-mail dorazit do Vaší **schránky došlé pošty**, či nikoliv.

Každý e-mail, který přichází z internetu prochází nejprve filtry White list/Black list. Je-li adresa odesilatele nalezena na White listu je e-mail přímo přesunut do Vaší **schránky došlé pošty**.

V opačném případě daný e-mail převezme filtr Black list a provede porovnání adresy odesilatele s adresami na svém seznamu. Pokud je nalezena shoda, bude e-mail označen jako SPAM a přesunut do složky **Spam** (umístěné v Microsoft Outlook).

Další filtr, Jazykový (znaková sada) filtr zkontroluje, zda e-mail je napsán v cyrilici nebo asijském písmu. Pokud ano, je tento e-mail označen jako SPAM a přesunut do složky **Spam**.

Pokud ne, je vpuštěn do Image filtr. **Image filtr** detekuje všechny e-mailové zprávy obsahující přiložené obrázky s nevyžádaným obsahem.

URL filtr pátrá po odkazech a nalezené odkazy srovnává s odkazy v databázi BitDefenderu. V případě shody přidá do e-mailu skóre Spamu.

Dále e-mail převezme Heuristický filtr a provede sérii testů na všech komponentách zprávy, prohledá slova, fráze, odkazy a ostatní charakteristiky Spamu. Výsledkem je, že do e-mailu rovněž přidá skóre Spamu.

Poznámka

Pokud je e-mail v předmětu označen jako SEXUÁLNĚ EXPLICITNÍ, bude jej BitDefender považovat za SPAM.

Bayesiánský filtr provede další analýzu zprávy na základě statistických propočtů udávajících míru výskytu specifických slov u zpráv klasifikovaných jako Spam v porovnání se zprávami prohlášenými (Vámi, nebo Heuristickým filtrem) za Ne-Spam. Do e-mailu pak přidá skóre Spamu.

Pokud celkové skóre (URL skóre + heuristické skóre + bayesiánské skóre) u zprávy převýší povolené skóre Spamu pro zprávu (nastavené uživatelem v sekci Antispam jako hladina tolerance), je zpráva považována za SPAM.

Důležité

Používáte-li jiného e-mailového klienta než Microsoft Outlook nebo Microsoft Outlook Express, měli byste vytvořit pravidlo pro přesun e-mailových zpráv označených BitDefenderem jako Spam do uživatelovy "custom" karanténní složky. BitDefender připojí prefix [SPAM] do předmětu zprávy považované za Spam.

4.4.2. Antispam filtry

Nástroj BitDefender Antispam obsahuje 7 různých filtrů, které zabezpečují, aby ve Vaší schránce Došlé pošty nebyl žádný spam: White list, Black list, Jazykový (znaková sada) filtr, Image filtr, URL filtr, Heuristický filtr a Bayesiánský filtr.

Poznámka

V modulu **Antispam**, v sekci Nastavení můžete každý z těchto filtrů aktivovat/deaktivovat.

White list / Black list

Mnozí lidé komunikují pravidelně se skupinou lidí nebo dokonce dostávají zprávy ze společností či organizací se stejnou doménou. Používáním **seznamu přátel nebo seznamu spamerů** můžete snadno rozlišit, od kterých lidí si přejete dostávat e-maily (přátelé) bez ohledu na obsah zprávy, a od kterých nechcete dostávat vůbec nic (spameři).

Poznámka

Seznamy **White list / Black list** jsou známé rovněž jako **Seznam přátel / Seznam spamerů**.

Seznam přátel / Seznam spamerů můžete spravovat v řídící konzoli nebo v liště nástrojů Antispam.

Poznámka

Doporučujeme, abyste přidali jména a e-mailové adresy Vašich přátel do **seznamu přátel**. BitDefender neblokuje zprávy od osob na seznamu; přidání přátel do seznamu napomůže tomu, aby legitimní zprávy mohly bez problémů přicházet.

Jazykový (znaková sada) filtr

Většina spamových zpráv je napsána v cyrilice nebo asijském znakovém písmu. Proveďte konfiguraci tohoto filtru, pokud si přejete, aby všechny e-maily napsané výše zmíněnými písmy byly odmítnuty.

Image filtr

Dnes se do elektronické pošty dostává stále více zpráv, které obsahují přiložené obrázky s nevyžádaným obsahem. S jejich detekcí může mít heuristický filtr potíže. Proto BitDefender představuje **Image filtr**, který porovnává příchozí obrázek s vlastní databází obrázků. V případě shody je pak takový e-mail označen jako spam.

URL filtr

Většina spamových zpráv obsahuje odkazy na různá weby (obvykle reklama či nabídka nákupu zboží). BitDefender má databázi odkazů na tento druh stránek.

Každý URL odkaz v e-mailové zprávě bude revidován s databází URL. Bude-li nalezena shoda, spamové skóre této zprávy bude zvýšeno o +45.

Heuristický filtr

Heuristický filtr provádí sadu testů ve všech komponentách zprávy (t.j. nejen v záhlaví, ale rovněž v těle zprávy a to jak v HTML tak textovém formátu), prohledává slova, fráze, odkazy či ostatní charakteristiky spamu.

Odhaluje rovněž e-mailové zprávy v předmětu uvedeno SEXUÁLNĚ EXPLICITNÍ. Tyto zprávy jsou považovány za SPAM.

Poznámka

Počínaje 19. květnem 2004 musí veškerý sexuálně orientovaný materiál obsahovat v řádku předmět varování SEXUÁLNĚ EXPLICITNÍ: v opačném případě hrozí pokuta za porušení federálních zákonů.

Bayesiánský filtr

Bayesiánský filtr klasifikuje zprávy na základě statistických propočtů udávajících míru výskytu specifických slov u zpráv klasifikovaných jako Spam v porovnání se zprávami prohlášenými (Vámi, nebo Heuristickým filtrem) za Ne-Spam.

To například znamená, že pokud se určité čtyřhláskové slovo často opakuje ve Spamu dá se s vyšší pravděpodobností předpokládat, že se u další příchozí zprávy, která ho

obsahuje, skutečně jedná o spam. V úvahu jsou brána veškerá relevantní slova ve zprávě. Syntézou statistických informací je vypočítávána celková pravděpodobnost Spamu u dané zprávy.

Tento modul má ještě jednu zajímavou vlastnost: dá se cvičit. Přizpůsobuje se rychle typu zpráv, které určitý uživatel získává a shromažďuje o nich informace. Aby mohl filtr efektivně fungovat, musí být trénován, v tom smyslu, že mu musí být prezentovány ukázky Spamu na straně jedné a legitimních zpráv na straně druhé, tak jako když trénujete psa ve stopování. Občas musí být filtr také korigován – pobídnut k seřízení, pokud dělá špatná rozhodnutí.

Důležité

Bayesiánský modul můžete korigovat použitím tlačítek **To je spam** a **To není spam** v *„Antispam lištu nástrojů“* (str. 105).

Poznámka

Pokaždé, když provedete aktualizaci:

- nové obrazové podpisy budou přidány do **Obrázkového filtru**;
- nové webové stránky budou přidány do **URL filtru**;
- nová pravidla budou přidána do **Heuristického filtru**;

To zvýší efektivitu fungování nástroje Antispam.

Důležité

Pro ochranu proti spammerům BitDefender může provádět autmatické aktualizace. Zachovejte zatrženu volbu **Automatická aktualizace**.

4.5. 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 zablokované ihned. To je velice efektivní při blokování trojských koní a dalších nástrojů instalovaných počítačovými hackery, kteří se pokoušejí proniknout do vašeho soukromí a poslat vaše osobní informace, jako např. čísla kreditních karet z vašeho počítače k hackerovi.

BitDefender může také testovat váš systém nebo jeho část na známé spywarové hrozby. Test používá stále aktualizovanou podpisovou Spyware databázi.

4.6. Modul Rodičovký kontrola

BitDefender modul pro kontrolu obsahu může blokovat přístup k webovým stránkám, které považujete za nevhodné, blokuje přístup k Internetu v určitém časovém rozmezí (jako např, když je čas se učit), blokuje spouštění aplikací jako jsou hry, chat, programy pro sdílení souborů a jiné.

4.7. Modul Aktualizace

Každý den jsou identifikovány nové viry. To je důvod, proč udržovat BitDefender aktualizovaný s novými virovými signaturami. V základním nastavení si BitDefender kontroluje nové aktualizace každé hodin.

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 definic virů**.

- **Aktualizace antispamových nástrojů** - přidání nových pravidel do heuristického a URL filtrů a nové obrazové podpisy budou přidány do Obrázkového filtru. To se projeví ve zvýšení efektivity nástroje Antispam. Tato aktualizace je rovněž známa pod názvem **Aktualizace Antispamu**.

- **Aktualizace antispyware** - 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:

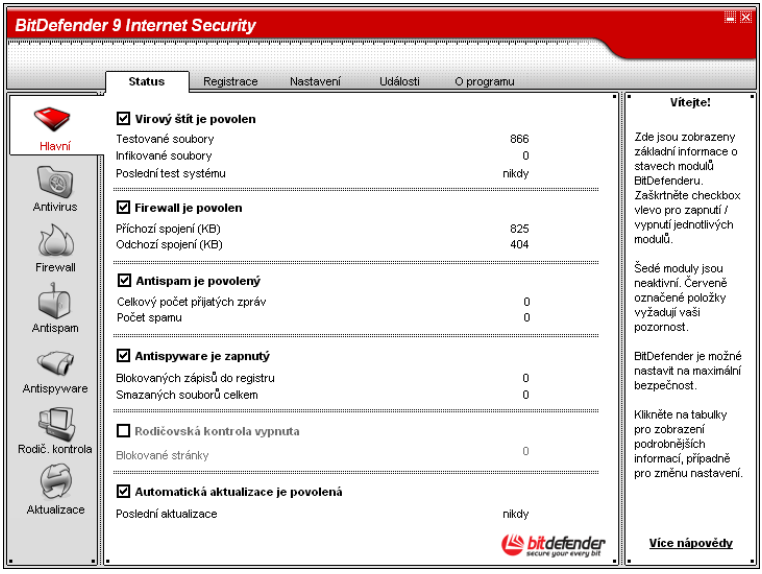
- Automatická aktualizace - antivirus automaticky kontaktuje server BitDefenderu, aby prověřil, zda byla zveřejněna nějaká aktualizace. Pokud ano, dojde k aktualizaci BitDefenderu automaticky. Automatická aktualizace může být provedena kdykoliv kliknutím na **Aktualizovat** nyní v Aktualizačním modulu.
- Ruční aktualizace - ověřující existenci aktualizace na žádost uživatele.

Řídící konzole

Kapitola 5. Přehled

BitDefender 9 Internet Security 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 management konzoli : **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Rodičovký kontrola** a **Aktualizace**.

Pro přístup k management konzoli použijte Start menu Windows a vyhledejte **Start** -> **Programy** -> **BitDefender 9** -> **BitDefender 9 Internet Security** nebo rychleji – stačí poklepat na **ikonu BitDefenderu** na liště.



Obrázek 5.1. Řídící konzole

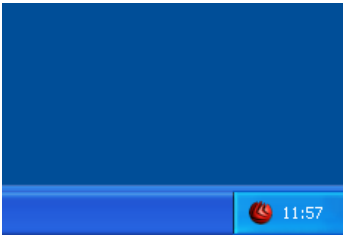
Na levé straně řídícího panelu vidíte nabídku modulů:

- 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**.
- Firewall - v této sekci můžete nastavovat modul **Firewall**.
- Antispam - v této sekci můžete nastavovat modul **Antispam**.
- Antispyware - v této sekci můžete nastavovat modul **Antispyware**.
- Rodičovská kontrola - v této sekci můžete nastavovat modul **Rodičovské kontroly**.
- Aktualizace - v této sekci můžete nastavovat modul **Aktualizace**.

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

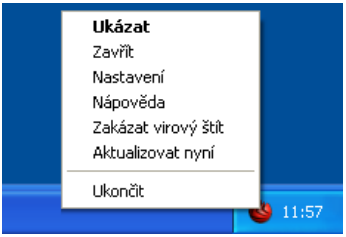
5.1. Systémové liště

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



Pokud dvakrát kliknete na tuto ikonu, otevře se řídící konzole.

Obrázek 5.2. Systémové liště



Stejně tak, pokud kliknete pravým tlačítkem myši na uvedenou ikonu, otevře se pop menu s následujícími možnostmi.

Obrázek 5.3. Kontextové menu

- **Ukázat** - otevřít řídící konzoli.
- **Zavřít** - minimalizuje řídící konzoli do systémové lišty.

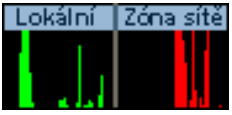
- **Nastavení** - otevře Nastavení management konzole.
- **Nápověda** - otevřít elektronickou dokumentaci.
- **Zakázat virový štít** - zapne/vypne antivirový štít.
- **Aktualizovat nyní** - provede okamžitou aktualizaci.
- **Ukončit** - vypnout aplikaci. Volbou této možnosti zmizí ikona ze systémové lišty a pro přístup do řídící konzole musíte aplikaci spustit znovu ze Startu v menu.

Poznámka

- Pokud vypnete jeden nebo více modulů BitDefenderu, ikona se změní na černou. Tak budete vědět, které moduly jsou vypnuté i bez otevření řídící konzole.
- Ikona bude blikat, pokud je dostupná nova aktualizace.

5.2. Panel aktivity skenování

Panel aktivity skenování je grafická vizualizace skenování Vašeho systému.



Zelené sloupce (**Lokální**) ukazuje počet skenovaných souborů za sekundu na stupnici 0 – 50.

Obrázek 5.4. Panel aktivity skenování

Červené sloupce zobrazené v **Zóna Sítě** ukazuje počet Kb přenesených (odeslaných a přijatých z Internetu) za sekdundu na stupnici 0-100.

Poznámka

Panel aktivity skenování vás informuje o vypnutí virového štítu nebo Firewallu zobrazením červeného kříže v odpovídajícím okně (**Lokální** nebo **Zóna sítě**). Tak stále víte, zda jste chránění i bez otevření řídící konzole.

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

Poznámka

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

Kapitola 6. Hlavní modul

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

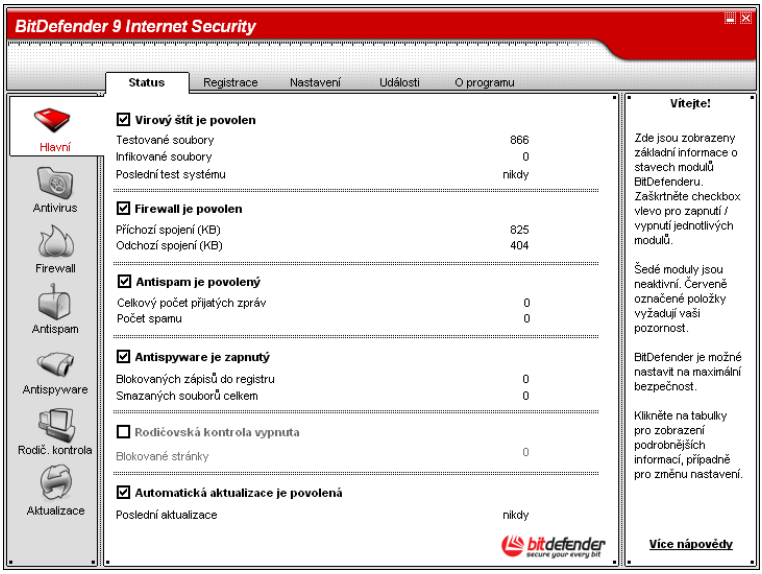
- Všeobecné informace
- Registrace produktu
- Nastavení řídící konzole
- Události
- O BitDefenderu

Poznámka

Podrobnější informace týkající se **Hlavního** modulu najdete v kapitole *„Hlavní modul“* (str. 19).

6.1. Všeobecné informace

Pro přístup do této sekce klikněte na záložku **Status** v **Hlavním** modulu.



Obrázek 6.1. Všeobecné informace

Zde můžete produkt registrovat a nastavit jeho chování.

Zatržením nebo odstraněním zatržítka aktivujete či deaktivujete hlavní parametry BitDefenderu.

Varování

Položky označené červeně vyžadují Vaši okamžitou pozornost.

6.1.1. Virový štít

Poskytuje nepřetržitou ochranu před viry a ostatními hrozbami v reálném čase. Zobrazuje počet skenovaných souborů, infikovaných souborů, skenovaných zpráv, infikovaných zpráv a datum posledního skenování systému.

Poznámka

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

Varování

Rozhodně doporučujeme minimálně jedenkrát týdně provést celkové skenování systému. V modulu **Antivirus** vstupte do sekce Test, zatrhněte **Místní disky** a klikněte **Test**.

6.1.2. Firewall

Firewall chrání před útoky z internetu. Čísla ukazují internetový provoz při jednom připojení.

Poznámka

Pro zajištění trvalé ochrany před itnernetovámi útoky udržujte **Firewall** zapnutý.

6.1.3. Antispam

Spamy představují pro jednotlivce i organizace stále větší problém. Vyskytují se v celé řadě forem a velikostí a vyskytují se hojně. **Antispam** spolupracuje s e-mailovými klienty a můžete jej konfigurovat v řídící konzoli (sekce **Antispam**).

Navíc je začleněný přímo do Microsoft Outlook a Microsoft Outlook Express a umožňuje tak hladkou interakci s Antispamovými filtry prostřednictvím intuitivního a uživatelsky snadného rozhraní.

Poznámka

Abyste zabránili vniknutí Spamu do Vaší schránky došlé pošty, mějte aktivovaný **Antispam filtr**. Sledujte, jak pracuje BitDefender Antispam.

6.1.4. Antispyware

Antispyware monitoruje desítky potenciálních míst, kudy může spyware do počítače proniknout. Čísla ukazují počet skenovanýh objektů při jednom připojení.

Poznámka

Pro zajištění trvalé ochrany před spyware udržujte **Antispyware** zapnutý.

6.1.5. Rodičovský zámek

BitDefender umí blokovat přístup na webové stránky, které považujete za nevhodné, blokuje přístup k internetu v určitou denní dobu (např. v době vyučování), případně blokuje aplikace jako jsou hry, chat, programy sdílející soubory apod.

6.1.6. Automatická aktualizace

Každý den jsou identifikovány nové viry. To je důvod, proč udržovat BitDefender aktualizovaný s novými virovými signaturami. Zobrazuje se datum poslední aktualizace.

Poznámka

Pro ochranu Vašich kritických dat může BitDefender provádět automatické aktualizace. Mějte zapnutou volbu **Automatická aktualizace**.

6.2. Registrace produktu

Pro přístup do této sekce klikněte na záložku **Registrace** v **Hlavním** modulu.

Obrázek 6.2. Registrace produktu

Tato sekce obsahuje informace o stavu Vaší licence na Bitdefender. Dále je uveden datum vypršení a můžete si zde produkt zaregistrovat.

Produkt je dodáván se zkušebním registračním klíčem platným 30 dnů. Pokud se na konci zkušební lhůty rozhodnete zakoupit tento produkt, musíte si opatřit nový licenční klíč. Klikněte na **Koupit** a z on-line obchodu obdržíte nový **Licenční klíč**.

Klikněte na **Online registrace** pro aktivování produktu. Budete tak moci využívat bezplatnou technickou podporu a další služby.

Pro zadání nového licenčního klíče klikněte na **Vložit nový klíč**. Otevře se následující okno:

Obrázek 6.3. Registrace

Vyplňte licenční klíč do políčka **Sériové číslo**. Klikněte na **Registrovat** pro dokončení registrace.

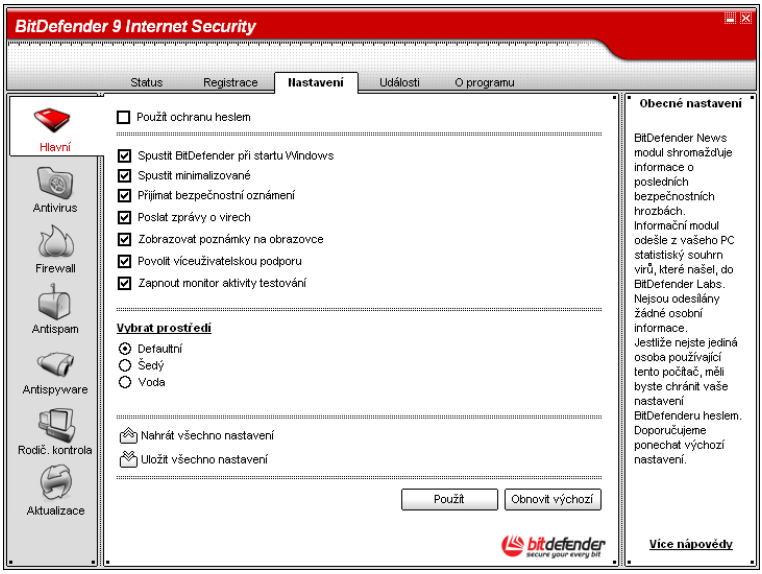
Pokud při zadávání licenčního klíče uděláte chybu, budete vyzváni k novému zadání.

Pokud zadáte platný licenční klíč, zobrazí se potvrzení, že aktivace proběhla úspěšně.

V sekci **Registrace** nyní uvidíte datum vypršení nového licenčního klíče.

6.3. Nastavení řídící konzole

Pro přístup do této sekce klikněte na záložku **Nastavení** v **Hlavním** modulu.



Obrázek 6.4. 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.

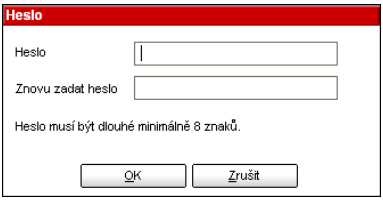
Pro výběr z možností, zaškrtněte myší odpovídající checkbox:

- **Použít ochranu heslem** - umožní nastavení hesla za účelem ochrany konfigurace BitDefenderu;

  Poznámka

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

  Pokud zvolíte tuto možnost, zobrazí se následující okno:



Zadejte heslo do pole **Heslo** a potvrďte jej znovu do pole **Zadejte heslo znovu**. Stiskněte **OK**.

Obrázek 6.5. Heslo

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

Důležité

Pokud zapomenete heslo, je třeba opravit produkt.

- **Spustit BitDefender při startu Windows** - automaticky spustí BitDefender při startu systému.

Poznámka

Doporučujeme ponechat tuto možnost zatrženu.

- **Spustit minimalizované** - minimalizuje řídící konzoli BitDefenderu poté, co je načten při startu systému. V systémové liště se zobrazí pouze ikona BitDefender.
- **Přijímat bezpečnostní oznámení** - přijímat občasná bezpečnostní sdělení o výskytu virových epidemií, zasílané serverem Bitdefender.
- **Poslat zprávy o virech** - odešle hlášení o virech identifikovaných ve Vašem počítači do laboratoře BitDefenderu. Umožní nám sledovat virové outbreaky.

  Hlášení nebudou obsahovat žádné tajné tajné informace typu: Vaše jméno, IP adresa adal., a nebudou použity pro komerční účely. Dodaná informace bude obsahovat pouze jméno viru a bude využita výhradně pro tvorbu statistických hlášení.
- **Zobrazovat poznámky na obrazovce** - zobrazovat vyskakovací okna s poznámkami o stavu produktu.

- **Povolit víceuživatelskou podporu** - umožňuje i dalším uživatelům počítače uložit si vlastní nastavení BitDefenderu.

Poznámka

Prosím proveďte skenování vašeho počítače dvakrát. Je možné, že napoprvé nemusí být vir z NTFS partition odstraněn.

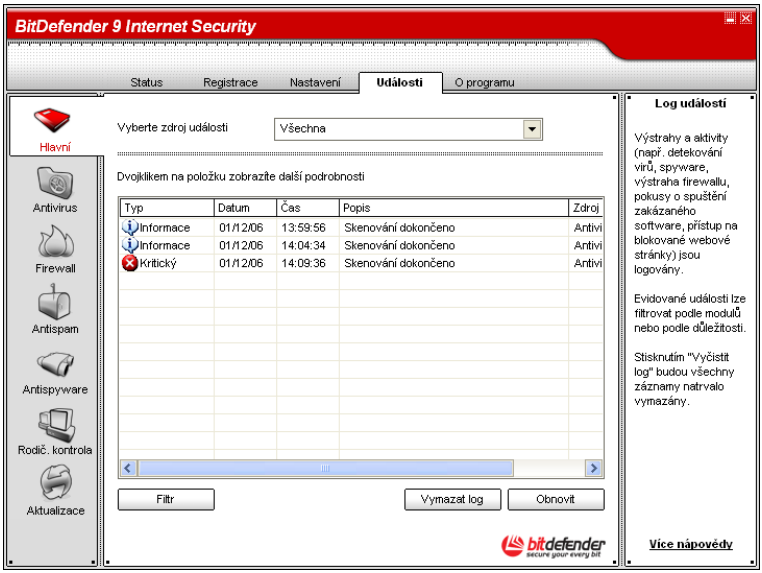
- **Zapnout monitor aktivity testování** - zobrazí / skryje „ *Panel aktivity skenování* “ (str. 31).
- **Vybrat prostředí** - umožňuje vybrat barvu řídící konzole. Skin představuje vzhled pozadí rozhraní. Pro změnu barvy pozadí, klikněte na požadovanou barvu.

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

Klikněte na **Použit** pro uložení změn. Pokud stisknete **Obnovit výchozí**, bude načteno defaultní nastavení.

6.4. Události

Pro přístup do této sekce klikněte na záložku **Události** v **Hlavním** modulu.



Obrázek 6.6. 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 byly nalezeny infikované soubory.

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

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

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

Jestliže je řídící konzole otevřený v záložce **Události** a ve stejnou dobu nastane událost, musíte kliknout na **Obnovit**, abyste událost viděly.

Pro vymazání všech událostí ze seznamu klikněte na **Vymazat log**.

6.5. O BitDefenderu

Pro přístup do této sekce klikněte na záložku **O BitDefenderu** v **Hlavním** modulu.

Obrázek 6.7. Všeobecné informace

V této sekci naleznete kontaktní informace a detaily o produktu.

BitDefenderTM nabízí bezpečnostní řešení požadavků na ochranu v dnešním počítačovém prostředí a dodává toto efektivní řízení hrozeb 38 milionům domácnostem a firemním uživatelům ve více než 100 zemích.

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

Kapitola 7. Modul Antivirus

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

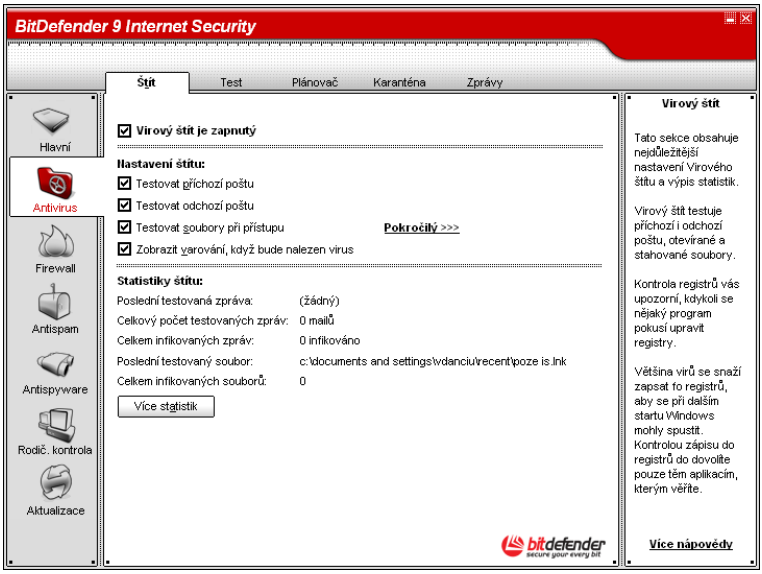
- Skenování při vstupu
- Skenování na požádání
- Plánování skenování
- Karanténa
- Zprávy

Poznámka

Pro více detailů týkajících se modulu **Antivirus** si prohlédněte popis „*Modul Antivirus*“ (str. 19).

7.1. Skenování při vstupu

Pro zpřístupnění této sekce klikněte na záložku **Štít** v modulu **Antivirus**.



Obrázek 7.1. Virový štít

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

Poznámka

Abyste zabránili infikaci Vašeho počítače viry, mějte aktivovaný **Virový štít**.

V dolní části sekce je možné vidět statistiky **Virový štítu** o souborech a emailech. Klikněte na **Více statistik** chcete-li vidět podrobnější okno se statistikami.

7.1.1. Nejdůležitější nastavení

Pro volbu následujících možností klikněte myší na odpovídající checkbox.

- **Testovat příchozí poštu** - skenuje všechny příchozí zprávy.

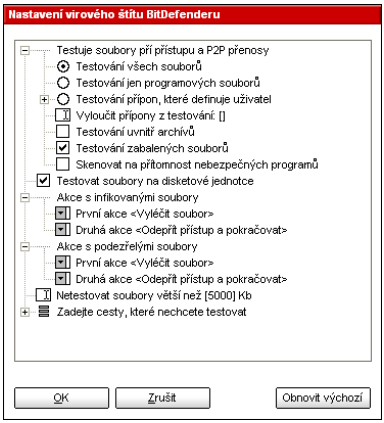
- **Testovat odchozí poštu** - skenuje všechny odchozí zprávy.
- **Testovat soubory při přístupu** - skenuje všechny otevírané soubory.
- **Zobrazit varování, když bude nalezen virus** - je-li v e-mailu nebo souboru nalezen vir, zobrazí se výstražné okno.

  V případě infikovaného souboru bude výstražené 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 BitDefender Laboratoře k další analyze. Můžete zadat také vaši e-mailovou adresu, abyste mohli obdržet zpětnou informaci.

7.1.2. Další možnosti nastavení

Pokročilí uživatelé mohou využít nastavení skenování. Skener může být nastaven tak, aby vynechal přípony, adresáře nebo archivy, o kterých víte, že jsou v pořádku. Klikněte na **Pokročilý >>>** odpovídá **Skenovat otevírané soubory** a vyhledejte požadovaná nastavení.



Obrázek 7.2. Nastavení virového štítu

Klikněte na "+" v checkboxu pro otevření dalších možností a "–" pro zavření dalších možností.

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

- **Testuje soubory při přístupu a P2P přenosy** - skenovat přístupových souborů a spojení prostřednictvím Okamžitých komunikačních softwarových aplikací (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Dále vyberte druh souboru, který má být skenován.

  Dostupné jsou následující možnosti:

Možnost	Popis
Testování všech souborů	Veškeré otevírané soubory budou skenovány, bez ohledu na jejich druh.
Testování jen programových souborů	Budou skenovány 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`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` a `.nws`.
Testování přípon, které definuje uživatel	Budou skenovány pouze soubory s příznaky, které určí uživatel. Příznaky oddělte středníkem ";".
Vyloučit přípony z testování	Soubory s příponami určenými uživatelem, NEBUDOU skenovány. Příznaky oddělte středníkem ";".
Testování uvnitř archivů	Budou skenovány rovněž otevírané archivy. Výběr této možnosti vede ke zpomalení počítače.
Testování zabalených souborů	Budou skenovány veškeré zabalené soubory.

- **Testovat soubory na disketové jednotce** - pro skenování diskety na vstupu.
- **Akce která bude provedena, když bude nalezen virus** - vyberte ze seznamu prvních akcí proti infikovaným souborům. V případě nalezení infikovaného souboru umožňuje BitDefender výběr ze dvou akcí.

  Můžete si vybrat jednu z následujících možností:

Akce	Popis
Odepřít přístup a pokračovat	V případě, že je zjištěn infikovaný soubor, přístup k němu bude odepřen.
Vyléčit soubor	Vyléčit nakažený soubor.
Smazat soubor	Okamžitě smaže infikované soubory, bez výstrahy.
Přesunout soubor do karantény	Infikované soubory jsou přesunuty do karantény.

- **Druhá akce která bude provedena, když první selže** - vyberte ze seznamu druhou akci proti infikovaným souborů.

  K dispozici jsou tyto možnosti:

Akce	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 soubor do karantény	Infikované soubory jsou přesunuty do karantény.

  Jsou dostupné stejné akce pro infikované i podezřelé soubory.

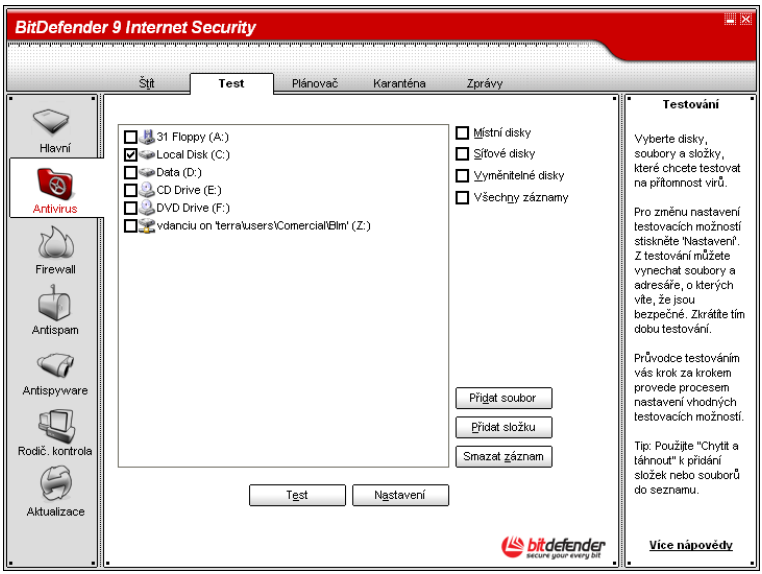
- **Netestovat soubory větší než** - uveďte maximální velikost souborů, které mají být skenovány. Pokud je velikost 0 Kb, budou skenovány všechny soubory.

- **Zadejte cesty, které nechcete testovat** - klikněte na “+” u zvolené možnosti pokud si přejete vynechat nějakou složku ze skenování. Otevře se nová položka `Nový záznam`. Zakšrtněte odpovídající checkbox a v okně, které se otevře vyberte složku, kterou si přejete vyloučit ze skenování.

Klikněte na **OK** pro uložení změn. Pokud stisknete **Obnovit výchozí**, bude načteno defaultní nastavení.

7.2. Skenování na požádání

Pro zpřístupnění této sekce klikněte na záložku **Test** v modulu **Antivirus**.



Obrázek 7.3. Test

V této sekci můžete nastavit BitDefender k proskenování vašeho počítače.

Hlavním úkolem BitDefenderu je udržovat Váš počítač čistý – bez virů. BitDefender postupuje především tak, že drží nové viry mimo Váš počítač a skenuje 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 skenovat na přítomné viry. Rovněž doporučujeme, abyste skenování Vašeho počítače prováděli často.

BitDefender nabízí 4 druhy skenování:

- Okamžité skenování - je třeba učinit několik kroků proto, aby byly skenovány viry ve Vašem počítači;
- Kontextové skenování - klikněte pravím tlačítkem myši na soubor nebo složku a vyberte BitDefender Antivirus v9;
- Uchopit & Přenést do skenování - uchopit a pustit daný soubor nebo složku do grafu průběhu skenování;
- Plánování skenování - můžete naprogramovat BitDefender, aby periodicky skenoval viry v systemu.

7.2.1. Okamžité skenování

Pro skenování virů ve Vašem počítači, proveďte tyto kroky:

Krok 1/5 - Zavřete všechny spuštěné programy

Proto, aby BitDefender mohl provést kompletní skenování, musíte zavřít všechny otevřené programy. Zejména je důležité zavřít Vašeho e-mailového klienta (tj. Outlook, Outlook Express nebo Eudora).

Krok 2/5 - Ověřte si, zda BitDefender zná i nejnovější viry

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

Krok 3/5 - Vyberte cíle skenování

V řídící konzoli vstupte do modulu **Antivirus** a klikněte na záložku Test. Sekce standardně obsahuje seznam oddílů v systému. Kromě seznamu se v sekci vyskytují i tlačítka a volby pro skenování.

Sekce obsahuje tato tlačítka:

- **Přidat soubor** - otevře okno Procházet, kde si můžete vybrat soubor(y), které chcete skenovat.

- **Přidat složku** - analogicky, v okně Procházet si vyberete složku (složky), které chcete skenovat.

Poznámka

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

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

Poznámka

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

- **Nastavení** - otevře okno, kde můžete nastavit, které soubory mají být skenovány, akci, která má být provedena s infikovanými soubory,generování výstražných hlášek, ukládání výsledků skenování.

- **Test** - spustí skenování systému podle vybraných možností.

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

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

Poznámka

Pokud chcete skenovat viry v celém počítači, zaškrtněte volbu **Všechny záznamy**.

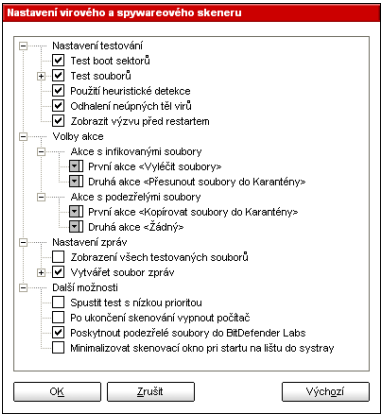
Důležité

Pokud se v počítačích příliš nevyznáte, klikněte jednoduše na tlačítko **Test**. BitDefender spustí skenování Vašeho počítače podle standardních nastavení, která jsou dostatečná.

Krok 4/5 - Vyberte možnosti skenování

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

Klikněte na **Nastavení** v sekci Skenování pro zjištění těchto možností.



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

Obrázek 7.4. Nastavení testu

Možnosti skenování jsou seskupeny do 4 kategorií:

- **Nastavení testování**
- **Volby akce**
- **Nastavení zpráv**
- **Další možnosti**

Poznámka

Klikněte na "+" pro otevření možnosti, nebo na "–" pro zavření možnosti.

- Specifikujte typy objektů, které mají být skenovány (archivy, e-mailové zrávy a další) a další možnosti. To lze provést zaškrtnutím požadované možnosti v **Nastavení testování**.

  Dostupné jsou následující možnosti:

Možnost		Popis
Test boot sektorů		Skenovat zaváděcí sector systému.
Test souborů	**Testovat všechny soubory**	Skenovat veškeré soubory bez ohledu na jejich druh.
	Testovat programových souborů	Skenovat pouze programové soubory. Tzn. pouze soubory s těmito příznaky: `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`.
	Testovat přípony definované uživatelem	Skenovat pouze soubory s příznaky určenými uživatelem. Příznaky musí být odděleny středníkem ";".
	Vyřadit přípony, které uživatel definoval	Skenovat všechny soubory, kromě těch, které mají příznak určený uživatelem. Příznaky musí být odděleny středníkem ";".
	Otevření zabalených programů	Skenovat zabalené soubory.
	Otevření archívů	Skenovat vnitřní archívy.
	Otevření archívů emailů	Skenovat vnitřní mailové archivy.
Použití heuristické detekce		Použít heuristické skenování souborů. Cílem heuristického skenování je identifikovat nové viry na bázi určitých šablon (vzorů) a algoritmů, předtím než je nalezena nova 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.
Odhalení neupných těl virů		Zjišťovat i nekompletní viry (viry s nekompletním tělem).

Možnost	Popis
Zobrazit výzvu před restartem	Pokud akce vyžaduje restart, uživatel bude vyzván k restartu.

- Specifikujte akci, která se má provést infikované a podezřelé soubory. Otevřete **Možnosti akcí** 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
Zádný	S infikovaným souborem 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 dezifnikovat, izolovat v karanténní zóně nebo jej smazat.
Vyléčit soubory	Vyléčit nakažené soubory.
Smazat soubory	Smazat infikované soubory.
Přejmenovat soubory	Změnit přípony infikovaných souborů. Nový příznak 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.
Kopírovat soubory do karantény	Kopírovat infikované soubory do karanténní zóny. Prakticky to znamená duplikaci infikovaného souboru a kopie tohoto souboru se objeví v karanténní zóně, avšak infikovaný soubor nebude přesunut z původního umístění.
Přesunout soubory do karantény	Přesunout infikované soubory do karanténní zóny.

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

Možnost		Popis
Zobrazení všech testovaných souborů		Ukáže všechny skenované soubory a jejich status (infikované nebo ne). Výběr této možnosti vede ke zpomalení počítače.
Vytvářet soubor zpráv	**Jméno soubor zpráv** `vscan.log`	Jedná se o editovatelné pole, které umožňuje změnit název souboru s zprávem. Klikněte na tuto volbu a zadejte nový název.
	Omezit velikost souboru zpráv do [0] KB	Omezení velikosti souboru zpráv. Zadejte požadovanou maximální velikost.

Poznámka

Soubor s zprávem naleznete i v modulu **Antivirus**, v sekci Zprávy.

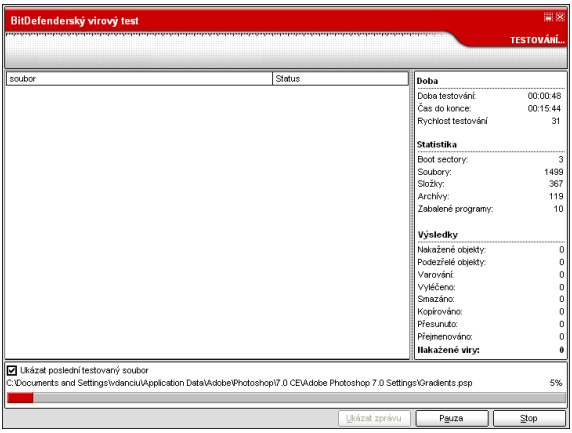
- Specifikujte další možnosti. Otevřete **Další možnosti**, kde můžete vybrat následující možnosti:

Možnost	Popis
Spustit test s nízkou prioritou	Sníží prioritu skenovacího procesu, tím se umožní ostatním programům pracovat rychleji. Zvýší se však doba skenovacího procesu.
Po ukončení skenování vypnout počítač	Vypne počítač po ukončení skenovacího procesu.
Poskytnout podezřelé soubory do BitDefender Laboratoří	Po ukončení skenování budete moci odeslat všechny podezřelé soubory do BD laboratoří k analyze.
Minimalizovat skenovací okno při startu na lištu do systray	Minimalizuje skenovací okno do tray-ikony, dvojklikem na tuto ikonu BitDefender opět otevřete.

Klikněte **OK** pro uložení změn, nebo klikněte **Výchozí** pro návrat k výchozímu nastavení.

Krok 5/5 - Skenování virů

Poté co jste nastavili možnosti skenování, zbývá odstartovat skenování systému. Klikněte proto na **Test**. Operace může trvat delší dobu, v závislosti na velikosti Vašeho hard disku.



Obrázek 7.5. Virový Test

V průběhu skenování Vám BitDefender bude ukazovat průběh skenování a upozorňovat Vás, pokud nalezne viry.

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

Jsou dostupná tři tlačítka:

- **Stop** - objeví se nové okno, v němž můžete ukončit ověřování (verifikaci) systému. Zvolte **Ano**&**Zavřít** pro opuštění okna.
- **Pauza** - skenování se dočasně zastaví - pro pokračování stiskněte tlačítko **Pokračovat**.
- **Ukázat zprávu** - otevře se report o skenování.

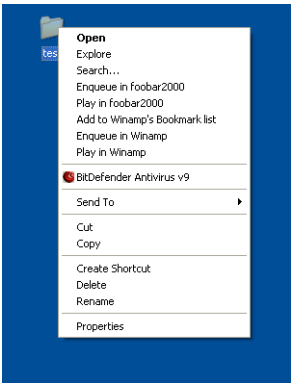
Poznámka

Soubor s reportem je automaticky uložen do sekce Zprávy v modulu **Antivirus**.

Na liště se zobrazí ikona, pokud běží skenovací process.

7.2.2. Kontextuální skenování

Pravým tlačítkem myši klikněte na soubor nebo složku, kterou chcete skenovat a vyberte možnost **BitDefender Antivirus v9**.



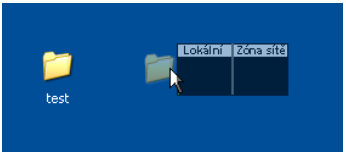
Obrázek 7.6. Kontextové skenování

Vytvoří se soubor s reportem nazvaný `vscan.log` a uvidíte jej v sekci Zprávy v modulu **Antivirus**.

7.2.3. Skenování pomocí uchopit & přenést

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

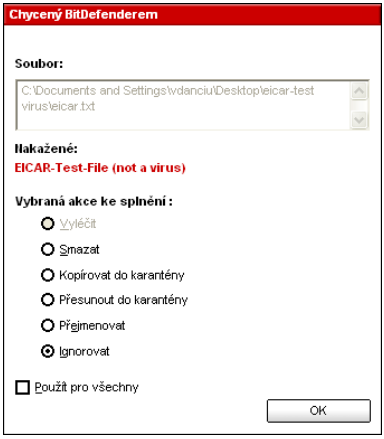
Obrázek 7.7. Táhnout soubor



Obrázek 7.8. Položit soubor

Vytvoří se soubor s reportem nazvaný `activbar.log` a uvidíte jej v sekci Zprávy v modulu **Antivirus**.

V obou případech se objeví skenovací okno. Jakmile je objeven infikovaný soubor, objeví se okno s výzvou k výběru akce pro tento soubor.



V okně uvidíte název souboru a jméno viru.

Obrázek 7.9. Výběr akcí

Můžete si vybrat jednu z následujících akcí pro infikovaný soubor:

- **Vyléčit** - vyléčit nakažené soubory;
- **Smazat** - smazat infikované soubory;
- **Kopírovat do karantény** - kopírovat infikovaný soubor do karanténní zóny;
- **Přesunout do karantény** - přesunout infikovaný soubor do karanténní zóny;
- **Přejmenovat** - změnit přípony infikovaných souborů. Nové přípony infikovaných souborů budou `.vir`.
- **Ignorovat** - ignorovat infekci. U infikovaného souboru nebude provedena žádná akce.

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

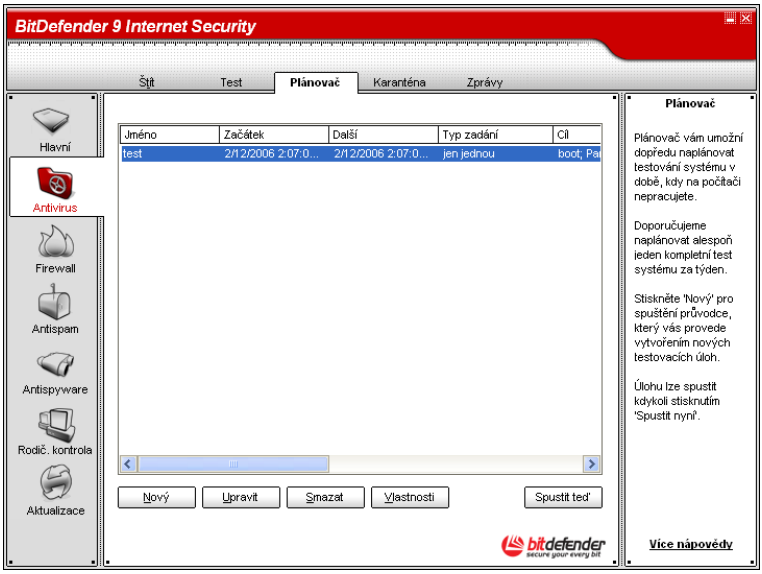
Poznámka

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

Klikněte **OK**.

7.2.4. Plánování skenování

Pro zpřístupnění této sekce klikněte na záložku **Plánovač** v modulu **Antivirus**.



Obrázek 7.10. Plánovač

Jelikož skenování zabere určitý čas a funguje nejlépe, když máte zavřené všechny ostatní programy, je pro Vás nejlepší naplánovat skenování na dobu, kdy nepoužíváte počítač. Předpokladem je, že uživatel musí nejprve vytvořit takzvané zadání (práci,událost).

Plánovač obsahuje průvodce tvorbou nových zadání pro skenování, který je Vám k dispozici při všech operacích spojených s plánováním skenování, ať již se jedná o vytváření nového zadání nebo modifikaci existujícího.

Plánovač obsahuje několik tlačítek pro administraci zadání skenování.

- **Nový** - spustí průvodce, který vás provede tvorbou nového zadání pro skenování.

- **Upravit** - modifikuje vlastnosti dříve vytvořených zadání. I zde se spustí průvodce.

Poznámka

Pokud změníte název události, bude vytvořena nová událost pod nově zavedeným jménem.

- **Smazat** - smaže vybrané zadání.
- **Spustit ted'** - okamžitě spustí vybrané zadání.
- **Vlastnosti** - zobrazí vlastnosti vybraného zadání.

Plánovač obsahuje rovněž seznam veškerých zadání, jejich názvů, datumů prvních provedení, datumů příštích provedení a typ zadání (periodické nebo pouze jednorázové).

Pokud kliknete pravým tlačítkem na naplánovanou událost, v kontextovém menu se zobrazí stejné akce jako výše uvedené.

Poznámka

Plánovač umožňuje neomezený počet zadání pro plánování skenování.

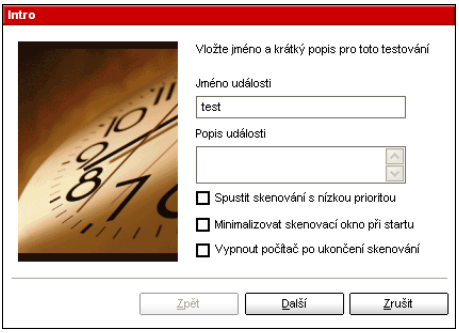
Nastavení zadání pro skenování můžete rovněž ovládat s použitím klávesnice: tlačítkem **Delete** můžete smazat vybrané zadání, tlačítkem **Enter** můžete zobrazit vlastnosti vybraných zadání, tlačítkem **Insert** můžete vytvořit nové zadání (objeví se průvodce Plánovačem).

Poznámka

Stiskem navigačních tlačítek můžete rolovat stránku nahoru, dolů, doprava, doleva.

Klikněte na **Nový** pro zadání nové položky do plánovače. Tím se spustí průvodce, který Vás provede krok za krokem nastavením plánovaného skenování.

Krok 1/9 - Začátek



Obrázek 7.11. Intro

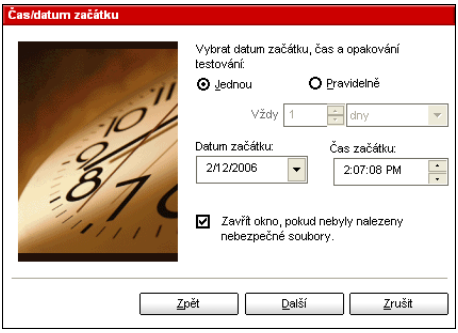
Napište název nového zadání do pole **Jméno** a krátký popis do pole **Popis události**.

Jsou dostupné následující možnosti:

- **Spustít skenování s nízkou prioritou** - sníží prioritu skenovacího procesu, tím se umožní ostatním programům pracovat rychleji. Zvýší se však doba skenovacího procesu.
- **Minimalizovat skenovací okno při startu** - minimalizuje skenovací okno do tray-ikony, dvojklikem na tuto ikonu BitDefender opět otevřete.
- **Vypnout počítač po ukončení skenování** - vypne počítač po ukončení skenovacího procesu.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 2/9 - Čas/datum startu



Obrázek 7.12. Čas/datum startu

Vyberte frekvenci skenování:

- **Jednou** - spustí skenování jen jednou, v určený okamžik.
- **Pravidelně** - spustí skenování opakovaně v určitých časových intervalech (hodiny, dny, týdny, měsíce, roky) počínaje zadaným datem.

Pokud chcete, aby se skenování opakovalo v určitých intervalech, zaškrtněte check box u **Pravidelně**. Do všech polí počínaje **Vždy** vyplňte příslušné číslo dne, měsíce, datum startu a čas opakování procesu skenování.

Poznámka

Můžete použít šipky nahoru / dolů pro zvětšení / zmenšení příslušného čísla.

Zvolte interval – minuty, hodiny, dny , týdny, měsíce, roky - ve kterém se má skenování opakovat.

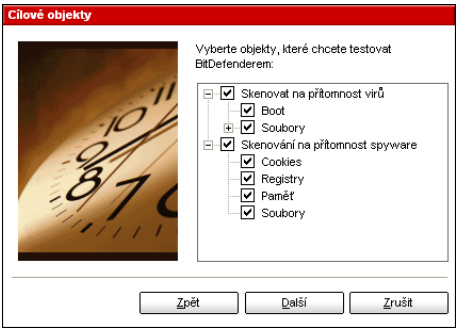
Důležité

Pokud jste se rozhodli pro opakované skenování, bude k němu docházet po neomezenou dobu. Pro ukončení opakování daného skenování jej musíte vymazat ze seznamu zadání v okně Plánovače.

Pokud chcete automaticky zavřít dialog o skenování, není-li nalezen zavirovaný soubor, zvolte checkbox odpovídající této možnosti.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 3/9 - Cílové objekty



Obrázek 7.13. Cílové objekty

Vyberte objekt, který chcete proskenovat:

- **Boot** - skenovat zaváděcí sector, identifikovat zaváděcí viry;
- **Soubory** - skenovat soubory;
- **Databázi pošty** - skenovat archivy mailů, nalézt mailové viry;
- **Archívy** - skenovat vnitřní archivy;
- **Zabalené soubory** - skenovat zabalené soubory;
- **Cookies** - skenuje cookies souborů proti spyware;
- **Registry** - skenuje zápisy do registrů proti spyware;
- **Paměť** - skenuje paměť proti spyware;
- **Soubory** - skenuje soubory proti spyware.

Zaškrtnutím vyberte jeden nebo více objektů pro skenování.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 4/9 - Cílová cesta

Obrázek 7.14. Cílová cesta

Specifikujte cestu k objektu, který chcete proskenovat.

Jedná se o rozbalovací okno, které Vám umožní vybrat oddíly a složky, které mají být skenovány. Postavíte-li se kurzorem na složku, v poli dole se objeví kompletní cesta k této složce.

Poznámka

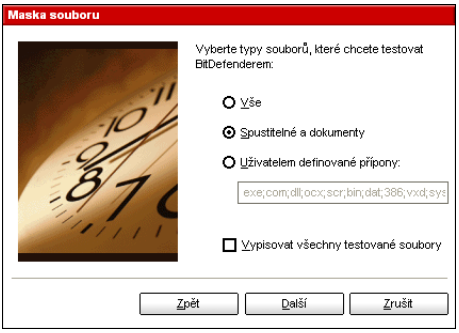
Klikněte na znaménko "+" pro otevření možnosti nebo na znaménko "–" pro zavření možnosti.

Rovněž můžete provést rychlý výběr umístění, pro který slouží dva checkboxy v okně zcela nahoře:

- **Místní disky** - pro skenování všech místních disků;
- **Síťové disky** - pro skenování všech síťových disků.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 5/9 - Maska souboru



Obrázek 7.15. Maska souboru

Specifikujte typy souborů, které mají být skenovány. Tento krok je nutný, pokud jste zvolili skenování souborů ve třetím kroku.

Můžete si vybrat:

- **Vše** - skenovat všech souborů, bez ohledu na jejich druh;
- **Spustitelné a dokumenty** - skenovat programové soubory a dokumenty;
- **Uživatelem definované přípony** - skenovat pouze soubory, jejichž přípony jsou na seznamu.

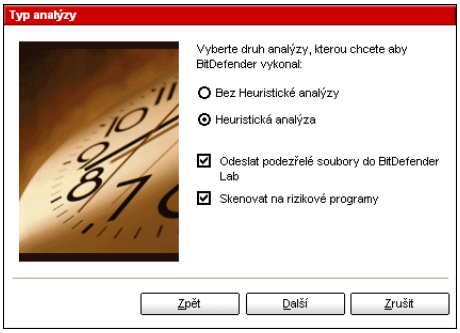
Poznámka

Tyto přípony musí být odděleny středníkem ";".

Pokud si přejete získat informaci o všech skenovaných souborech, jak infikovaných tak neinfikovaných, vyberte možnost **Vypisovat všechny testované soubory**. Výběr této možnosti vede ke zpomalení počítače.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 6/9 - Typ analýzy



Obrázek 7.16. Typ analýzy

Vyberte si typ skenování:

- **Bez Heuristické analýzy** - znamená skenování souborů metodou založenou na známých virových signaturách;
- **Heuristická analýza** - představuje metodu založenou na určitých algoritmech, jejichž cílem je identifikovat nové neznámé viry. Příležitostně může být oznámen podezřelý kód v normálních programech, generující tzv "falešný poplach".

K dispozici jsou tyto možnosti:

- **Odeslat podezřelé soubory do BitDefender Laboratoří** - Po ukončení skenování budete moci odeslat všechny podezřelé soubory do BD laboratoří k analyze.
- **Skenovat na rizikové programy** - Skenovat na přítomnost nebezpečného software jako jsou dialery, spyware, adware. S nalezenými soubory bude zacházeno jako s infikovanými soubory. Software, který obsahuje adawre komponenty může přestat fungovat, pokud bude tato možnost zvolena.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 7/9 - Mód akcí

Obrázek 7.17. Mód akcí

BitDefender umožňuje vybrat dvě akce, které mají být provedeny v případě nalezení infikovaného nebo podezřelého souboru. Zvolte požadovanou akci.

Akce	Popis
Zádný	S infikovaným souborem 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 dezifnikovat, izolovat v karanténní zóně nebo jej smazat.
Vyléčit soubory	Vyléčit nakažené soubory.
Smazat soubory	Smazat infikované soubory.
Přejmenovat soubory	Změnit přípony infikovaných souborů. Nový příznak 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.
Kopírovat soubory do karantény	Kopírovat infikované soubory do karanténní zóny. Prakticky to znamená duplikaci infikovaného souboru a kopie tohoto souboru se objeví v karanténní zóně, avšak infikovaný soubor nebude přesunut z původního umístění.

Akce	Popis
Přesunout soubory do karantény	Přesunout infikované soubory do karanténní zóny. Pokud je virus v karanténě, nemůže způsobit žádnou škodu.

Poznámka

Doporučujeme v první akci zvolit **Vyléčit** a v druhé akci **Přesunout soubory do karantény**.

Jsou dostupné stejné akce pro infikované i podezřelé soubory.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 8/9 - Informační zpráva

Obrázek 7.18. Informační zpráva

Pro vytvoření reportu o skenování, zaškrtněte **Vytvořit soubor zpráv**. Zaškrtnutím této volby budou zpřístupněny další možnosti pro tvorbu souboru s reportem.

Vyplňte název souboru s reportem do pole **Jméno souboru zpráv**. Defaultně je název nastaven `schedule.log`. Soubor bude obsahovat všechny informace o procesu skenování: počet nalezených virů, počet skenovaných souborů, počet vyléčených a smazaných souborů.

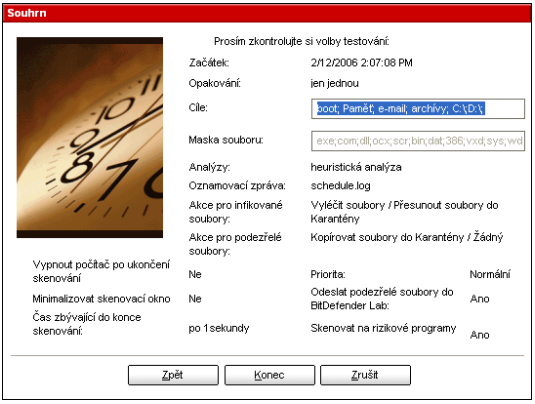
Můžete omezit velikost souboru zpráv. Zadejte požadovanou maximální velikost.

Poznámka

Soubor s reportem naleznete v modulu **Antivirus**, v sekci Zprávy.

Klikněte **Další** pro pokračování. Kliknete-li na **Zrušit**, objeví se okno požadující potvrzení Vaší volby: zrušit nebo pokračovat v průvodci.

Krok 9/9 - Souhrn



Obrázek 7.19. Souhrn

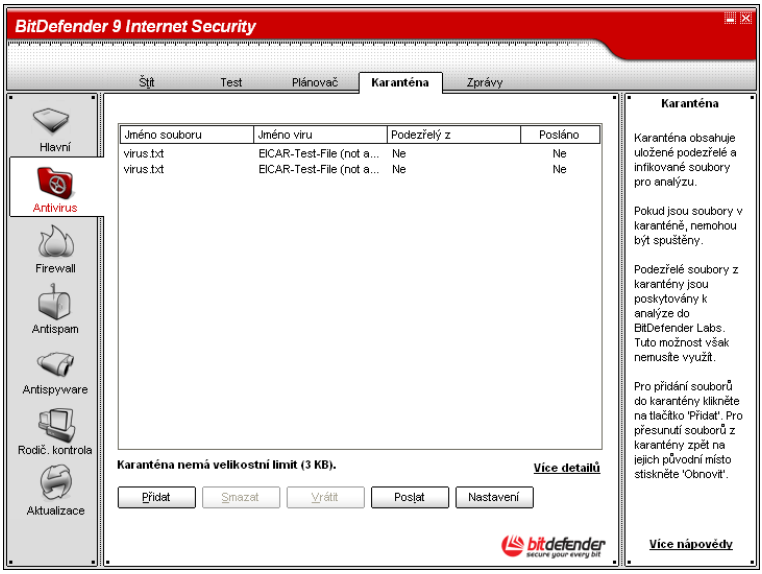
Toto je poslední krok tvorby zadání pro skenování. V tomto okně jsou zobrazena nastavení všech zadání. Změny v nastavení můžete provést, vrátíte-li se do předchozích kroků kliknutím na **Zpět**.

Pokud již žádné modifikace provádět nechcete, klikněte na **Konec**.

V sekci Plánovač se objeví Začátek nového zadání.

7.3. Karanténa

Pro zpřístupnění této sekce klikněte na záložku **Plánovač** v modulu **Antivirus**.



Obrázek 7.20. 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 BitDefenderu.

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

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

Poznámka

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

Sekce **Karanténa** obsahuje několik tlačítek pro administraci souborů.

- **Přidat** - přidat soubory do karantény. Použijte toto tlačítko pro přidání souboru, u kterého máte podezření z infikace do karantény. Otevře se okno pro výběr souboru z místa na disku. This way the file is copied to quarantine.

  Pokud chcete přesunout soubor do karantény musíte zaškrtnout checkbox **Vymazat z původního umístění**. Rychleji lze podezřelé soubory přidat do Karantény pomocí metody chytit & položit.

- **Smazat** - smaže vybrané soubory z vašeho počítače.

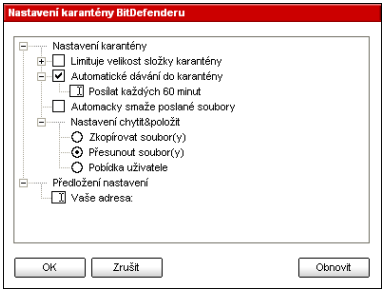
- **Vrátit** - vrátí vybrané soubory do jejich původního umístění.

- **Poslat** - odešle vybrané soubory na další analýzu do laboratoře BitDefenderu.

Důležité

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

- **Nastavení** - otevře rozšířené možnosti pro karanténní zónu. Objeví se následující okno:



Obrázek 7.21. Nastavení karantény

Možnosti karantény jsou seskupeny do dvou kategorií:
- **Nastavení karantény**
- **Předložení nastavení**

Poznámka

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

Nastavení karantény

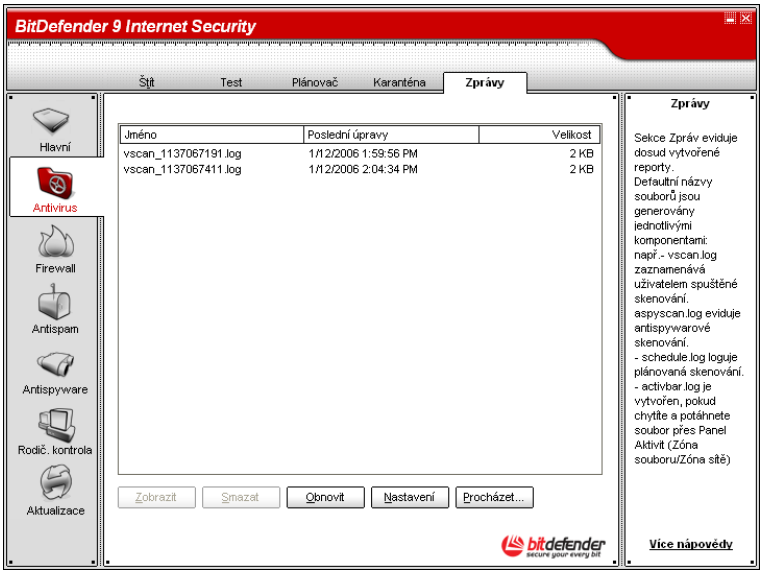
- **Limituje velikost složky Karanténa** - tato volba Vám pomůže regulovat velikost složky karanténa. Tato volba je přístupná a velikost je defaultně nastavena na 12000 KB.
- **Automatické dávání do karantény** - automaticky odesílat soubory v karanténě do laboratoře BitDefenderu na další analýzu. V poli **Posílat každých** můžete nastavit periodu (v minutách) mezi jednotlivými odesláními.
- **Automaticky smaže poslané soubory** - automaticky vymazat soubory z karantény, poté co byly odeslány do laboratoře BitDefenderu na analýzu.
- **Nastavení chytit&položit** - používáte-li metodu chytit&položit pro přidávání souborů do karantény, můžete zde specifikovat akci.

Předložení nastavení

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

7.4. Zprávy

Pro zpřístupnění této sekce klikněte na záložku **Zprávy** v modulu **Antivirus**.



Obrázek 7.22. Zprávy

Sekce **Zprávy** obsahuje seznam veškerých dosud vygenerovaných souborů s reporty. U každého souboru je uveden jeho název, velikost a datum poslední modifikace.

Po započetí procesu skenování má uživatel možnost zvolit si vytvoření souboru s reportem, kde může nalézt informace o procesu skenování. Uživatel si může tyto reporty prohlédnout přímo z řídící konzole.

BitDefender vede záznamy o svých hlavních aktivitách provedených na Vašem počítači. Jedná se o tyto defaultní soubory s reporty:

- Vscan.log je pořízen okamžitě, když skenujete Váš systém;
- Schedule.log je záznam pořizovaný z plánovaných skenování, která jste si nastavili;
- Activbar.log tento záznam je vytvořen, když skenujete pomocí metody chytit&položit.

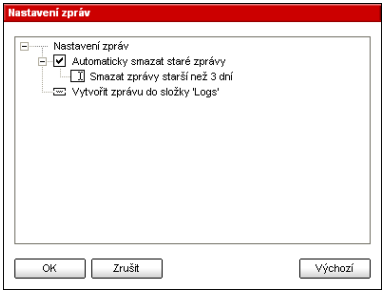
Sekce **Zprávy** obsahuje tlačítka pro administraci reportů. Funkce jednotlivých talčítek bude vystvětlena dale:

- **Zobrazit** - otevře vybraný soubor s reportem.
- **Smazat** - smaže vybraný soubor s reportem.
- **Obnovit** - obnovit sekci **Zprávy**. Za situace, kdy máte otevřenou sekci **Zprávy** v řídící konzoli a současně provádíte skenování Vašeho počítače , objeví se nový report s výsledky tohoto skenování pouze za předpokladu, že kliknete na tlačítko **Obnovit**.
- **Procházet...** - otevře okno, v němž si můžete vybrat soubory s reporty, které si chcete prohlédnout.

Poznámka

Soubory s reporty jsou defaultně uloženy ve složce, kde je instalován BitDefender. Pokud jste uložili soubory s reporty do jiného adresáře, musíte použít tlačítko **Procházet**, abyste se k nim dostali.

- **Nastavení** - otevře možnosti rozšířených nastavení reportů. Objeví se následující okno:



Obrázek 7.23. Nastavení zpráv

Poznámka

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

- **Automaticky smazat staré zprávy** - kontroluje počet zpráv, maže starší než zadaný počet dní. Defaultní hodnota je 3 dny. Defaultní čas můžete změnit.
- **Vytvořit zprávu do složku** - specifikuje složku, do které bude uložena vytvořená zpráva.

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

Kapitola 8. Modul Firewall

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

- Průvodce nastavením Firewallu
- Status Firewallu
- Ochrana spojení
- Aktivita Firewallu
- Zpráva o výsledcích
- Pokročilá nastavení

Poznámka

Pro více detailů týkajících se modulu **Firewall** si prohlédněte popis „*Modul Firewall*“ (str. 20).

8.1. Průvodce nastavením Firewallu

Po prvním spuštění Bitdefenderu se objeví průvodce, který vám pomůže nastavit Firewall, abyste vytvořili pravidla Firewallu. Ty jsou potřebné pro vaše nejčastěji používané aplikace. Konečným výsledkem je chráněný systém s fungujícím poštovním klientem a internetovým prohlížečem.

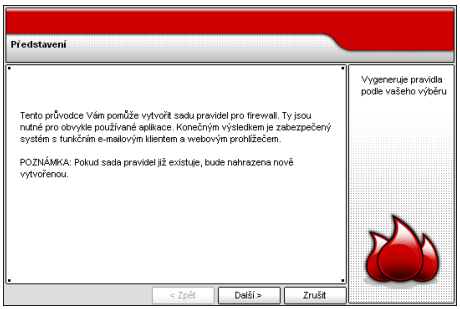
Poznámka

Průvodce může být také spuštěn, kdykoliv chcete kliknutím **Průvodce pravidel** z menu „*Pokročilá nastavení*“ (str. 92).

Důležité

Jestli průvodce nebude správně ukončen, bude Firewall vypnut. Průvodce se automaticky objeví, když se pokusíte Firewall zapnout.

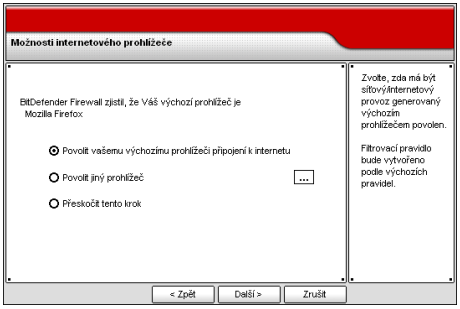
8.1.1. Krok 1/6 - Uvítací okno



Obrázek 8.1. Uvítací okno

Klikněte na **Další**.

8.1.2. Krok 2/6 - Nastavení internetového prohlížeče



Obrázek 8.2. Nastavení internetového prohlížeče

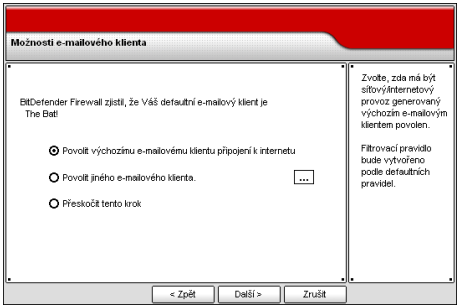
BitDefender detekuje váš standardní prohlížeč. Vyberte, zda síťové/internetová doprava standardního prohlížeče má být povolena, nebo vyberete jiný prohlížeč.

Důležité

Jestliže přeskočíte tento krok, pravidla, která závisí na této volbě, nebudou vytvořena. Budete muset vytvořit váš vlastní soubor pravidel. Nepřeskakujte tento krok, jestliže si nejste jistí, že chcete vytvořit vhodná pravidla sám.

Klikněte na **Další**.

8.1.3. Krok 3/6 - Nastavení poštovního klienta



Obrázek 8.3. Nastavení poštovního klienta

BitDefender detekuje vašeho standardního poštovního klienta. Vyberte, zda síťová/internetová spojení standardního poštovního klienta budou povolena, nebo vyberete jiného poštovního klienta.

Důležité

Jestliže přeskočíte tento krok, pravidla, která závisí na této volbě, nebudou vytvořena. Budete muset vytvořit váš vlastní soubor pravidel. Nepřeskakujte tento krok, jestliže si nejste jistí, že chcete vytvořit vhodná pravidla sám.

Klikněte na **Další**.

8.1.4. Krok 4/6 - Nastavení proxy serveru

Obrázek 8.4. Nastavení proxy serveru

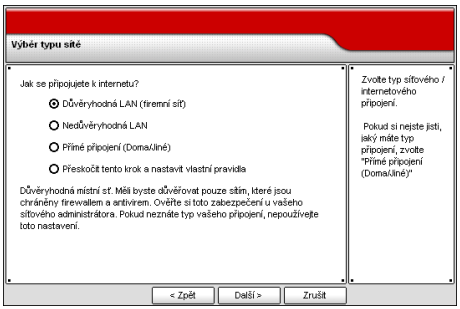
Jestliže používáte proxy server pro připojení k Internetu, BitDefender to zjistí. Vyberte, zda síťové/internetové spojení k proxy serveru má být povoleno, nebo klikněte na . . . odpovídající **Používám jiný server** a vepište IP adresu a port vašeho Proxy Serveru.

Důležité

Jestliže přeskočíte tento krok, pravidla, která závisí na této volbě, nebudou vytvořena. Budete muset vytvořit váš vlastní soubor pravidel. Nepřeskakujte tento krok, jestliže si nejste jistí, že chcete vytvořit vhodná pravidla sám.

Klikněte na **Další**.

8.1.5. Krok 5/6 - Výběr typu sítě



Obrázek 8.5. Výběr typu sítě

Musíte vybrat typ vašeho síťového/internetového připojení. Následující volby jsou dostupné:

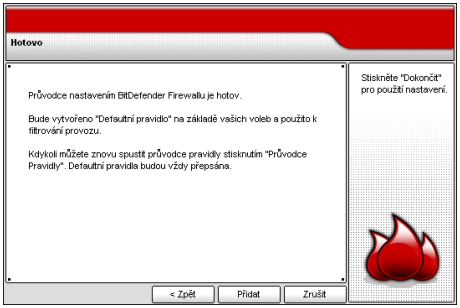
Možnost	Popis
Důvěryhodná místní síť (LAN)	Měli byste důvěřovat jen sítím, které jsou chráněny Firewallem a Antivirem. Prosím kontaktujte vašeho správce sítě, abyste toto ověřili. Jestliže nevíte, jaký typ připojení používáte, nezaškrtávejte tuto volbu.
Nedůvěryhodná místní síť (LAN)	Vyberte toto nastavení, jestliže jste hostem v jiné síti než vaše domácí nebo firemní. Jestliže, nevíte jaký typ připojení používáte, nezaškrtávejte tuto volbu.
Přímé připojení	Vyberte toto nastavení, jestliže jste připojeni přímo k internetu nebo jestli nevíte, jaký typ připojení používáte. Všechna příchozí spojení budou zakázána. Zatímco toto může způsobit některým aplikacím problémy s připojením, zajistí to zvýšenou úroveň bezpečnosti. Můžete přidat pravidla ručně pro aplikace, které nefungují.

Důležité

Jestliže přeskočíte tento krok, pravidla, která závisí na této volbě, nebudou vytvořena. Budete muset vytvořit váš vlastní soubor pravidel. Nepřeskakujte tento krok, jestliže si nejste jistí, že chcete vytvořit vhodná pravidla sám.

Klikněte na **Další**.

8.1.6. Krok 6/6 - Shrnutí



Obrázek 8.6. Nastavení proxy serveru

Toto je závěrečný krok konfiguračního průvodce. Můžete provádět jakékoliv změny návratem na libovolný předchozí krok (klikněte na **Zpět**).

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

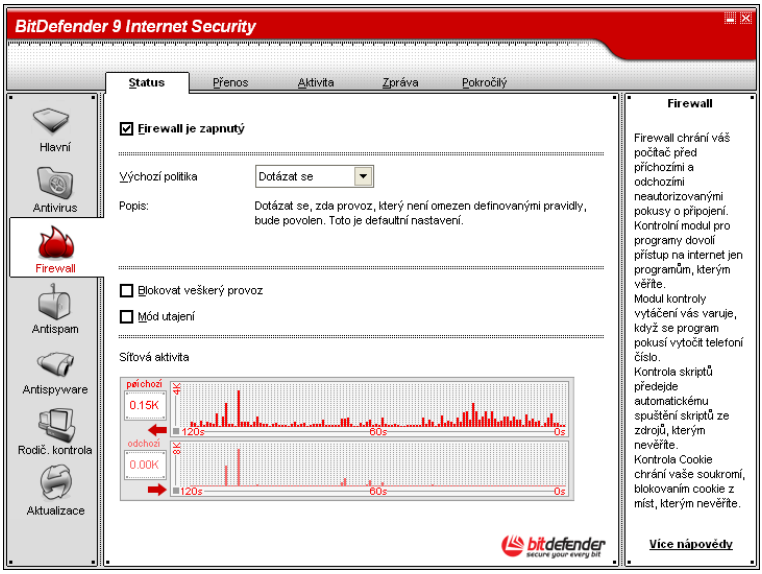
Vytvoří se pravidla nazvaná `Standardní soubor pravidel` v závislosti na vašich volbách a aplikují se na filtr spojení. Můžete kdykoliv znovu pustit Průvodce nastavení Firewallem kliknutím na tlačítko **Průvodce pravidel** v menu „*Pokročilá nastavení*“ (str. 92).

Důležité

Standardní soubor pravidel se přepíše pokaždé, když úspěšně spustíte a ukončíte průvodce.

8.2. Status Firewallu

Pro zpřístupnění této sekce klikněte na záložku **Status** v modulu **Firewall**.



Obrázek 8.7. Status Firewallu

Firewall chrání váš počítač před nepovolenými příchozími i odchozími pokusy o spojení.

V této části můžete povolit/zakázat používání **Firewallu**, aktivovat **Mód utajení**, pozastavit veškerou síťovou komunikaci a nastavit standardní chování při nových událostech.

Zaškrtněte/Odškrtněte zatrhávací políčko **Firewall** jestli chcete povolit/zakázat používání **Firewallu**.

Vyberte tlačítko **Blokovat veškeré provoz** pro zablokování veškeré síťové komunikace.

Poznámka

Pokud nejste jedinou osobou používající tento počítač, doporučujeme chránit nastavení vašeho BitDefenderu heslem. Pro nastavení hesla klikněte na **Hlavní** modul, Nastavení a zvolte **Použít ochranu heslem**.

Ve spodní části sekce můžete vidět statistiky Bitdefenderu týkající se příchozího a odchozího spojení. Graf ukazuje stav internetového spojení za poslední dvě minuty.

Poznámka

Graf se zobrazí, i když je **Firewall** vypnutý.

8.2.1. Nastavení reakcí

Vyberte, jak má BitDefender reagovat, pokud narazí na událost, pro kterou není definováno žádné pravidlo.

Existují 3 typy reakci:

- **Dotázat se** - Zeptá se, jestli pokusy o spojení, která nesplňují žádné ze stávajících pravidel, mají být povoleny. Toto je standardní reakce.
- **Povolit** - Povolí veškeré pokusy o spojení, které neodpovídají žádnému ze stávajících pravidel bez dotázání. Tuto reakci silně nedoporučujeme, ale může být užitečná pro správce sítí.
- **Zakázat** - Zakáže veškeré pokusy o spojení, které neodpovídají žádnému ze stávajících pravidel bez dotázání. Použijte toto nastavení, pokud jste určili pravidla pro všechny programy a spojení, které potřebujete.

Důležité

Jestli je Řídící konzole zavřená a nebylo nalezeno žádné standardní pravidlo pro novou událost, nastaví se reakce **Zakázat**.

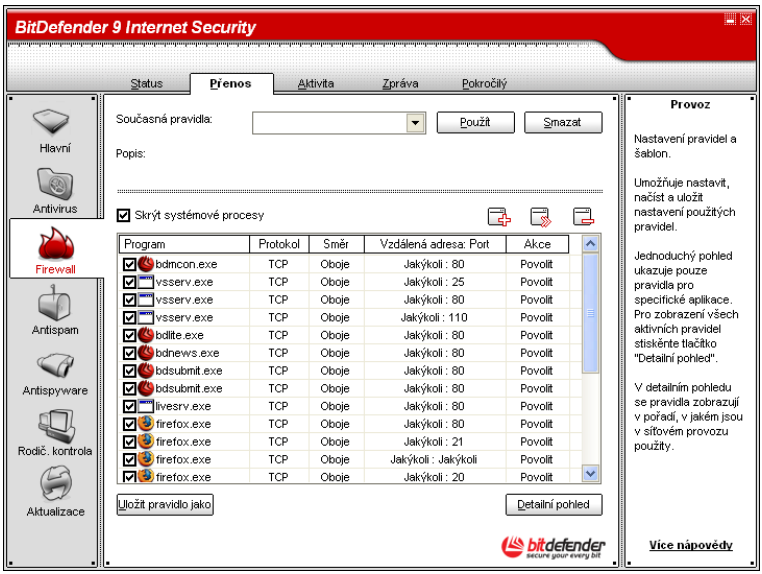
8.2.2. Neviditelný mód(Mód utajení)

Hackeři nebo softwarové programy nemusí zjistit, že váš počítač vůbec existuje. **Neviditelný mód** zastaví odpovědi vašeho počítače na pokusy, jež zkouší, které porty jsou otevřené nebo kde přesně se váš počítač nachází.

Vyberte zatrhávací políčko **Neviditelný mód**, jestli chcete "skrýt" váš počítač před záludnými programy a hackery.

8.3. Kontrola spojení

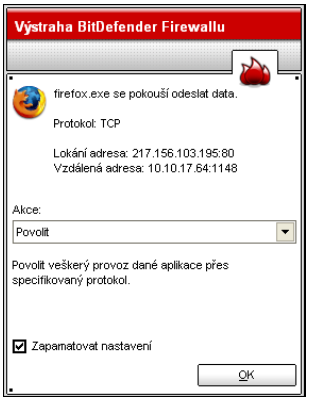
Pro zpřístupnění této sekce klikněte na záložku **Přenos** v modulu **Firewall**.



Obrázek 8.8. Kontrola spojení

V této části můžete specifikovat, která příchozí nebo odchozí spojení se mají povolit/zakázat vytvořením pravidel se specifickými protokoly, porty, aplikacemi a nebo vzdálenými adresami. Můžete také uložit a nahrát soubor pravidel aplikovaných na síťové/internetové připojení.

Se zapnutým **Firewallem** vás bude BitDefender žádat o povolení, kdykoli se bude provádět spojení s Internetem:



Obrázek 8.9. Výstraha Firewallu

Uvidíte následující hlášku: aplikace, která se pokouší připojit k internetu, protokol, IP adresa a port, na kterém se aplikace zkouší připojit.

Zaškrtněte **Zamapatovat nastavení**, vyberte požadovanou **akci** z nabídky a stiskněte **OK** a pravidlo se vytvoří, aplikuje a uloží do tabulky pravidel. Tímto způsobem už nebudete dotazováni, když se tento proces bude opakovat.

Můžete zvolit jednu z následujících možností:

Akce	Popis
Povolit	Povolí všechna spojení této aplikace daným protokolem.
Zakázat	Zakáže všechna spojení této aplikace daným protokolem.
Povolit veškerá spojení této aplikace	Povolí veškerá spojení této aplikace všemi IP protokoly.
Zakázat veškerá spojení této aplikace	Zakáže veškerá spojení této aplikace všemi IP protokoly.
Povolit pouze tohoto vzdáleného hosta	Povolí spojení této aplikaci daným protokolem s určitým vzdáleným hostem.
Povolit pouze tento port	Povolí spojení této aplikaci daným protokolem na určeném portu pro libovolný cíl.
Zakázat tohoto vzdáleného hosta	Zakáže spojení této aplikaci daným protokolem s tímto vzdáleným hostem.
Zakázat pouze tento port	Zakáže spojení této aplikaci daným protokolem na tomto portu pro libovolný cíl.

Důležité

Povolte pokusy o příchozí spojení pouze IP adresám nebo doménám, kterým výslovně věříte.

Pravidla jsou přidána do seznamu, pokud zodpovíte otázky BitDefenderu o novém programu, který se pokouší připojit k Internetu.

Každé zapamatované pravidlo může být zpřístupněno v sekci **Přenos** pro podrobnější nastavení.

Pravidla mohou být uložena do různých souborů pravidel kliknutím na **Uložit pravidlo jako**. Pro použití souboru pravidel jej vyberte z rozevírací nabídky a klikněte na **Použít**.

Jednoduchý náhled zobrazí jen ta pravidla, která se týkají konkrétních aplikací. Pro zobrazení všech aktivních pravidel klikněte na **Detailní pohled**. V detailním náhledu v pořadí, v kterém jsou pravidla zobrazena, jsou aplikována na síťová spojení.

Vyberte zatrhávací políčko **Skrýt systémové procesy** pro skrytí pravidel týkajících se systémových procesů.

Důležité

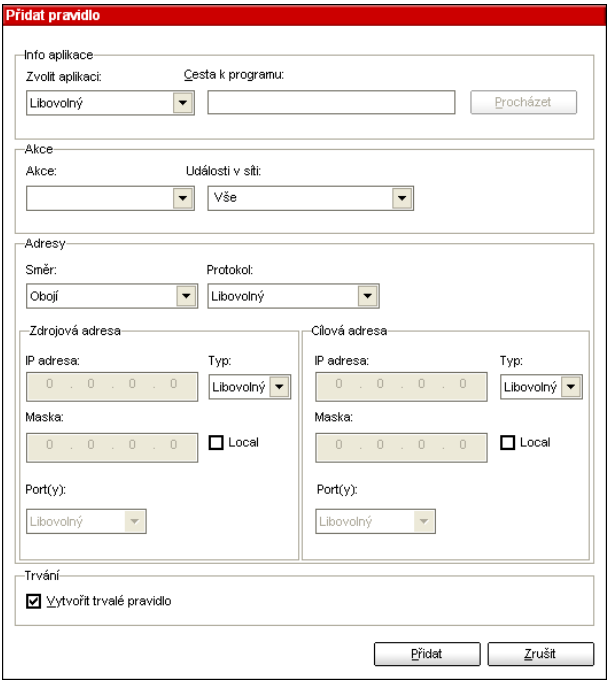
Pravidla jsou uvedená v seznamu z vrchu podle priority, to znamená, že první pravidlo má nejvyšší prioritu. Zvolte **Detailní pohled** za účelem změny jejich priority posunem nahoru a dolů.

Pro vymazání pravidla stačí pravidlo vybrat a stisknout **Vymazat**. Pro vymazání všech pravidel zvolte **Detailní pohled** a stiskněte na **Smazat vše**. Pro změnu pravidla jej vyberte a stiskněte **Upravit**. Pro dočasně ignorování pravidla bez jeho smazání zaškrtněte příslušné políčko.

Poznámka

K dispozici je také kontextová nabídka a obsahuje následující možnosti: **Vymazat**, **Upravit** a **Přidat**.

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



Obrázek 8.10. Volba parametrů

Můžete nastavit parametry:

Klikněte na **Přidat**.

- **Aplikace** - vyberte aplikaci, pro kterou má být pravidlo použito. Můžete vybrat pouze jednu aplikaci (z nabídky **Zvolit aplikaci** vyberte **Cesta k programu**, poté kliknete na **Procházet** a vyberte aplikaci) nebo všechny aplikace (z nabídky **Zvolit aplikaci** vyberte **Libovolný**).
- **Akce** - vyberte akci pro pravidlo a odpovídající událost(i).

Akce	Popis
Povolit	Akce bude povolena.

Akce	Popis
Zakázat	Akce bude zakázána.

- **Adresy** - vyberte směr spojení a protokol pro pravidlo.

  Směr - vyberte směr spojení.

Směr	Popis
Odchozí	Pravidlo se použije pouze pro odchozí spojení.
Příchozí	Pravidlo se použije pouze pro příchozí spojení.
Obojí	Pravidlo se použije pro oba směry.

Protokol - vyberte jeden z protokolů ICMP, TCP, UDP, IGMP, SMP nebo všechny.

Seznam nejpoužívanějších protokolů je k dispozici, aby vám pomohl zvolit pouze vybraný protokol. Vyberte požadovaný protokol (na který se má použít pravidlo) z odpovídající rozevírací nabídky nebo vyberte **Libovolný** pro vybrání všech protokolů.

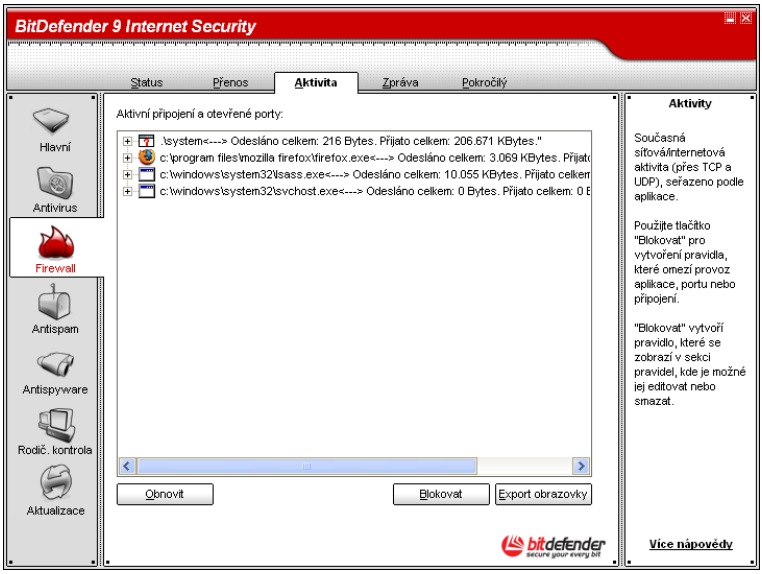
Protokol	Popis
ICMP	Internet Control Message Protocol - je rozšířením internetového protokolu (IP). ICMP podporuje pakety obsahující chybové, kontrolní a informační zprávy. Například příkaz PING používá ICMP pro testování internetového spojení.
TCP	Transmission Control Protocol - TCP umožňuje dvěma počítačům vytvořit spojení a vyměňovat data. TCP zabezpečuje doručení dat a rovněž zaručuje, že pakety budou doručeny v tom samém pořadí, ve kterém byly odeslány.
UDP	User Datagram Protocol - UDP je přenos na bázi IP určený pro vysoký výkon. Hry a další na obrazu založené aplikace často používají UDP.
IGMP	Internet Group Management Protocol - je definován jako standart pro IP multicasting v internetu. Používá se pro vytvoření členství v určitých multicastingvých skupinách na jedné síti.

Protokol	Popis
	Mechanismus protokolu povoluje členům informovat místní router pomocí členských zpráv, že chce přijímat zprávy adresované určité multicastingové skupině.
SMP	Simple Management Protocol - je vylepšená verze tzv. Simple Network Management Protocol (SNMP) s vlastnostmi potřebnými pro podporu větších sítí pracujících na velkém přenosu dat. SMP podporuje také vícenásobné síťové pracovní stanice organizované v hierarchické struktuře.

- **Zdrojová adresa** - vepište IP adresu, masku nebo zaškrtněte **Místní**, jestliže se pravidlo aplikuje na místní počítač. Pokud jste vybrali TCP nebo UDP protokol, můžete vybrat určitý port nebo rozsah portu mezi 0 až 65535. Zda-li chcete pravidlo použít pro všechny porty, zvolte **Libovolný**.
- **Cílová adresa** - vepište IP adresu, masku nebo zaškrtněte **Místní**, jestliže cílem pravidla je místní počítač. Pokud jste vybrali TCP nebo UDP protokol, můžete vybrat určitý port nebo rozsah portu mezi 0 až 65535. Zda-li chcete pravidlo použít pro všechny porty, zvolte **Libovolný**.
- **Trvání** - zaškrtněte políčko **Vytvořit trvále pravidlo** pro uložení pravidla pro budoucí použití. Pokud není toto políčko zaškrtnuté, pravidlo se smaže po restartu počítače nebo aktualizaci Bitdefenderu.

8.4. Kontrola připojení

Pro zpřístupnění této sekce klikněte na záložku **Aktivita** v modulu **Firewall**.



Obrázek 8.11. Kontrola připojení

V této části můžete vidět aktuální síťovou/internetovou aktivitu (přes TCP a UDP) rozdělenou podle aplikací.

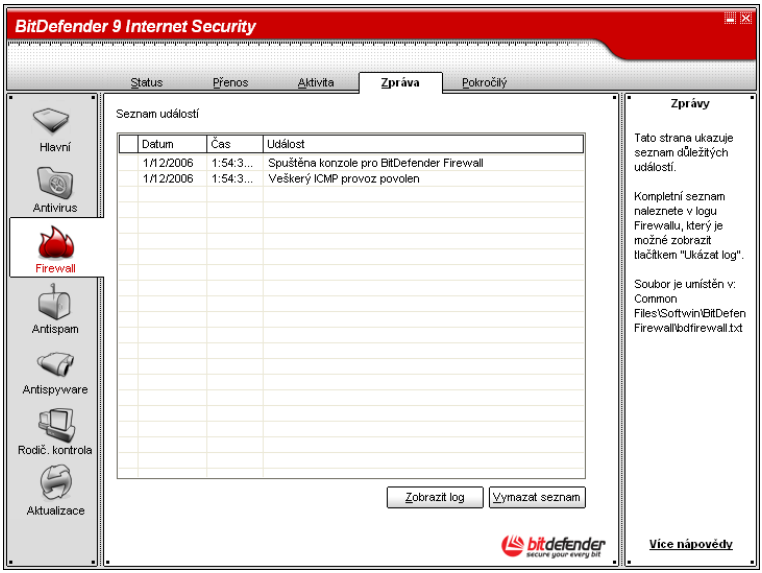
Klikněte na **Blokovat** pro vytvoření pravidla, které zakazuje spojení pro vybranou aplikaci, port nebo připojení.

Použijte tlačítko **Obnovit** pro znovuotevření sekce **Aktivita** (pro zobrazení poslední aktivity modulu **Firewall**).

Stisknutím **Export obrazovky** pro exportování seznamu do souboru `.txt`.

8.5. Zpráva

Pro zpřístupnění této sekce klikněte na záložku **Zpráva** v modulu **Firewall**.



Obrázek 8.12. Zpráva

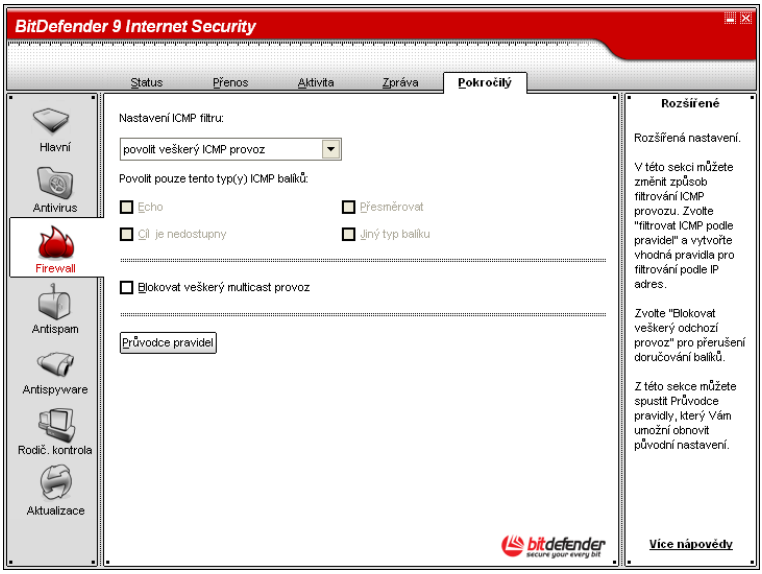
V této části můžete vidět seznam nedávných událostí týkajících se používání modulu Firewall spuštění/zastavení firewallu, zablokované spojení, povolení Neviditelného módu, změny v nastavení, aplikování souboru pravidel) nebo vygenerovaných aktivitami objevených Firewallem (testování portů, zakázané pokusy o spojení podle pravidel).

Pro úplný seznam se prosím podívejte do log souboru BitDefender Firewallu, který může být prohlížen stisknutím **Zobravit log**. Soubor je umístěn ve složce Data Aplikací aktuálního uživatele Windows, pod cestou: `...\Aplication Data\ Bitdefender\Firewall\ log`.

Stiskněte **Vymazat seznam** pro smazání všech údajů z log souboru.

8.6. Pokročilá nastavení

Pro zpřístupnění této sekce klikněte na záložku **Pokročilý** v modulu **Firewall**.



Obrázek 8.13. Pokročilá nastavení

V této části můžete změnit způsob filtrování ICMP spojení a můžete spustit průvodce nastavením, který vám umožní resetovat nastavení do počátečního stavu.

ICMP je zkratka Internet Control Message Protocol - je rozšířený internetový protokol (IP). ICMP podporuje pakety obsahující chybové, kontrolní a informační zprávy. Například příkaz PING používá ICMP pro testování internetového spojení.

Z nabídky **Nastavení ICMP filtru** vyberte povolit/zakázat veškeré ICMP spojení nebo můžete přizpůsobit ICMP filtr a uložit nastavení do souboru pravidel použitím volby **Přidat ICMP filtr do souboru pravidel**.

Vyberte **Povolit pouze tento typ(y) ICMP filtr balíků** a budete schopni nastavit následující volby:

Možnost	Popis
Echo	Tato volba povolí zpětnou žádost o odpověď. Zpětná žádost je ICMP zpráva, která pošle paket dat k hostu a očekává,

Možnost	Popis
	že host pošle zpátky zpětnou odpovědi. Host musí reagovat na všechny zpětné žádosti pomocí zpětné odpovědi obsahující přesná data přijatá ve zpětné žádosti Zpětná odpověď je ICMP zpráva vygenerovaná jako odpověď na ICMP zpětnou žádost, a je povinné pro všechny hostitele a routery.
Cíl je nedostupný	Toto je ICMP zpráva, která je vygenerovaná routerem, aby informovala klienta, že cílový hostitel není dostupný, jestliže paket s adresou není multicastingový. Důvody pro tuto zprávu mohou zahrnout neexistující fyzické spojení s hostitelem (vzdálenost je nekonečná), indikovaný protokol nebo port nejsou aktivní nebo data musí být fragmentovaná, ale je nastaven příznak 'nefragmentovat'.
Přesměrovat	Toto je ICMP zpráva, která informuje hostitele, aby přesměroval své informace (poslat pakety na alternativní router). Jestliže se hostitel pokusí poslat data skrz router(R1), další router (R2) se snaží spojit s hostitelem, nakonec se vytvoří přímé spojení s routerem R2, přesměrování informuje hostitele o vzniku takového spojení. Router bude stále posílat originální paket s adresou příjemce k zamýšlenému cíli. Bohužel jestliže paket s adresou příjemce obsahuje informace o přesměrování, nebude tato zpráva poslána, dokonce i když je k dispozici lepší spojení.
Jiný typ balíku	Pokud je tato volba povolena jakýkoliv jiný paket jiný než **Echo**, **Cíl není k dispozici** nebo **Přesměrovat** projde.
Blokovat veškeré multicast provoz	Pokud je tato volba povolena, veškeré multicastingové zprávy nebudou přijímány.

Jestliže zvolíte použít ICMP nastavení do stávajícího souboru pravidel , pak se na ICMP události objeví reakce (ptát se, povolit nebo zakázat) nastavené v sekci Stav.

Klikněte na **Průvodce pravidel** pro spuštění „*Průvodce nastavením Firewallu*“ (str. 77), pomůže vám vytvořit soubor pravidel Firewallu. Ty jsou potřebné pro vaše běžně používané aplikace. Konečným výsledkem je zabezpečený systém s fungujícím poštovním klientem a internetovým prohlížečem.

Důležité

Jestliže soubor pravidel již existuje, bude nahrazen nově vytvořeným.

Kapitola 9. Modul Antispam

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

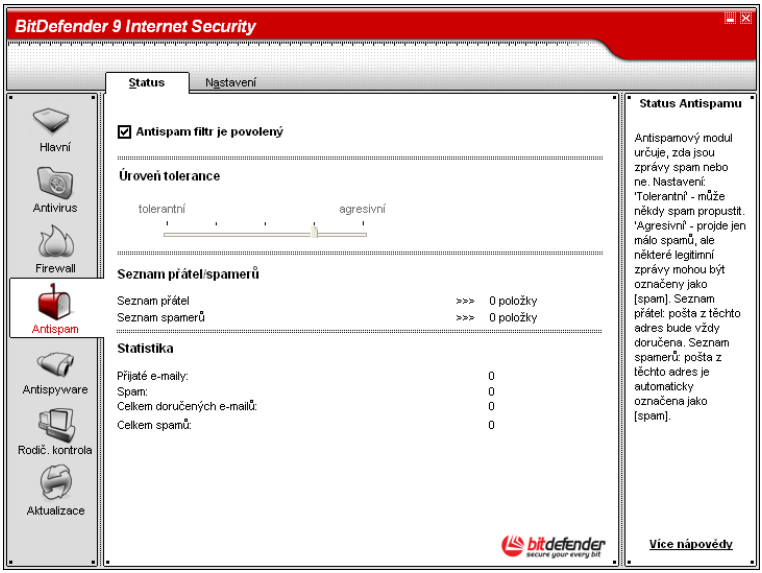
- Status Antispam
- Nastavení antispamu
- Integrace s MS Outlook /Outlook Expres

Poznámka

Pro více detailů týkajících se modulu **Antispam** si prohlédněte popis „*Modul Antispam*“ (str. 20).

9.1. Status Antispam

Pro vstup do této sekce klikněte na **Antispam** a zvolte **Status**.



Obrázek 9.1. Status Antispam

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

V sekci **Statistika** můžete zobrazit statistiky týkající se modulu Antispam. Výsledky jsou presentovány jak za poslední seanci (tj. od posledního spuštění Vašeho počítače) tak i jako přehled a ntispamové aktivity od okamžiku instalace filtru Antispam.

Důležité

Abyste zabránili vstupu spamu do vaší **schránky doručené pošty**, mějte aktivovaný **Antispam filtr**.

Abyste mohli konfigurovat modul **Antispam**, je nezbytné provést následující činnosti:

9.1.1. Nastavení uroveň tolerance

Posouvátkem změňte stupňe tolerance.

- **Tolerantní** - znamená, že filtr nechá některé spamy projít.
- **Agresivní** - znamená, že projde jen velmi málo Spamů, ale současně mohou být některé legitimní zprávy označeny jako spam.

9.1.2. Vyplnění seznamu adres

Seznam adres obsahuje informaci o e-mailových adresách, ze kterých Vám přicházejí legitimní e-mailové zprávy nebo spamy.

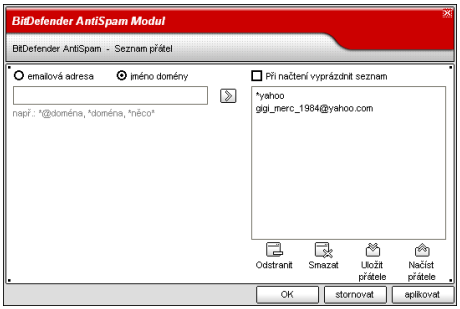
Seznam přátel

Seznam přátel - je seznam e-mailových adres, ze kterých chcete vždy přijímat zprávy, bez ohledu na jejich obsah. Zprávy od přátel nejsou nikdy označeny jako spam, i kdyby svým obsahem spam připomínaly.

Poznámka

Každý e-mail, který přijde z adresy na seznamu přátel bude automaticky doručen do Vašeho **schránky došlé pošty** bez dalších procedur.

Pro správu **Seznamu přátel** klikněte na >>> (u položky **Seznam přátel**), nebo klikněte na tlačítko **Přátel** v *„Antispam lištu nástrojů“* (str. 105).



Obrázek 9.2. Seznam přátel

Můžete zde přidat nebo odebrat údaje ze **Seznamu přátel**.

Chcete-li přidat e-mailovou adresu , zaskrtněte pole **emailová adresa**, napište adresu a klikněte na tlačítko . Daná adresa se posléze objeví v **Seznamu přátel**.

Důležité

Syntaxe: <jméno@doména.com>.

Pokud chcete přidat doménu, zaškrtněte pole **jméno domény**, natypujte jej a klikněte na tlačítko . Doména se objeví na **Seznamu přátel**.

Důležité

Syntaxe:

- <@doména.com>, <*doména.com> a <doména.com> - veškerá pošta přicházející z <doména.com> dorazí do Vaší **schránky došlé pošty** bez ohledu na obsah;
- <*doména*> - veškerá pošta přicházející z <doména> (lhostejno s jakou příponou domény) dorazí do Vaší **schránky došlé pošty** bez ohledu na obsah;
- <*com> - veškerá pošta mající příponu domény <com> dorazí do Vaší **schránky došlé pošty** bez ohledu na obsah;

Pro smazání kterékoliv položky ze seznamu, vyberte ji a klikněte na tlačítko **Odstranit**.

Kliknete-li na tlačítko **Smazat**, smažete všechny položky ze seznamu, ale uvědomte si, že je nemožné je znovu obnovit.

Použijte tlačítka **Uložit přátele**/ **Načíst přátele** pro uložení/načtení **Seznamu přátel** do/z umístění, které si určíte. Soubor bude mít příponu .bwl.

Poznámka

Doporučujeme, abyste přidali jména Vašich přátel a jejich e-mailové adresy do **Seznam přátel**. BitDefender neblokuje zprávy od lidí na seznamu, a proto přidáním přátel pomůžete tomu, aby legitimní zprávy mohly projít.

Klikněte **aplikovat** a **OK** pro uložení a zavření **Seznamu přátel**.

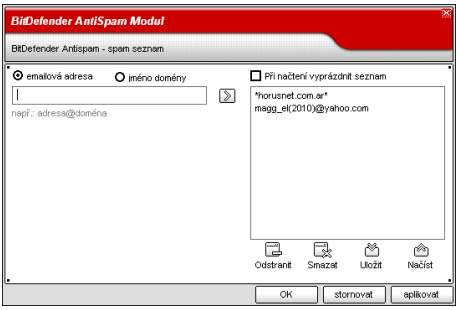
Seznam spamerů

Seznam spamerů - je seznam veškerých e-mailových adres, ze kterých nechcete dostávat žádné zprávy, bez ohledu na jejich obsah.

Poznámka

Každý e-mail, který přijde z adresy na **Seznamu spammerů** bude automaticky označen jako spam, bez dalších procedur.

Pro správu **Seznamu spamerů** klikněte na >>> (u položky **Seznam spamerů**), nebo klikněte na tlačítko **Spamerů** v *„Antispam lištu nástrojů“* (str. 105).



Obrázek 9.3. Seznam spamerů

Můžete zde přidat nebo odebrat údaje ze **Seznamu spamerů**.

Chcete-li přidat e-mailovou adresu , zaskrtněte pole **emailová adresa**, napište adresu a klikněte na tlačítko . Daná adresa se posléze objeví v **Seznamu spamerů**.

Důležité

Syntaxe: <jméno@doména.com>.

Pokud chcete přidat doménu, zaškrtněte pole **jméno domény**, natypujte jej a klikněte na tlačítko . Doména se objeví na **Seznamu spamerů**.

Důležité

Syntaxe:

- <@doména.com>, <*doména.com> a <doména.com> - veškerá pošta z <doména.com> bude označena jako spam;
- <*doména*> - veškerá pošta z <doména> (bez ohledu na příponu domény) bude označena jako spam;
- <*com> - veškerá pošta, která má příponu domény <com> bude označena jako spam.

Abyste odstranili položku ze seznamu, nejprve ji vyberte a pak klikněte na tlačítko **Odstranit**.

Kliknete-li na tlačítko **Smazat**, vymažete ze seznamu všechny položky, ale uvědomte si, že je nemožné je znovu obnovit.

Použijte tlačítka **Uložit spamery**/ **Načíst spamery** pro uložení/načtení **Seznamu spamerů** do umístění, které si určíte. Soubor bude mít příznak .bwl.

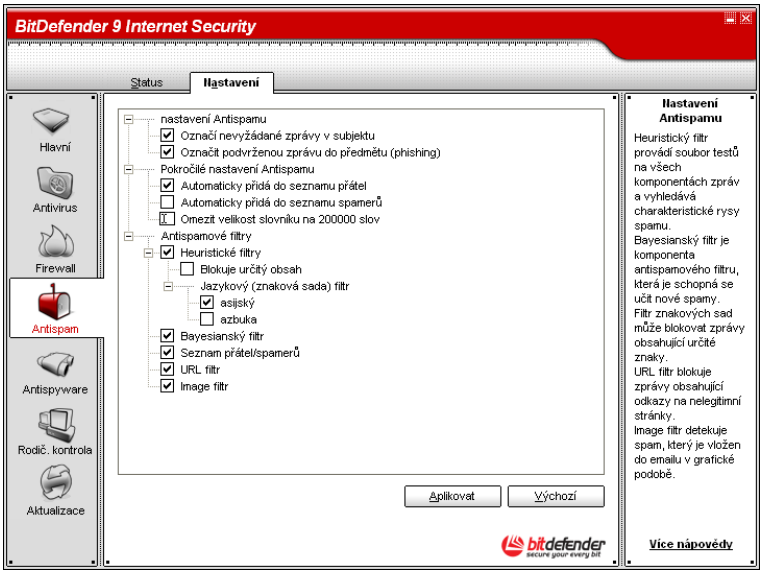
Klikněte **aplikovat** a **OK** pro uložení a zavření **Seznamu spamerů**.

Důležité

Pokud se chystáte přeinstalovat BitDefender, bylo by dobré, abyste si předtím uložili seznamy **přátel** / **spamerů** a po reinstalaci si je můžete znovu načíst.

9.2. Nastavení antispamu

Pro vstup do této sekce klikněte na **Antispam** a zvolte **Nastavení**.



Obrázek 9.4. Nastavení antispamu

Zde můžete zapnout / vypnout jednotlivé antispamové filtry a specifikovat některá další nastavení antispamového modulu.

Dostupné jsou tři kategorie možností (**nastavení Antispamu**, **Pokročilé nastavení Antispamu** a **Antispamové filtry**) organizované jako rozbalovací menu, podobně jako ve Windows.

Poznámka

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

9.2.1. Nastavení antispamu

- **Označí nevyžádané zprávy v subjektu** - všechny e-maily považované za spam budou v předmětu označeny jako SPAM.

- **Označit podvrženou zprávu do předmětu** - všechny e-maily považované za podvržené (pishing) budou v předmětu označeny jako SPAM.

9.2.2. Pokročilé nastavení Antispamu

- **Automaticky přida do seznamu přátel** - pak při příštím kliknutí na tlačítko **To není spam** z *„Antispam lištu nástrojů“* (str. 105) bude odesilatel automaticky přidán do **Seznamu přátel**.
- **Automaticky přida do seznamu spammerů** - pak při příštím kliknutí na tlačítko **To je spam** v *„Antispam lištu nástrojů“* (str. 105) bude odesilatel automaticky přidán do **Seznamu spammerů**.

Poznámka

Tlačítka **To není spam** a **To je spam** jsou využívána pro “výcvik” Bayesiánského filtru.

- **Omezit velikost slovníku na 200000 slov** - nastaví velikost Bayesianksského adresáře - menší je rychlejší, větší je přesnější.

Poznámka

Doporučená velikost je 200000 slov.

9.2.3. Antispamové filtry

- **Heuristické filtr** - aktivuje/deaktivuje Heuristické filtr;
- **Blokuje určitý obsah** - aktuvije / deaktivuje detekci zpráv s explicitním obsahem SEX v předmětu;
- **Jazykový (znaková sada) filtr** - otevře Charset filtr , kde můžete zvolit blokování zpráv napsaných v Cyrilici a / nebo v asijských znacích;
- **Bayesiánský filtr** - aktivuje/deaktivuje Bayesiánský filtr;
- **Seznam přátel/spamerů** - aktivuje/deaktivuje Seznam přátel / spamerů;

- **URL filtr** - aktivuje/deaktivuje URL filtr;
- **Image filtr** - aktivuje/deaktivuje Image(Obrázkový) filtr.

Poznámka

Pro aktivování / deaktivování filtru vyberte / odškrtněte odpovídající checkbox.

Klikněte na **Aplikovat** pro uložení změn. Pokud stisknete **Výchozí**, bude načteno defaultní nastavení.

9.3. Integrace s MS Outlook /Outlook Expres

BitDefender je přímo integrován s MS Outlook / Outlook Expres prostřednictvím intuitivního panelu.

9.3.1. Antispam lištu nástrojů

V horní části Microsoft Outlooku / Outlook Expressu naleznete lištu nástrojů.

Obrázek 9.5. Antispam lišta

Důležité

Hlavní rozdíl mezi BitDefender Antispamem pro Microsoft Outlook a BitDefender Antispamem pro Outlook Express je, že u Microsoft Outlooku jsou spamové zprávy přesunuty do složky **Spam**, a u Outlook Expressu jsou přesunuty do složky **Smazaných položek**. V obou případech jsou zprávy označené jako Spam v řádce předmětu zprávy.

Složka **Spam** vytvořená BitDefenderem pro Microsoft Outlook se nachází na stejné úrovni jako ostatní položky ze **Seznamu složek**(Kalendář, Kontakty, atd.).

Obrázek 9.6. Složka Spam

Každé tlačítko z lišty BitDefenderu bude vysvětleno níže:

- **To je spam** - pošle zprávu do Bayesiánského modulu s označením, že se jedná o spam. E-mail bude označen jako SPAM a přesunut do složky **Spamů**.

  Další zprávy, které budou vykazovat tytéž rysy budou označeny jako SPAM.

  Poznámka

  Můžete vybrat jeden či více e-mailových zpráv.

- **To není spam** - pošle zprávu do Bayesiánského modulu s označením, že se nejedná o spam a BitDefender by ji neměl označovat. E-mail bude přesunut ze složky **Spamů** do adresáře **došlé pošty**.

  Další zprávy, které budou vykazovat tytéž rysy nebudou již nikdy označovány jako SPAM.

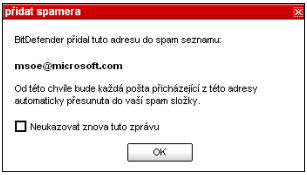
  Poznámka

  Můžete vybrat jeden či více e-mailových zpráv.

  Důležité

  Tlačítko **To není spam** se zaktivuje, jakmile vyberete zprávu označenou BitDefenderem jako SPAM (obvykle jsou tyto zprávy umístěny ve složce **Spam**).

- **Přidat spamera** - přidá odesílatele vybrané zprávy do **Seznamu spamerů**.



Zaškrtněte **Neukazovat znova tuto zprávu** pokud nechcete být pokaždé vyzváni k potvrzení, poté co přidáte adresu spamera do seznamu.

Klikněte **OK** pro uzavření tohoto okna.

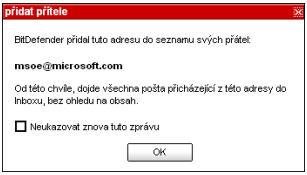
Obrázek 9.7. Přidat spamera

Budoucí e-mailové zprávy z této adresy budou označeny jako SPAM.

Poznámka

Můžete vybrat jednoho či více odesilatelů.

- **Přidat přátele** - přidá odesílatele vybrané zprávy do **Seznamu přátel**.



Zaškrtněte **Neukazovat znova tuto zprávu** pokud nechcete být pokaždé vyzváni k potvrzení, poté co přidáte adresu přítele do seznamu.

Klikněte **OK** pro uzavření tohoto okna.

Obrázek 9.8. Přidat přátele

E-mailové zprávy z těchto adres obdržíte vždy, bez ohledu na jejich obsah.

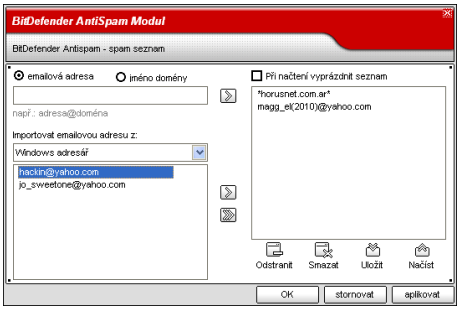
Poznámka

Můžete vybrat jednoho či více odesilatelů.

- **Spameři** - otevře **Seznam spamerů** , který obsahuje e-mailové adresy, odkud nechcete dostávat zprávy, bez ohledu na jejich obsah.

Poznámka

Každý e-mail, který přijde z adresy na **seznamu spammerů** bude automaticky označen jako spam, bez dalších procedur.



Obrázek 9.9. Seznam spamerů

Můžete zde přidat nebo odebrat údaje ze **Seznamu spamerů**. Chcete-li přidat e-mailovou adresu , zaskrtněte pole **emailová adresa**, napište adresu a klikněte na tlačítko . Daná adresa se posléze objeví v **Seznamu spamerů**.

Důležité

Syntaxe: <jméno@doména.com>.

Pokud chcete přidat doménu, zaškrtněte pole **jméno domény**, natypujte jej a klikněte na tlačítko . Doména se objeví na **Seznamu spamerů**.

Důležité

Syntax:

- <@doména.com>, <*doména.com> a <doména.com> - veškerá pošta z <doména.com> bude označena jako spam;
- <*doména*> - veškerá pošta z <doména> (bez ohledu na příponu domény) bude označena jako spam;
- <*com> - veškerá pošta, která má příponu domény <com> bude označena jako spam.

Z menu **Importovat e-mailové adresy z** zvolte **Adresář Windows/Outlook Express složka** a naimportujte tam adresy z **MS Outlook/Outlook Express**.

Pro **MS Outlook Express** se zobrazí nové okno, kde můžete zvolit složku, která obsahuje e-mailové adresy, které chcete přidat do **Seznamu spamerů**. Vyberte je a zvolte **Vybrat**.

V obou případech se e-mailové adresy objeví na seznamu importu. Adresy vyberte a klikněte na tlačítko pro přidání do **Seznamu spamerů**. Kliknete-li na tlačítko , budou do seznamu přidány všechny e-mailové adresy.

Abyste odstranili položku ze seznamu, nejprve ji vyberte a pak klikněte na tlačítko **Odstranit**.

Kliknete-li na tlačítko **Smazat**, vymažete ze seznamu všechny položky, ale uvědomte si, že je nemožné je znovu obnovit.

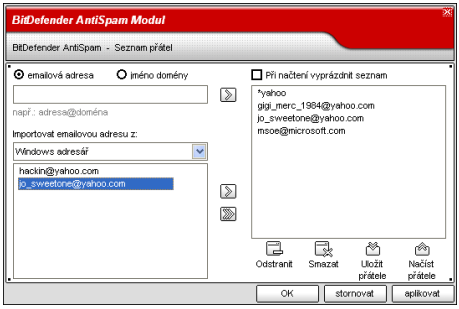
Použijte tlačítka **Uložit spamery**/ **Načíst spamery** pro uložení/načtení **Seznamu spamerů** do umístění, které si určíte. Soubor bude mít příznak `.bwl`.

Klikněte **aplikovat** a **OK** pro uložení a zavření **Seznamu spamerů**.

- **Přátelé** - otevře **Seznam přátel**, který obsahuje e-mailové adresy, ze kterých Vám bude pošta doručována bez ohledu na její obsah.

Poznámka

Každý e-mail, který přijde z adresy na **Seznamu přátel** bude automaticky doručen do Vašeho Inboxu, bez dalších procedur.



Obrázek 9.10. Seznam přátel

Můžete zde přidat nebo odebrat údaje ze **Seznamu přátel**. Chcete-li přidat e-mailovou adresu , zaskrtněte pole **emailová adresa**, napište adresu a klikněte na tlačítko . Daná adresa se posléze objeví v **Seznamu přátel**.

Důležité

Syntaxe: <jméno@doména.com>.

Pokud chcete přidat doménu, zaškrtněte pole **jméno domény**, natypujte jej a klikněte na tlačítko . Doména se objeví na **Seznamu přátel**.

Důležité

Syntaxe:

- <@doména.com>, <*doména.com> a <doména.com> - veškerá pošta přicházející z <doména.com> dorazí do Vaší **schránky došlé pošty** bez ohledu na obsah;
- <*doména*> - veškerá pošta přicházející z <doména> (lhostejno s jakou příponou domény) dorazí do Vaší **schránky došlé pošty** bez ohledu na obsah;
- <*com> - veškerá pošta mající příponu domény <com> dorazí do Vaší **schránky došlé pošty** bez ohledu na obsah;

Z menu **Importovat e-mailové adresy z** zvolte **Adresář Windows/Outlook Express složka** a naimportujte tam adresy z **MS Outlook/Outlook Express**.

Pro **MS Outlook Express** se zobrazí nové okno, kde můžete zvolit složku, která obsahuje e-mailové adresy, které chcete přidat do **Seznamu přátel**. Vyberte je a zvolte **Vybrat**.

V obou případech se e-mailové adresy objeví na seznamu importu. Adresy vyberte a klikněte na tlačítko pro přidání do **Seznamu přátel**. Kliknete-li na tlačítko , budou do seznamu přidány všechny e-mailové adresy.

Pro smazání kterékoliv položky ze seznamu, vyberte ji a klikněte na tlačítko **Odstranit**.

Kliknete-li na tlačítko **Smazat**, smažete všechny položky ze seznamu, ale uvědomte si, že je nemožné je znovu obnovit.

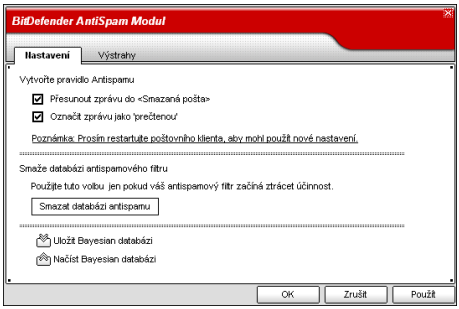
Použijte tlačítka **Uložit přátele**/ **Načíst přátele** pro uložení/načtení **Seznamu přátel** do/z umístění, které si určíte. Soubor bude mít příponu .bwl.

Poznámka

Doporučujeme, abyste přidali jména Vašich přátel a jejich e-mailové adresy do **Seznam přátel**. BitDefender neblokuje zprávy od lidí na seznamu, a proto přidáním přátel pomůžete tomu, aby legitimní zprávy mohly projít.

Klikněte **aplikovat** a **OK** pro uložení a zavření **Seznamu přátel**.

- **Nastavení** - otevře okno **Nastavení**, kde můžete specifikovat možnosti **Antispamového** modulu.



Obrázek 9.11. Nastavení

Dostupné jsou následující možnosti:

- **Přesunout zprávu do Smazaná pošta** - přesunout spamové zprávy do **Smazaná pošta** (pouze v Microsoft Outlook Expressu);
- **Označit zprávu jako 'prečtenou'** - označit všechny spamové zprávy jako přečtené, tak aby Vás nové spamové zprávy, které přijdou, nerušily.

Je-li Váš filtr velmi nepřesný, budete možná potřebovat “přemazat” databázi filtru a znovu “vycvičit” Bayesiánský filtr. Klikněte na **Smazat databázi antispamu** pokud chcete resetovat Bayesiánskou databázi.

Použijte **Uložit Bayesian databázi**/ **Načíst Bayesian databázi** tlačítka pro uložení / načtení Bayesianské databáze na požadované umístění. Soubor má `.dat` příponu.

Klikněte na záložku **Výstrahy** pokud chcete vstoupit do sekce, kde můžete zakázat zobrazování potvrzovacích oken u tlačítek **Přidat spamera** a **Přidat přítele**.

- **Průvodce** - otevře průvodce, který Vás bude provázet celým procesem tréninku Bayesiánského filtru, díky čemuž se ještě zvýší efektivita BitDefender Antispamu. Rovněž můžete přidat adresy z Vašeho **Adresáře** do **Seznamů přátel** / **spamerů**.
- **BitDefender Antispam** - otevře řídící konzole.

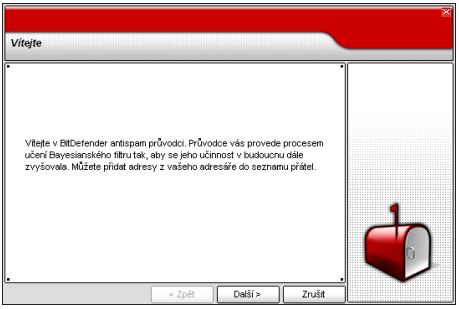
9.3.2. Průvodce konfigurací

Když poprvé spustíte MS Outloo / Outlook Expres po instalaci BitDefenderu, zobrazí se Průvodce, který Vám pomůže nastavit Seznam přátel, Seznam spamerů a vyzkoušet Bayesianský filtr, abyste mohli neustále zvyšovat efektivitu antispamových filtrů.

Poznámka

Průvodce může být kdykoli spuštěn poklikáním na tlačítko **Průvodce** v *„Antispam lištu nástrojů“* (str. 105).

Krok 1/6 - Uvítací okno



Obrázek 9.12. Uvítací okno

Klikněte **Další**.

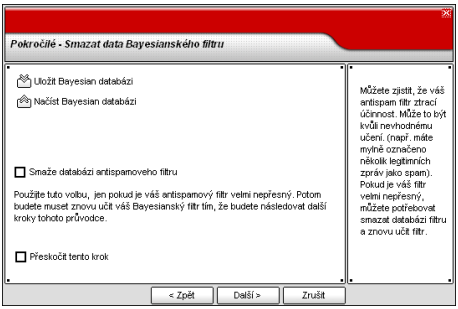
Krok 2/6 - Přidat z adresáře

Obrázek 9.13. Přidat z adresáře

Zde můžete vidět veškeré adresy z Vašeho **Adresáře**. Vyberte ty, které chcete přidat do Vašeho **seznamu přátel** (doporučujeme vybrat všechny). Z těchto adres budete dostávat všechny e-mailové zprávy, bez ohledu na jejich obsah.

Zvolte možnost **Přeskočit tento krok** pokud chcete vynechat tento krok. Kliknout **Zpět** pro návrat do předchozího kroku nebo kliknout **Další** pro pokračování.

Krok 3/6 - Smazat data Bayesiánského filtru



Obrázek 9.14. Smazat data Bayesiánského filtru

Možná zjistíte, že Antispam filtr přestává být dostatečně efektivní. Příčinou může být nesprávný trénink (tzn. , že jste chybně označili řadu legitimních zpráv jako spam, a

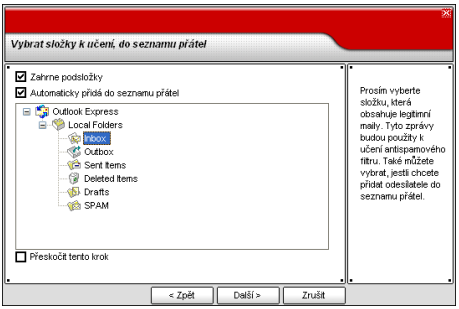
naopak). Je-li Váš filtr velmi nepřesný, budete možná potřebovat “přemazat” databázi filtru a znovu “vycvičit” filtr. Postupovat společně s průvodcem můžete v těchto krocích.

Zvolit možnost **Smaže databázi antispamového filtru** tedy resetovat Bayesiánskou databázi.

Použijte **Uložit Bayesian databázi**/ **Načíst Bayesian databázi** tlačítka pro uložení / načtení Bayesianské databáze na požadované umístění. Soubor má `.dat` příponu.

Zvolte možnost **Přeskočit tento krok** pokud chcete vynechat tento krok. Kliknout **Zpět** pro návrat do předchozího kroku nebo kliknout **Další** pro pokračování.

Krok 4/6 - Trénink Bayesiánského filtru pomocí legitimních e-mailových zpráv



Obrázek 9.15. Trénink Bayesiánského filtru pomocí legitimních e-mailových zpráv

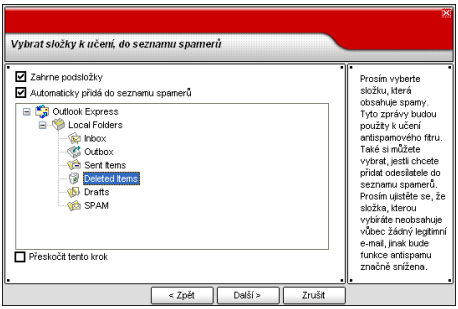
Vyberte složku, která obsahuje legitimní e-mailové zprávy. Tyto zprávy budou použity pro výcvik antispamového filtru.

V horní části okna jsou nabídnuty 2 možnosti:

- **Zahrne podsložky** - do výběru zahrnout i podsložky;
- **Automaticky přida do seznamu přátel** - přidat odesilatele do **seznamu přátel**.

Zvolte možnost **Přeskočit tento krok** pokud chcete vynechat tento krok. Kliknout **Zpět** pro návrat do předchozího kroku nebo kliknout **Další** pro pokračování.

Krok 5/6 - Trénink Bayesiánského fitru pomocí SPAMových zpráv



Obrázek 9.16. Trénink Bayesiánského fitru pomocí SPAMových zpráv

Vyberte složku, která obsahuje spamové e-mailové zprávy. Tyto zprávy budou použity pro výcvik antispamového filtru.

Důležité

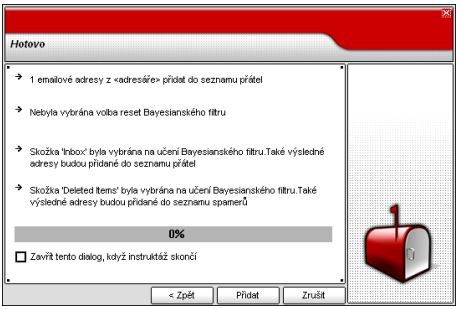
Ujistěte se, že složka, kterou vyberete, neobsahuje žádné legitimní e-maily, jinak by byl výkon Antispamu značně redukovaný.

V horní části okna jsou nabídnuty 2 možnosti:

- **Zahrne podsložek** - výběru zahrnout i podsložky;
- **Automaticky přida do seznamu spamerů** - přidat odesilatele do **seznamu spamerů**.

Zvolte možnost **Přeskočit tento krok** pokud chcete vynechat tento krok. Kliknout **Zpět** pro návrat do předchozího kroku nebo kliknout **Další** pro pokračování.

Krok 6/6 - Hotovo



Obrázek 9.17. Hotovo

V tomto okně můžete zobrazit všechna nastavení průvodce konfigurací a můžete provést některé změny tak, že se vrátíte na předchozí kroky kliknutím na **Zpět**).

Pokud již nechcete provádět žádné modifikace, klikněte **Přidat**.

Kapitola 10. Modul Antispyware

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

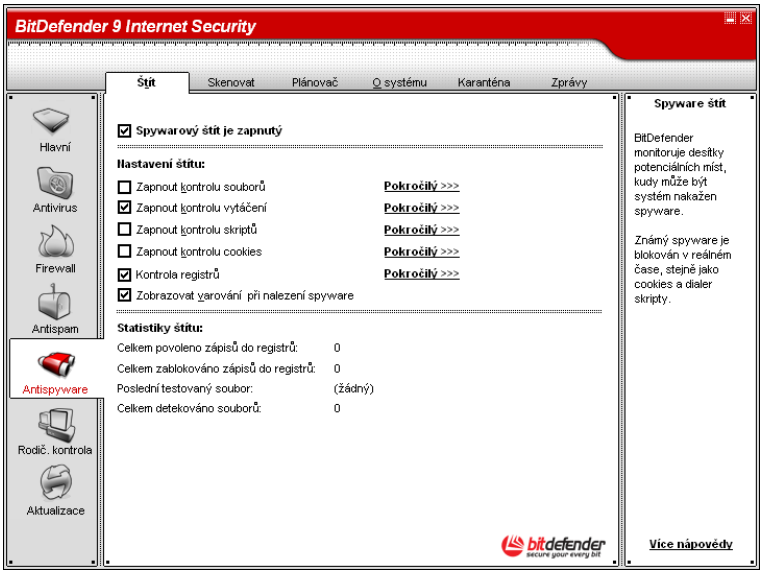
- Spyware štít
- Testování na žádost
- Plánované testování
- Systémová informace
- Karanténa
- Záznamy

Poznámka

Pro více detailů týkajících se modulu **Antispyware** si prohlédněte „*Modul Antispyware*“ (str. 24).

10.1. Spyware štít

Pro zpřístupnění této sekce klikněte na záložku **Štít** v modulu **Antispyware**.



Obrázek 10.1. Spyware štít

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 zablokované ihned.

V této části můžete nastavit **Spyware štít** a můžete prohlížet informace o jeho aktivitách.

Poznámka

Abyste ochránili svůj počítač před Spywarem, musíte mít zapnutý **Spyware štít**.

Ve spodní části této sekce můžete vidět statistiky **Spyware štítu**.

Vyberte **Zobrazovat varování při nalezení spyware**, pokud chcete být upozorněni v případě nálezu Spywaru. Varování o nakaženém souboru obsahuje jméno Spywaru, cestu k němu, akci podniknutou BitDefenderem a odkaz na stránky BitDefenderu, kde můžete najít více informací o daném Spywaru.

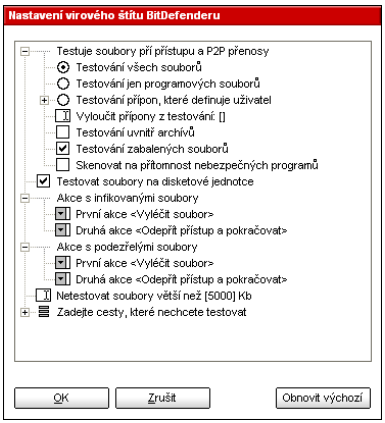
V případě, že je nalezen podezřelý soubor, můžete spustit z varovného okna průvodce, který vám pomůže poslat daný soubor laboratořím BitDefenderu pro podrobnou analýzu. Můžete připsat vaši e-mailovou adresu, abyste obdrželi informace o této analýze.

Spyware štít chrání váš počítač proti Spywaru pomocí 5 důležitých ochranných kontrol:

- Kontrola souborů
- Kontrola vytáčení
- Kontrola scriptů
- Kontrola cookies
- Kontrola registrů

10.1.1. Kontrola souborů

Klikněte na **Pokročilé >>>** zvolte **Kontrola souborů** a nastavte požadovanou kontrolu.



Obrázek 10.2. Kontrola souborů

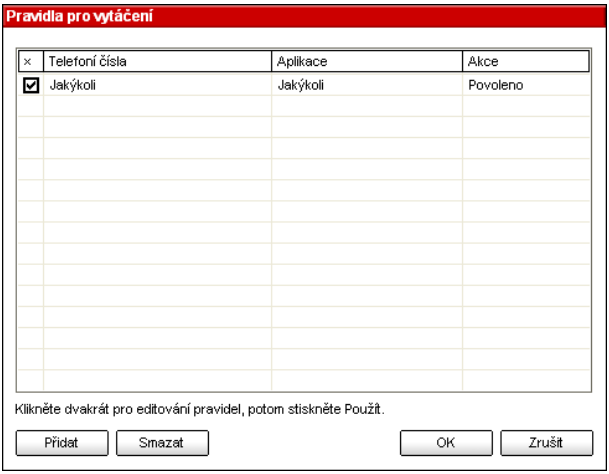
Kontrola souborů je stejná pro **Antivirový** a **Antispywarový** modul a je dostupná z obou modulů.

Poznámka

Podívejte se do sekce „ *Další možnosti nastavení* “ (str. 47) pro detailnější popis tohoto tématu.

10.1.2. Kontrola vytáčení

Klikněte na **Pokročilé >>>** zvolte **Kontrola vytáčení** a nastavte požadovanou kontrolu.



Obrázek 10.3. 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:

Obrázek 10.4. Výstraha vytáčení

Zde vidíte názvy aplikací a telefonní čísla.

Zaškrtněte volbu **Zapamatovat si tuto odpověď**, pak klikněte **Ano** nebo **Ne** a pravidlo bude vytvořeno, aplikováno a zobrazeno v tabulce pravidel. Kdykoliv se proces v budoucnu zopakuje, 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 zeshora, první pravidlo má nejvyšší prioritu. Pravidlo můžete chytit a přesunout a tím změnit jeho prioritu.

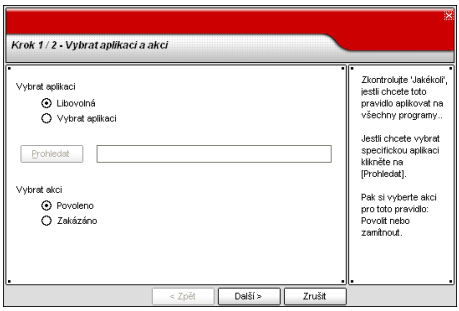
Pro smazání pravidla, je potřeba jej nejprve vybrat a poté kliknout **Smazat pravidlo**. Pro modifikaci atributů pravidla na ně klikněte dvakrát. Pro dočasnou deaktivaci pravidla bez jeho smazání odškrtněte odpovídající checkbox.

Pravidla mohou být iniciována automaticky (prostřednictvím upozorňovacího okna) nebo ručně (klikněte **Nové pravidlo** a zvolte parametry pravidla). Průvodce konfigurací zobrazí první krok.

Průvodce nastavením

Průvodce nastavení má 2 kroky.

Krok 1/2 - Vybrat aplikaci a akci



Obrázek 10.5. Vybrat aplikaci a akci

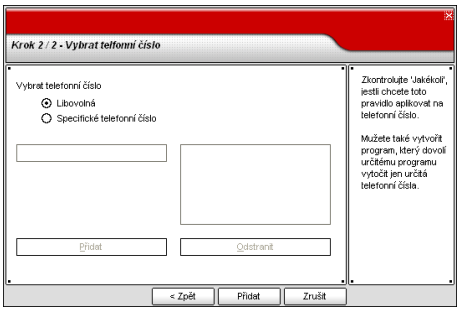
Můžete nastavit parametry:

- **Aplikace** - vyberte aplikaci. Můžete vybrat buďto jen jednu aplikaci (klikněte **Vybrat aplikaci**, potom **Prohledat** a vyberte aplikaci), nebo všechny aplikace (klikněte **Libovolná**).
- **Akce** - zvolte akci.

Akce	Popis
Povoleno	Akce bude povolena.
Zakázáno	Akce bude zakázána.

Klikněte **Další**.

Krok 2/2 - Vybrat telefonní čísla



Obrázek 10.6. Vybrat telefonní čísla

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

Poznámka

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

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

Poznámka

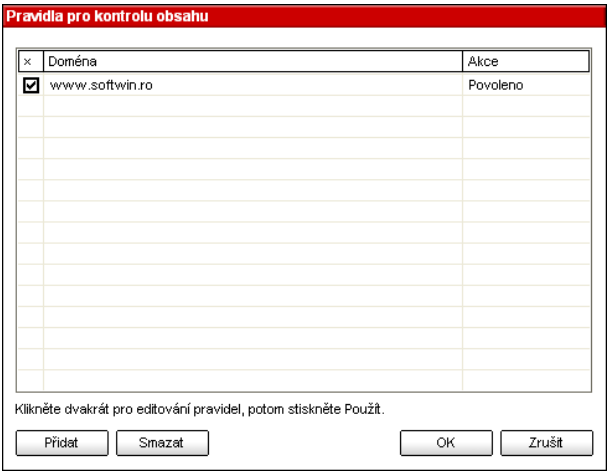
Můžete rovněž vytvořit pravidlo, které povolí určitému programu vytáčet jen určitá čísla (např. číslo vašeho internetového servisního providera nebo fax news servis).

Klikněte **Přidat**.

Klikněte **Aplikovat** pro uložení změn.

10.1.3. Kontrola skriptu

Klikněte na **Pokročilé >>>** zvolte **Kontrola skriptu** a nastavte požadovanou kontrolu.



Obrázek 10.7. Kontrola skriptu

Scripty a ostatní kódy jako jsou Kontrola ActiveX 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 script nebo jiný aktivní obsah:

Obrázek 10.8. Výstraha skriptu

Zde vidíte název zdroje.

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

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

Důležité

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

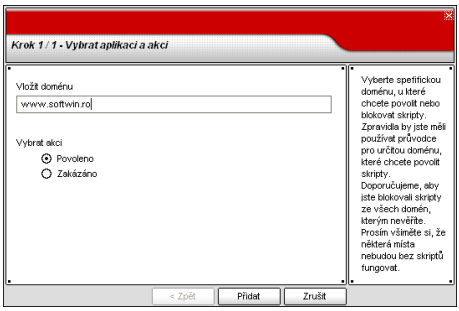
Pro smazání pravidla, je potřeba jej nejprve vybrat a poté kliknout **Smazat pravidlo**. Pro modifikaci atributů pravidla na ně klikněte dvakrát. Pro dočasnou deaktivaci pravidla bez jeho smazání odškrtněte odpovídající checkbox.

Pravidla mohou být iniciována automaticky (prostřednictvím upozorňovacího okna) nebo ručně (klikněte **Nové pravidlo** a zvolte parametry pravidla). Průvodce konfigurací zobrazí první krok.

Průvodce nastavením

Průvodce nastavením má 1 krok.

Krok 1/1 - Vybrat aplikaci a akci



Obrázek 10.9. Vybrat aplikaci a akci

Zde můžete nastavit parametry:

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

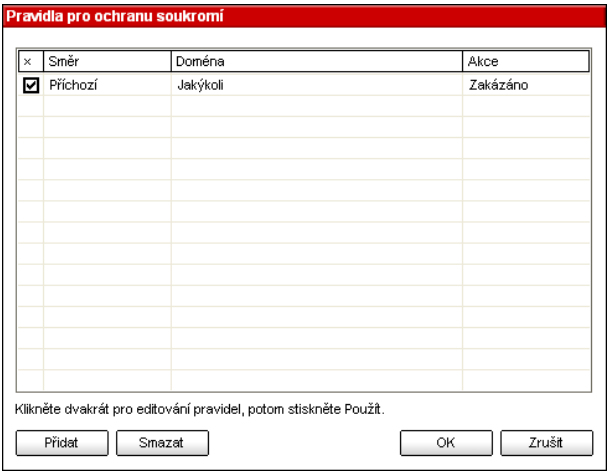
Akce	Popis
Povoleno	Skript na doméně se spustí.
Zakázáno	Skript na doméně se nespustí.

Klikněte **Přidat**.

Klikněte **Aplikovat** pro uložení změn.

10.1.4. Kontrola cookie

Klikněte na **Pokročilé >>>** zvolte **Kontrola cookie** a nastavte požadovanou kontrolu.



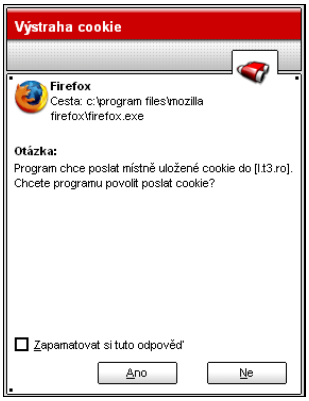
Obrázek 10.10. Kontrola cookie

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 je stopovány Vaše surfovací šablony.

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



Obrázek 10.11. Výstraha cookies

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

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

Tohle Vám pomůže rozhodnout, kterým webovým stránkám věřit a kterým nikoliv.

Poznámka

Z důvodu obrovského množství cookies používaných v dnešní době na internetu je zahájení procesu **Kontroly cookie** 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 zeshora, první pravidlo má nejvyšší prioritu. Pravidlo můžete chytit a přesunout a tím změnit jeho prioritu.

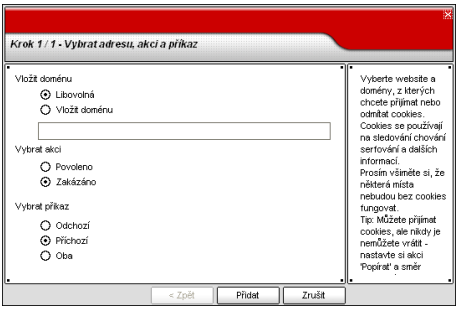
Pro smazání pravidla, je potřeba jej nejprve vybrat a poté kliknout **Smazat pravidlo**. Pro modifikaci atributů pravidla na ně klikněte dvakrát. Pro dočasnou deaktivaci pravidla bez jeho smazání odškrtněte odpovídající checkbox.

Pravidla mohou být iniciována automaticky (prostřednictvím upozorňovacího okna) nebo ručně (klikněte **Nové pravidlo** a zvolte parametry pravidla). Průvodce konfigurací zobrazí první krok.

Průvodce nastavením

Průvodce nastavením má 1 krok.

Krok 1/1 - Vybrat adresu, akci a příkaz



Obrázek 10.12. Vybrat adresu, akci a příkaz

Zde můžete nastavit parametry:

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

Akce	Popis
Povoleno	Cookies z této domény budou provedeny.
Zakázáno	Cookies z této domény nebudou provedeny.

- **Příkaz** - vyberte směr provozu.

Směr	Popis
Odchozí	Pravidlo bude aplikováno pouze pro cookies, které jsou odeslány zpět na připojenou stránku.

Směr	Popis
Příchozí	Pravidlo bude aplikováno, pouze pro cookies, které jsou získané z připojené stránky.
Oba	Pravidlo bude aplikováno na oba případy.

Klikněte **Přidat**.

Poznámka

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

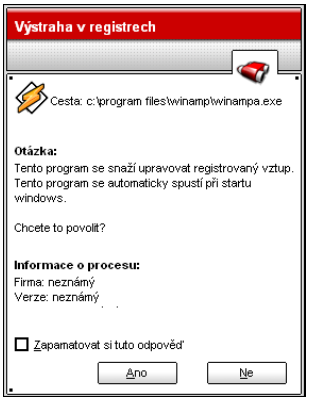
Klikněte **Aplikovat** pro uložení změn.

10.1.5. Kontrola registru

Velmi důležitou částí operačního systém Windows je **Registr**. Je to místo, kde Windows uchovává 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.



Obrázek 10.13. Výstraha v registrech

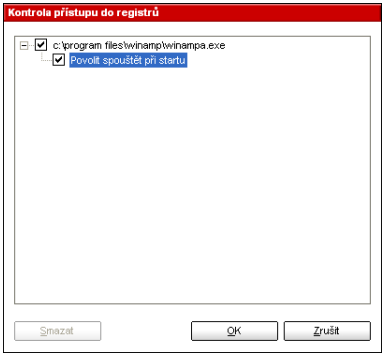
Tuto modifikaci můžete zamítnout kliknutím **Ne** nebo povolit kliknutím **Ano**.

Chcete-li, aby si BitDefender zapamatoval Vaši odpověď, zaškrtněte: **Pamatovat si odpověď'**.

Poznámka

Vaše odpovědi se stanou součástí seznamu pravidel.

Chcete-li vidět seznam vstupů do registru, klikněte **Pokročilé >>>** pro **Kontrolu Registru**.



Obrázek 10.14. Kontrola přístupu do registrů

Pro každou aplikaci bude vytvořeno malé zvětšitelné menu, v němž jsou obsaženy veškeré modifikace registru.

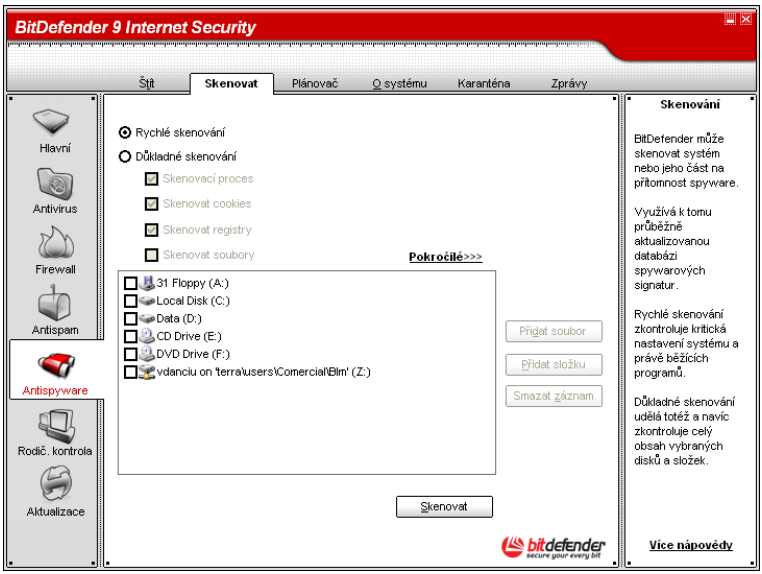
Pro smazání položky v registru, nejprve tuto položku vyberte a pak klikněte **Smazat**. Pro dočasné deaktivování zápisu do registru bez mazání odškrtněte odpovídající checkbox.

Poznámka

BitDefender Vás při instalaci nových programů obvykle upozorní, že je potřeba jej spustit při příštím startu Vašeho počítače.

10.2. Testování na žádost

Pro zpřístupnění této sekce klikněte na záložku **Skenovat** v modulu **Antispyware**.



Obrázek 10.15. Testování

Tato část je podobná té z modulu **Antivirus** s jediným rozdílem a to, že si můžete vybrat ze 2 typů testů:

- **Rychlé skenování** - jestliže vyberete tuto možnost, budou testovány pouze registry, cookies, procesy a některé specifické soubory;
- **Důkladné skenování** - jestliže vyberete tuto možnost, budete mít možnost otestovat váš počítač proti Spywaru a virům.

  Pro Antispywarový test máte 3 možnosti:
  - **Skenovací proces** - testuje všechny procesy v paměti proti výskytu Spyware;
  - **Skenovat cookies** - testuje všechny soubory cookies proti výskytu Spyware;
  - **Skenovat registrů** - testuje všechny záznamy v registrech proti výskytu Spyware.

Pro testování vašeho počítače proti virům musíte nejprve vybrat možnost **Skenovat soubory**, pak vybere testovanou oblast a klikněte na **Skenovat**.

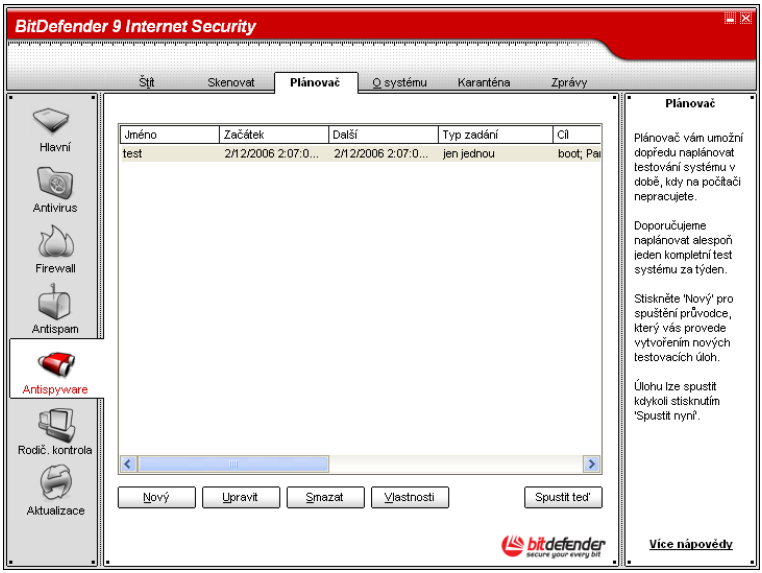
Poznámka

Pokročilí uživatelé mohou využít výhod nastavení testů, které BitDefender nabízí. Testovací rozhraní může být nastaveno, aby přeskakovalo přípony souborů, adresáře nebo archivy, o kterých víte, že jsou neškodné. Toto může rapidně snížit čas testu a zlepšit reakce počítače v jeho průběhu. Klikněte na **Pokročilé nastavení** odpovídající tlačítku **Skenovat soubory** pro zobrazení takovýchto nastavení.

Kontrolujte sekci „ *Krok 4/5 - Vyberte možnosti skenování* “ (str. 53) pro úplný popis.

10.3. Plánované testování

Pro zpřístupnění této sekce klikněte na záložku **Plánovač** v modulu **Antispyware**.



Obrázek 10.16. Plánovač

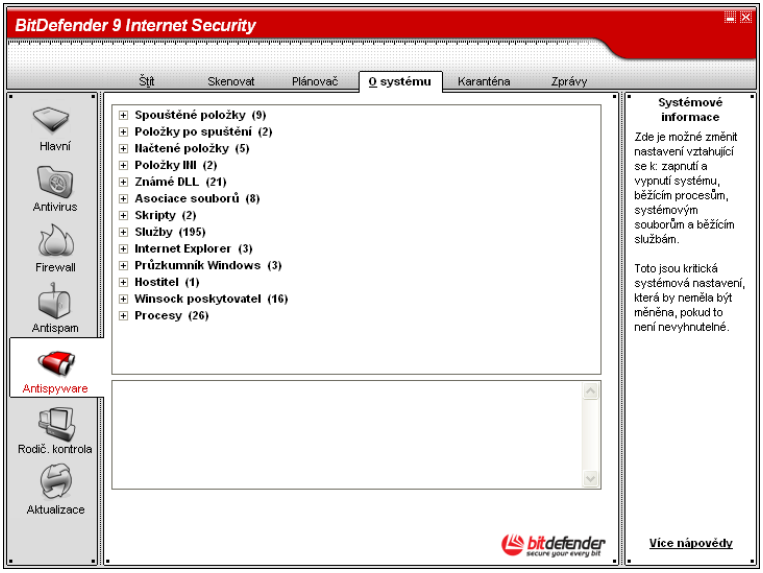
Sekce **Plánovač** je společná pro modul **Antivirus** a **Antispyware** a může být zpřístupněna z obou modulů kliknutím na záložku **Plánovač**.

Poznámka

Podívejte se do sekce *„Plánování skenování“* (str. 60) pro detailnější popis tohoto tématu.

10.4. Systémové informace

Pro zpřístupnění této sekce klikněte na záložku **O systému** v modulu **Antispyware**.



Obrázek 10.17. Systémové informace

Zde můžete vidět a měnit nastavení o informacích.

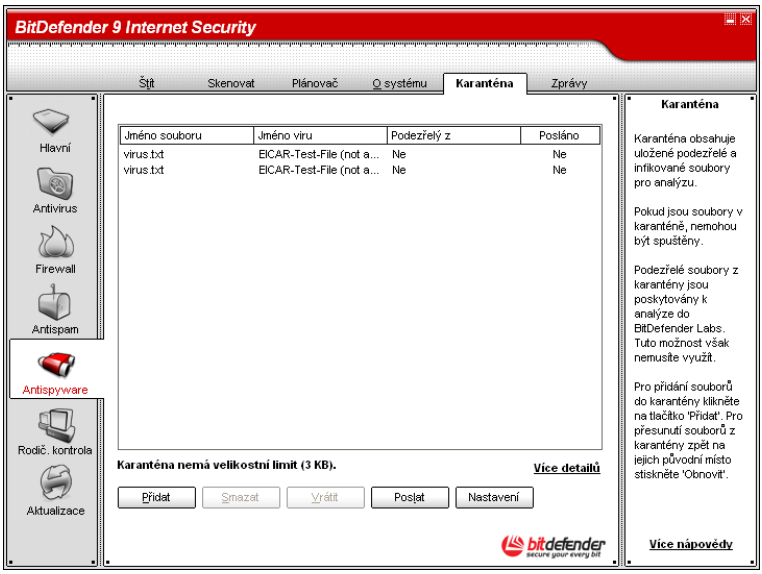
Seznam obsahuje všechny položky nahrané při startu systému právě tak jako položky nahrané různými aplikacemi.

Tři tlačítka jsou k dispozici:

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

10.5. Karanténa

Pro zpřístupnění této sekce klikněte na záložku **Karanténa** v modulu **Antispyware**.



Obrázek 10.18. Karanténa

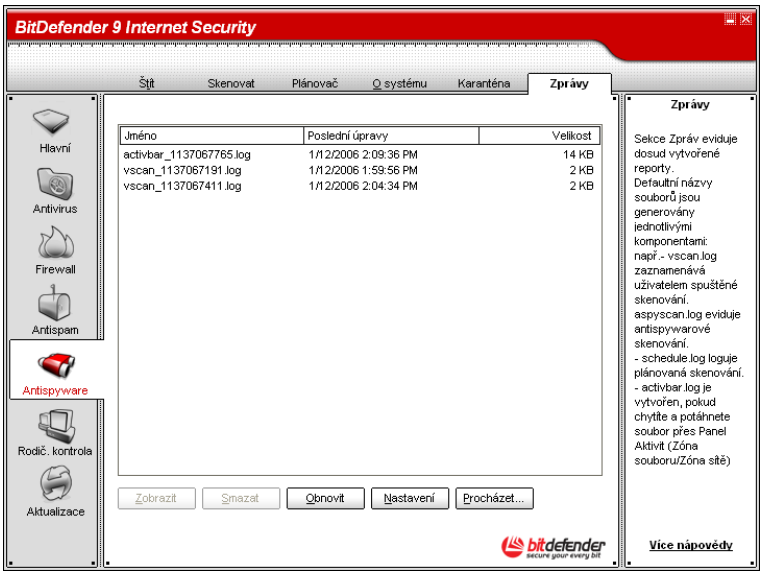
Sekce **Karanténa** je společná pro oba moduly **Antivirus** a **Antispyware** a může být zpřístupněná z obou modulů kliknutím na záložku **Karanténa**.

Poznámka

Prohlédněte si sekci *„Karanténa“* (str. 70) pro detailní popis tohoto tématu.

10.6. Zprávy

Pro zpřístupnění této sekce klikněte na záložku **Zprávy** v modulu **Antispyware**.



Obrázek 10.19. Zprávy

Sekce **Zprávy** je společná pro oba moduly **Antivirus** a **Antispyware** a může být zpřístupněna z obou modulů kliknutím na záložku **Zprávy**.

Poznámka

Prohlédněte si sekci *„Zprávy“* (str. 73) pro detailní popis tohoto tématu.

Kapitola 11. Modul Rodičovský kontrola

Sekce **Rodičovský kontrola** této uživatelské příručky obsahuje následující témata:

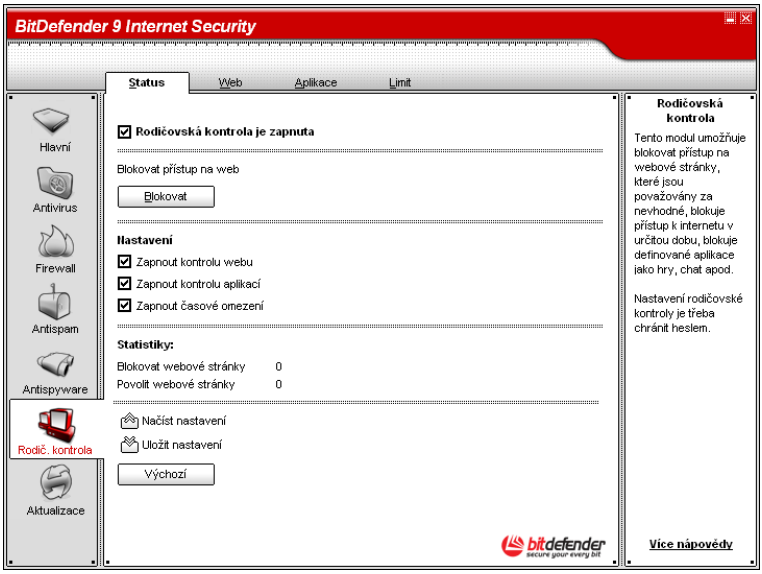
- Status rodičovského kontrolu
- Kontrola webových stránek
- Kontrola aplikací
- Omezovač pobytu na webových stránkách

Poznámka

Pro podrobnější informace týkajících se **Rodičovského kontrolu** se podívejte na popis „*Modul Rodičovký kontrola*“ (str. 25).

11.1. Status rodičovského zámku

Pro zpřístupnění této sekce klikněte na záložku **Status** v modulu **Rodičovský zámek** module.



Obrázek 11.1. Status rodičovského zámku

V této části můžete povolit / zakázat libovolnou ochranu nabízenou **Rodičovským zámkem** (Kontrola web, Kontrola aplikací a časove omezení). Ochrana je povolena, když je zaškrtnuté odpovídající políčko.

Zaškrtněte políčko **Rodičovský kontrola** za účelem povolení/zakázaní ochrany **Rodičovským zámkem**.

Kliknutím na **Blokovat** zakážete přístup ke všem webovým stránkám (ne jen těm ze sekce Kontrola web).

Poznámka

Pokud nejste jedinou osobou používající tento počítač, doporučujeme chránit nastavení vašeho BitDefenderu heslem. Pro nastavení hesla klikněte na **Hlavní** modul, Nastavení a zvolte **Použít ochranu heslem**.

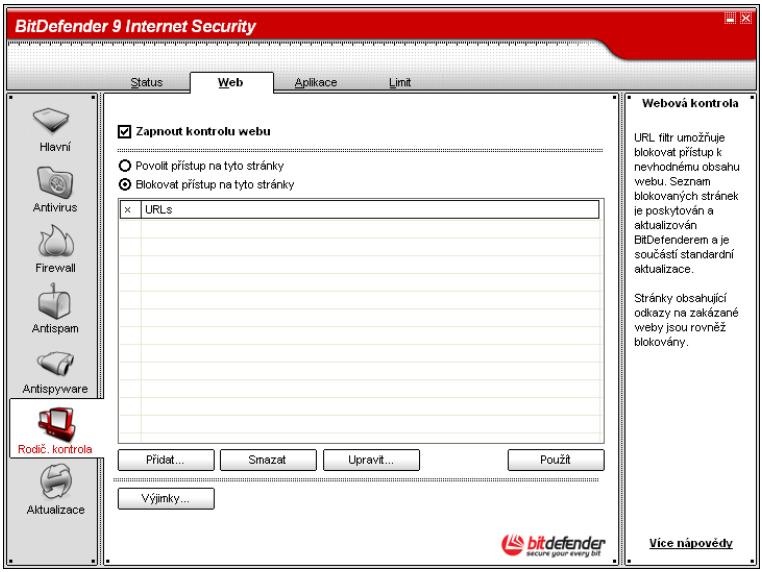
Použijte tlačítka **Uložit nastavení** / **Načíst nastavení** pro uložení / načtení nastavení modulu **Rodičovský zámek**. Takto můžete použít stejná nastavení poté, co znovu nainstalujete nebo opravíte váš produkt BitDefender.

V dolní části této sekce můžete vidět počet povolených nebo zablokovaných webových stránek.

Jestliže stiskněte tlačítko **Obnovit výchozí**, načte se standardní nastavení.

11.2. Kontrola Web

Pro zpřístupnění této sekce klikněte na záložku **Web** v modulu **Rodičovský kontrola** module.



Obrázek 11.2. Kontrola Web

Kontrola Web vám pomáhá zablokovat přístup k webovým stránkám s nevhodným obsahem. Seznam kandidátů pro zablokování jak stránek, tak jejich částí bude poskytnutý a dodaný od BitDefenderu jako součást standardního aktualizačního procesu. Stránky obsahující odkazy na zakázané webové stránky mohou být podle přání také zablokovány.

Pro povolení této ochrany zaškrtněte políčko **Zapnout kontrolu webu**.

Pravidla musí být zadána ručně vybráním akce a přidáním stránky (kliknutím na **Přidat**).

11.2.1. Průvodce nastavením

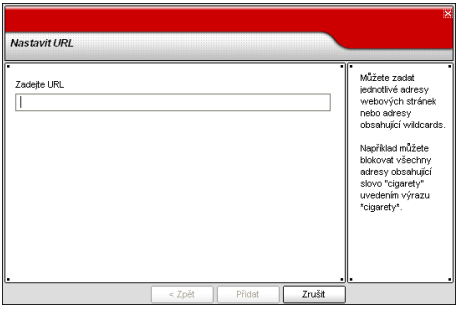
Průvodce nastavení má 3 kroky.

Krok 1/3 - Výběr akce

Zaškrtněte **Určit povolené stránky**/**Určit zakázané stránky** pro povolení/zakázaní přístupu k webovým stránkám, které budou specifikovány v **Kroku 2**.

Krok 2/3 - Určení webových stránek

Klikněte na **Přidat**, napište adresu webové stránky, pro kterou se má použít pravidlo, a stiskněte **Přidat**.



Obrázek 11.3. Určení webových stránek

Důležité

Syntaxe:

- <*.xxx.com> - akce pravidla se použije na všechny adresy zakončené na <.xxx.com>;
- <*porn*> - akce pravidla se použije na všechny stránky obsahující slovo <porn> ve své webové adrese;

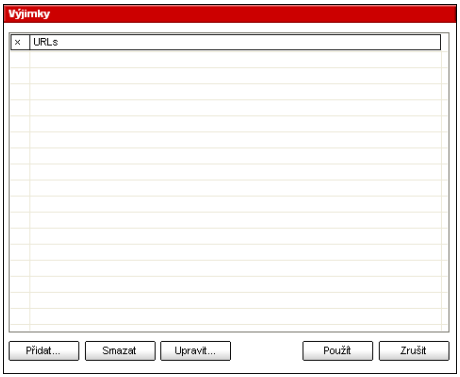
- <www.*.com> - akce pravidla se provede na všechny adresy mající doménu s příponou <com>;
- <www.xxx.*> - akce pravidla se provede na všechny adresy začínající na <www.xxx.> bez ohledu na doménovou příponu;

Kliknutím na **Použít** uložíte změny.

Pro vymazání pravidla jej stačí vybrat a kliknout na **Smazat**. Pro změnu pravidla jej vyberte a klikněte na **Upravit** nebo na pravidlo poklikejte. Pro dočasně pozastavení funkce pravidla bez jeho smazání odškrtněte políčko.

11.2.2. Krok 3/3 - Určení výjimek

Klikněte na **Výjimky**, dále **Přidat**, vepište webovou adresu, pro kterou pravidlo bude provádět výjimku, a klikněte na **Přidat**.



Obrázek 11.4. Určení výjimek

Důležité

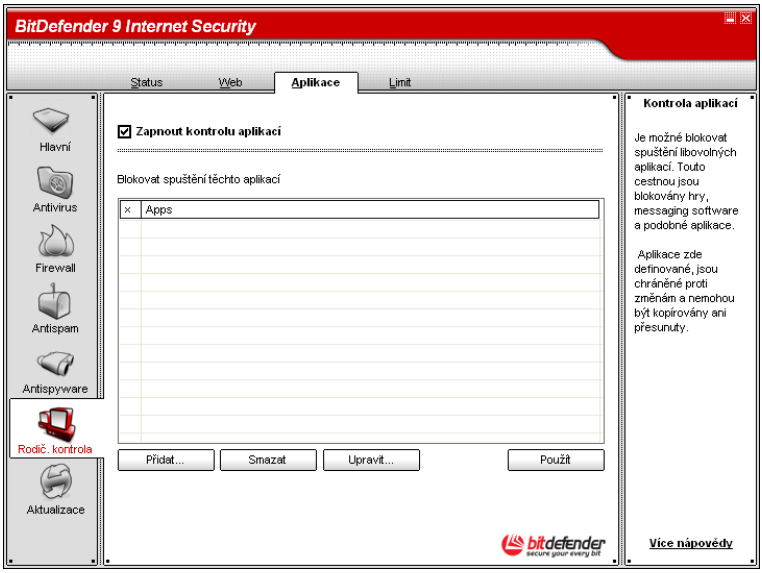
Syntaxe je podobná té popsané v **Kroku 2**.

Kliknutím na **Použít** uložíte změny.

Pro vymazání pravidla jej stačí vybrat a kliknout na **Smazat**. Pro změnu pravidla jej vyberte a klikněte na **Upravit** nebo na pravidlo poklikejte. Pro dočasně pozastavení funkce pravidla bez jeho smazání odškrtněte políčko.

11.3. Kontrola aplikací

Pro zpřístupnění této sekce klikněte na záložku **Aplikace** v modulu **Rodičovský kontrola** module.



Obrázek 11.5. Kontrola aplikací

Kontrola aplikací vám pomáhá zablokovat libovolnou aplikaci před spuštěním. Hry, mediální a chatovací software, stejně tak jako jiný libovolný software může být tímto způsobem zablokován. Takto zablokované aplikace jsou chráněné proti změnám a nemohou být zkopírovány ani přesunuty.

Pro povolení této ochranu zaškrtněte **Zapnout kontrolu aplikací**.

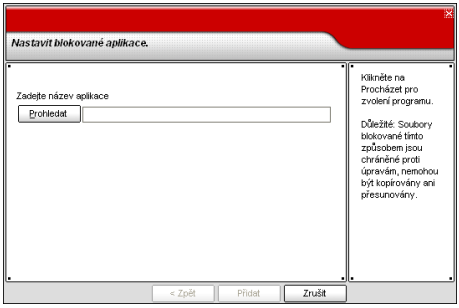
Pravidla musí být zadána ručně vybráním akce a přidáním stránky (kliknutím na **Přidat**).

11.3.1. Průvodce nastavením

Průvodce nastavením má 1 krok.

Krok 1/1 - Vyberte aplikaci pro zablokování

Klikněte **Přidat**, klikněte na **Přidat**, vyberte aplikaci, která má být zablokována a stiskněte **Přidat**.



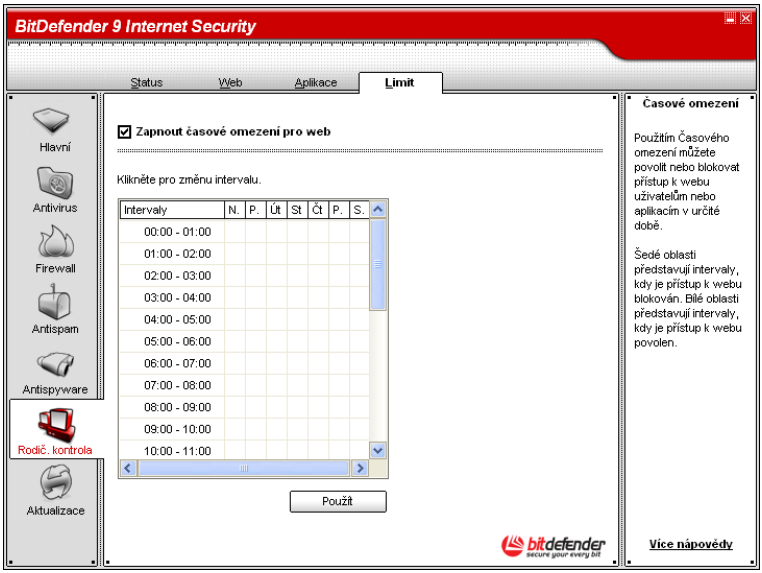
Obrázek 11.6. Vyberte aplikaci pro zablokování

Kliknutím na **Použít** uložíte změny.

Pro vymazání pravidla jej stačí vybrat a kliknout na **Smazat**. Pro změnu pravidla jej vyberte a klikněte na **Upravit** nebo na pravidlo poklikejte. Pro dočasně pozastavení funkce pravidla bez jeho smazání odškrtněte políčko.

11.4. Omezovač pobytu na webových stránkách

Pro zpřístupnění této sekce klikněte na záložku **Limit** v modulu **Rodičovský kontrola** module.



Obrázek 11.7. Omezovač pobytu na webových stránkách

Omezovač pobytu na webu vám pomáhá povolit nebo zablokovat přístup k internetu uživatelům nebo aplikacím v určitém časovém rozmezí.

Poznámka

BitDefender bude provádět aktualizace každou hodinu bez ohledu na nastavení **Omezovače pobytu na webových stránkách**.

Pro povolení této ochrany zaškrtněte **Zapnout časové omezení pro web**.

Vyberte časové intervaly, kdy se mají veškerá internetová spojení zablokovat. Můžete kliknout na jednotlivé buňky nebo můžete kliknout a táhnout pro vetší rozmezí.

Důležité

Buňky s šedou barvou reprezentují časové intervaly, kdy budou veškerá internetová spojení zablokována.

Kliknutím na **Použít** uložíte změny.

Kapitola 12. Aktualizační modul

Aktualizační část této uživatelské příručky obsahuje následující témata:

- Automatické aktualizace
- Ruční aktualiazce
- Nastavení aktualizací

Poznámka

Podrobnější informace týkající se **Aktualizačního** modulu najdete v kapitole *„Modul Aktualizace“* (str. 25).

12.1. Automatické aktualizace

Pro zpřístupnění této sekce klikněte na záložku **Aktualizace** z modulu **Aktualizace**.

Obrázek 12.1. Automatické aktualizace

Jestliže jste připojení k Internetu širokopásmovým nebo DSL připojím, BitDefender pečuje o sebe sám. Kontroluje nové virové podpisy po zapnutí vašeho počítače i každé následující **hodin**.

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-li 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 manualní aktualizace, buďto budete vyzváni k potvrzení aktualizace, nebo aktualizace proběhne automaticky.

Důležité

Může být nezbytné restarovat počítač po ukončení aktualizace. Doporučujeme to udělat co nejdříve.

Poznámka

Jestliže jste připojení k Internetu vytáčenou linkou, pak je dobrý nápad zvyknout si provádět aktualizaci BitDefenderu ručně uživatelem.

12.2. 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 archiv`.

12.2.1. 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 poklikejte na něj, tím spustíte aktualizaci.
3. Klikněte na **Next**.
4. Zaškrtněte **I accept the terms in the License Agreement** a klikněte na **Next**.

5. Klikněte na **Install**.
6. Klikněte na **Finish**.

12.2.2. 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 riozhraní.

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

- Windows 2000, Windows XP.

Windows 2000, Windows XP

Body, které musí být splněny:

1. **Stáhněte příslušnou aktualizaci .** Jestliže je pondělí, prosím stahujte 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, prosím stáhněte oba archivy.
2. Vypněte BitDefender antivirovou ochranu
   - **Vypněte BitDefender řídící konzoli .** Klikněte pravým tlačítkem na ikonku BitDefenderu v Systémové liště a vyberte **Exit**.
   - **Otevřete služby .** Otevřete nabídku **Start**, vyberte **Ovládací panely**, klikněte na **Nástroje pro správu** a potom na **Services**.
   - **Zastavte BitDefender Virus Shield service .** Vyberte **BitDefender Virus Shield** ze seznamu a klikněte na **Stop**.

- **Zastavte BitDefender Scan Server service .** Vyberte **BitDefender Scan Server** ze seznamu a klikněte na **Stop**.

3. **Rozbalte obsah archívu .** Začněte `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.

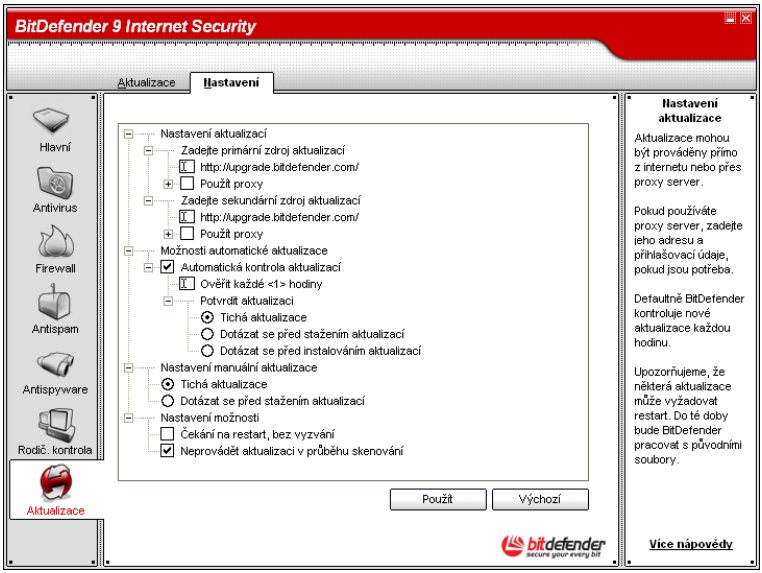
   - **Zapněte BitDefender Scan Server service .** Vyberte **BitDefender Scan Server** ze seznamu a klikněte na **Start**.

   - **Zapněte BitDefender Virus Shield service .** Vyberte **BitDefender Virus Shield** ze seznamu a klikněte na **Start**.

   - Otevřete řídící konzoli BitDefenderu.

12.3. Nastavení aktualizací

Pro zpřístupnění této sekce klikněte na záložku **Nastavení** z modulu **Aktualizace**.



Obrázek 12.2. Nastavení aktualizací

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

Okno s nastavením aktualizací obshauje 4 kategorie možností (**Nastavení aktualizací**, **Možnosti automatické aktualizace**, **Nastavení manualní aktualizace** a **Možnosti rozhraní**) uspořádané v rozbalovacím menu, podobně jakko ve Windows.

Poznámka

Klikněte na tlačítko "+" a rozbalte požadovanou kategorii nebo klikněte na "-" a zavřete ji.

12.3.1. Aktualizovat nastavení lokality

Pro rychlejší aktualizace můžete nastavit dvě lokality: **Zadejte primární zdroj aktualizací** a **Zadejte sekundární zdroj aktualizací**. Pro obě locality musíte nastavit následující:

- **Aktualizovat lokalitu** - Pokud jste připojeni do sítě, která používá BitDefender signatury lokálně, změňte toto nastavení. Defaultní 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 prosy 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.

12.3.2. Možnosti automatické aktualizace

- **Automatické kontrola aktualizací** - BitDefender automaticky kontroluje, zda jsou na serverech dostupné nové aktualizace.
- **Ověřit každé x hodiny** - Nastavení, jak často BitDefender kontroluje dostupnost aktualizací. Defaultní hodnota je 1 hodina.
- **Tichá aktualizace** - BitDefender automaticky stáhne a nahraje aktualizaci.
- **Dotázat se před stažením 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 stažením aktualizací** nebo **Dotázat se před instalováním aktualizací** a zvolíte ukončit a zavřít management konzoli, automatická aktualizace nebude provedena.

12.3.3. Nastavení manualní aktualizace

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

Důležité

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

12.3.4. Možnosti rozhraní

- **Cekání na restart, bez vyzvání** - Pokud aktualizace vyžaduje restart, product bude nadále pracovat s původními soubory, dokud počítač nebude restartován. Uživatel nebude k restartu počítače vyzýván, takže jej aktualizace BitDefenderu nebude vyrušovat při práci.

Klikněte na **Použít** pro uložení změn nebo klikněte na **Výchozí** pro načtení defaultního nastavení.

Doporučený postup

Kapitola 13. Doporučený postup

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

- Antivirus
- Firewall
- Antispam
- Antispyware

13.1. Antivirus

Kroky, které musí být splněny pro zajištění počítače bez virů:

1. Po skončení instalace prosím zaregistrujte váš produkt, jak je popsáno v sekci „*Registrace produktu*“ (str. 36).
2. Proveďte manuální aktualizaci virových podpisů popsanou v sekci „*Automatické aktualizace*“ (str. 145).
3. Proveďte úplný test vašeho systému popsaného v sekci „ *Okamžité skenování* “ (str. 51).
4. V sekci Stav v **Hlavním** mějte aktivované všechny dostupné ochrany BitDefenderu: **Virový štít**, **Firewall** a **Automatická aktualizace**.
5. Nastavte váš BitDefender, aby testoval váš systém nejméně týdně, jak je popsáno v sekci „*Plánování skenování*“ (str. 60).

13.2. Firewall

Kroky ke správnému nastavení modulu **Firewall**:

1. Po skončení instalačního procesu se objeví průvodce. Následujte jeho instrukce, jak je popsáno v sekci *„Průvodce nastavením Firewallu“* (str. 77).

Poznámka

Průvodce může být také spuštěn, kdykoliv chcete kliknutím na **Průvodce pravidel** z menu *„Pokročilá nastavení“* (str. 92).

2. V sekci Status **Hlavního** modulu mějte zapnutý **Firewall**.
3. V sekci Ochrana spojení modulu **Firewall** uložte soubor pravidel.
4. V sekci Pokročilá nastavení modulu **Firewall** nastavte ICMP filtr.

13.3. Antispam

Kroky, které musí být splněny, aby váš počítač zůstal bez spamu:

1. Pokud používáte Microsoft Outlook nebo Microsoft Outlook Express, postupujte dle průvodce konfigurací, který se otevře, jakmile poprvé otevřete Vašeho e-mailového klienta. Rovněž jej můžete otevřít z *„Antispam lištu nástrojů“* (str. 105).
2. Do Seznamu přátel přidejte adresy lidí, od nichž rozhodně musíte dostávat e-maily.

Poznámka

BitDefender nebude blokovat zprávy od lidí na seznamu. Používání seznamu tedy zabezpečí, že prijdou pouze legitimní zprávy.

3. Trénujte *„ Bayesiánský filtr “* (str. 23). Pokaždé, když obdržíte e-mail, který považujete za SPAM, ale BitDefender jej jako spam neoznačil, vyberte tento e-mail a v liště nástrojů Antispamu klikněte na tlačítko **To je spam**. Další e-maily, které budou vykazovat stejné rysy, budou označeny jako SPAM.

Poznámka

Bayesiánský filtr se aktivuje, pokud jste jej vytrénovali s více než 60 legitimními e-mailovými zprávami. Postupujte podle průvodce konfigurací.

4. Aktualizujte váš BitDefender.

Poznámka

Pokaždé, když provedete aktualizaci:
- nové obrazové podpisy budou přidány do **Obrázkového filtru**;
- nové webové stránky budou přidány do **URL filtru**;
- nová pravidla budou přidána do **Heuristického filtru**.

Tím se zvýší efektivita nástroje Antispam.

5. Konfigurujte Charset filtr - většina spamových zpráv je napsána cyrilicí a /nebo Asijskými znaky. Konfigurujte tento filtr, pokud chcete odmítnout všechny e-maiové zprávy napsané v těchto písmech..

Poznámka

Můžete aktivovat / deaktivovat každý z filtrů **Antispamu** v sekci Nastavení modulu **Antispam**.

13.4. Antispyware

Kroky, které musí být splněny, aby váš počítač zůstal bez spywaru:

1. Proveďte ruční aktualizaci spywarových podpisů popsanou v sekci *„Automatické aktualizace“* (str. 145).

2. Proveďte úplný test vašeho systému, jenž je popsán v sekci *„ Okamžité skenování “* (str. 51).

3. V sekci Status **Hlavního** modulu mějte zapnutý **Antispyware** a **Automatické aktualizace**.

4. V sekci Štít modulu **Antispyware** mějte aktivované všechny dostupné ochrany BitDefenderu: **Kontrola souborů**, **Kontrola vytáčení** a **Kontrola registrů**.

5. Nastavte váš BitDefender, aby testoval váš počítač nejméně jednou týdně, jak je popsáno v sekci *„Plánované testování“* (str. 133).

Záchranné CD BitDefenderu

BitDefender 9 Internet Security přináší bootovatelné CD (Záchranné CD BitDefenderu založeného na LinuxDefenderu) schopné testovat a léčit všechny existující pevné disky před startem vašeho operačního systému.

Měli byste použít Záchranné CD BitDefendru, 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.

Kapitola 14. Přehled

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

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

14.1. Co je KNOPPIX?

Citace z http://knopper.net/knoppix:

„ KNOPPIX je bootovatelné CD se sbírkou GNU/Linuxového (http://www.linux.com/) sotwaru, automatickou detekcí hardwaru a podporou pro mnoho grafických karet, zvukových karet, SCSI a USB zařízení a dalších periferních zařízení. KNOPPIX může být používán jako Linuxová demo verze, vzdělávací CD, záchranný systém nebo upraven a používán jako platforma pro komerční demo software. Není nutné instalovat cokoliv na harddisk. “

14.2. 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 pro aktualizovanou ochranu internetové připojení je NUTNOSTÍ.
Grafické rozlišení	Grafické rozlišení minimálně 800x600 je doporučeno pro internetovou správu.

14.3. Zahrnutý 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)
- Linuxové jádro 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

14.4. 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.

14.4.1. 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 jedinečnépatentované 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.

14.4.2. BitDefender Vzdálená správa

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

1. Spusťte Firefox prohlížeč a spusťte BitDefender Vzdálenou správu URL: https://localhost:8139 (nebo poklikejte na BitDefender ikonu pro Vzdálenou správu 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 emailové 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")

14.4.3. 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**.

Kapitola 15. LinuxDefender nápověda

15.1. Spuštění a ukončení

15.1.1. Spuštění LinuxDefenderu

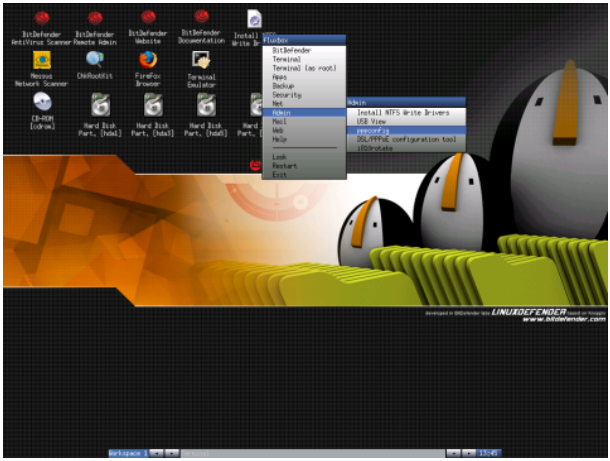
Ke spuštění CD nastavte BIOS vašeho počítače na bootování z CD, vložte CD do mechaniky a restartujte počítač. Ujistěte se, že váš počítač může bootovat z CD.

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

Obrázek 15.1. 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 standartním nastavením pouze stiskněte ENTER.

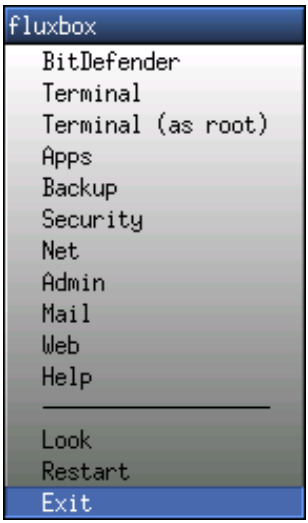
Poté, co je dokončen proces bootovaní, spatříte další obrazovku. Nyní můžete začít používat LinuxDefender.



Obrázek 15.2. Plocha

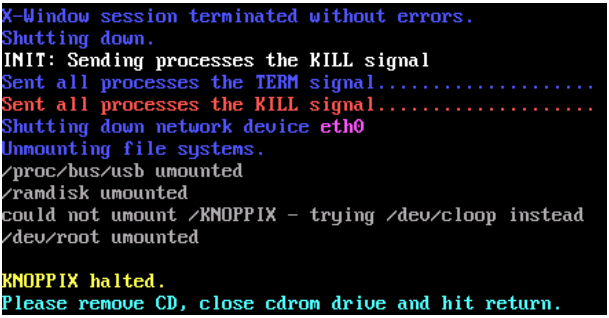
15.1.2. Ukončení LinuxDefender

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.



Obrázek 15.3. "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.



Obrázek 15.4. Čekání na zprávu, když se počítač vypíná

15.2. Nastavte internetové 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.

15.3. Aktualizace BitDefenderu

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, **Configuration** ho v nabídce **Live! Update**.

15.4. Hledání virů

15.4.1. Jak mohu zpřístupnit má Windows data?

Podpora pro zápis NTFS

Podpora pro zápis NTFS k dispozici používáním metody Captive NTFS write project. Potřebujete dva soubory řadičů z vaší Windows instalace: `ntoskrnl.exe` a `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).

15.4.2. 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.

15.5. Vytvořte okamžitý filtr 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.

15.5.1. 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 Průvodce Linuxových připojení a do dokumentace Netfilter.

15.5.2. Emailový obránce

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

Pro nastavení BitDefender 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.

15.6. Proveďte síťovou bezpečnostní prověrku

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.

15.6.1. Kontrola systémových nástrojů

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 **Scan for viruses**, 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 zkoontrolovali 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**.

15.6.2. Nessus - síťový skener

Co je Nessus? „ Nessus je nejoblíbenější testovací program zranitelnosti sítě na světě používaný ve více než 75,000 organizacích na celém světě. Mnoho největších světových organizací si uvědomilo významné úspory nákladů použitím programu Nessus pro kontrolu důležitých obchodních podnikových zařízení a aplikací. “

Nessus může být užívaný pro vzdálené testování vašich síťových počítačů proti různé zranitelnosti. Také doporučuje některé opatření ke snížení bezpečností 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 všechny všechny 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, Nessus zobrazí výsledky a doporučení. Můžete uložit zprávu do několika formátů, včetně HTML s koláčovými grafy a tabulkamy Uloženou zprávu můžete zobrazit vaším oblíbeným prohlížečem.

15.7. 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.

Jak získat pomoc

Kapitola 16. Podpora

16.1. Odborná pomoc

Jakožto seriozní firma, se SOFTWIN snaží poskytovat svým zákazníkům rychlou a přesnou podporu nesrovnatelné úrovně. Asistenční centrum je nepřetržitě zásobováno nejnovějšími popisy virů a disponuje odpověďmi na běžné otázky, tak aby včas pomohlo nalézt řešení Vašich problémů.

My, kdo pracujeme v SOFTWINu, jsme odhodláni šetřit zákazníkův čas a peníze poskytováním nejpokročilejších produktů za nejlepší ceny. Myslíme si, že úspěšný business závisí na dobré komunikaci a smyslu pro dokonalou podporu zákazníka.

Pište nám o kdykoliv o pomoc na e-mail <antiviry@officeplus.cz>. Pro rychlou odezvu, prosím zahrňte ve vašem e-mailu co nejvíce detailů o vašem BitDefender, systému a popište váš problém co možná nejpřesněji.

16.2. On-line nápověda

16.2.1. 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 k 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.

16.3. Kontaktní informace

Schopná komunikace je klíčem k úspěšnému obchodu. Posledních 10 let 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.

16.3.1. Webové adresy

Prodejní oddělení: <sales@bitdefender.com>
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>
Ounámení zneužívání produktu: <abuse@bitdefender.com>
Tvorba webových stránek: http://www.bitdefender.com
Tvorba ftp archívů: ftp://ftp.bitdefender.com/pub
Lokální distributoři: http://www.bitdefender.com/partner_list
BitDefender databáze znalostí: http://kb.bitdefender.com

16.3.2. Kontakty

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

ČESKÁ REPUBLIKA

OfficePlus s.r.o.
Pod Vrchem 676
276 01 Mělník
Technická podpora: <antiviry@officeplus.cz>
Vertrieb: <obchod@officeplus.cz>
Telefon: +420 315 602 333
Fax: +420 315 602 333
Web: http://www.antiviry.officeplus.cz

Germany

Softwin GmbH
Karlsdorfer Straße 56 88069
Tettnang
Technischer Support: <support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Product web site: http://www.bitdefender.de

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128

Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support: <support@bitdefender.us>
Sales: <sales@bitdefender.us>
Phone: 954 776 62 62, 800 388 80 62
Fax: 954 776 64 62, 800 388 80 64
Product web site: http://www.bitdefender.us

Rumunsko

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Kapitola 17. Často kladené otázky

17.1. Hlavní

Otázka Jak se mohu přesvědčit o tom, že BitDefender skutečně pracuje?

Odpověď V modulu **Hlavní** vstupte do sekce Status a prohlédněte si statistiky.

Otázka Jaké jsou systémové požadavky?

Odpověď Naleznete je v sekci „*Systémové požadavky*“ (str. 3).

Otázka Jak odinstaluji BitDefender?

Odpověď Proces odstranění je popsán v sekci „*Odstranění, oprava nebo modifikace charakteristik BitDefenderu*“ (str. 7).

Otázka Jak registrovat BitDefender?

Odpověď Registrační proces je popsán v sekci „*Registrace produktu*“ (str. 36).

17.2. Antivirus

Otázka Jak mohu provést celkové skenování systému?

Odpověď V modulu **Antivirus** vstupte do sekce Test, zaškrtněte **Místní disky** a klikněte **Test**.

Otázka Jak často mám počítač skenovat?

Odpověď Doporučujeme skenovat Váš počítač minimálně jednou týdně.

Otázka Mohu nějak automaticky skenovat každý soubor, který přesouvám do svého počítače?

Odpověď BitDefender skenuje všechny soubory na vstupu. Vše co musíte udělat, je mít aktivovaný Virový štít.

Otázka Jak mohu naprogramovat BitDefender, aby periodicky skenoval můj počítač?

Odpověď V modulu **Antivirus**, vstupte do sekce Plánovač klikněte na **Nový** a postupujte dle průvodce.

Otázka Co je možné udělat se soubory z karanténní zóny?

Odpověď Můžete odeslat tyto soubory do laboratoře BitDefenderu na analýzu, ale nejprve musíte specifikovat nastavení e-mailů (vstupte do sekce Karanténa a klikněte **Nastavení**).

17.3. Firewall

Otázka Jak mohu blokovat veškerý internetový provoz?

Odpověď V modulu **Firewall**, v sekci Status, klikněte **Blokovat**.

Otázka Proč je důležité sledovat Průvodce firewallem?

Odpověď Průvodce vám pomůže nastavit firewall a vytvořit potřebná pravidla. Ta jsou nutná pro většinu běžně používaných aplikací. Konečným výsledkem je zabezpečený system s funkčním mailovým klientem a internetovým prohlížečem.

17.4. Antispam

Otázka Co je spam?

Odpověď Spam je nevyžádaný komerční e-mail.

Otázka Jak pracuje BitDefender Antispam?

Odpověď Prosím podívejte se do sekce „*Modul Antispam*“ (str. 20).

Otázka Kam poté spam odchází?

Odpověď Používáte-li **Microsoft Outlook** / **Microsoft Outlook Express**, jsou spamové zprávy přesunuty do složky **spamů** / **smazaných položek**.

Poznámka

Pokud používáte jiného e-mailového klienta, měli byste vytvořit pravidlo pro přesun e-mailových zpráv označených jako Spam do složky “custom” karanténa. BitDefender připojí titul [SPAM] do předmětu zpráv považovaných za Spam.

Otázka: Zablokoval jsem e-mailovou adresu, ale nepřestal jsem dostávat e-mailové zprávy z této adresy. Proč?

Odpověď: Pokud dostáváte spam z adresy, kterou jste blokovali, ujistěte se, že adresa není také na White listu. **White list** má přednost před Black listem.

Otázka: Co je White list?

Odpověď: Je to seznam e-mailových adres, z nichž vždy chcete dostávat poštu, bez ohledu na její obsah.

Otázka: Co je Black list?

Odpověď: Je to seznam všech e-mailových adres, ze kterých nechcete dostávat zprávy, bez ohledu na jejich obsah.

Otázka: Co je Jazykový (znaková sada) filtr?

Odpověď: Je to filtr, který blokuje všechny e-mailové zprávy napsané v cyrilice a/nebo asijském znakovém písmu.

Otázka: Co je URL filtr?

Odpověď: Je to filtr, který prohledává odkazy ve zprávách a srovnává je s odkazy v databázi URL filtr BitDefender. V případě shody je přičteno ke spamovému skóre číslo 45.

Otázka: Co je Heuristický filtr?

Odpověď: Je to filtr, který provádí sadu testů na všech komponentách zprávy (tj. nejen na záhlaví, ale rovněž na těle zprávy jak v HTML tak v textovém formátu), prohledává slova, fráze, odkazy a ostatní charakteristiky spamu. Výsledkem je, že k e-mailu přidá spamové skóre.

Otázka: Co je Bayesiánský filtr?

Odpověď Je to filtr, který klasifikuje zprávy na základě statistických propočtů udávajících míru výskytu specifických slov ve zprávách klasifikovaných jako Spam v porovnání se zprávami prohlášenými (Vámi, nebo Heuristickým filtrem) za Ne-Spam.

17.5. Antispyware

Otázka Co je to rychlé skenování?

Odpověď Rychlé skenování je skenovací proces proti spyware, kdy jsou skenovány jen zápisy do registrů, cookies, procesy a některé specifické soubory.

Otázka Jaký je rozdíl mezi rychlým a podrobným skenováním?

Odpověď Podrobné skenování skenuje na přítomnost nejen spyware, ale i virů.

Otázka Co dělá Kontrola vytáčení?

Odpověď **Kontrola vytáčení** monitoruje všechny dialery (voliče telefonních čísel) pokoušející se o přístup do počítačového modemu, okamžitě varuje uživatele a vyzývá jej, aby rozhodl, že se takové operace mají blokovat nebo povolit.

Otázka Co dělá Kontrola scriptu?

Odpověď **Kontrola scriptu** monitoruje všechny webové stránky, které se pokoušejí aktivovat script nebo jiný aktivní obsah. Můžete určit, kterým stránkám lze věřit, a kterým nikoliv.

Otázka Co dělá Kontrola cookie?

Odpověď **Kontrola cookie** chrání Vaše soukromí, když používáte internet.

17.6. Aktualizace

Otázka Proč je nutné aktualizovat BitDefender?

Odpověď Pokaždé, když provedet aktualizace jsou do skenovacích nástrojů přidány nové virové signatury, nové obrazové podpisy budou přidány do **Obrázkového filtru**, nové webové stránky budou přidány do **URL filtru** nová pravidla budou přidána do **Heuristického filtru**.

Otázka Jak mohu aktualizovat BitDefender?

Otázka BitDefender je defaultně nastaven tak, že je automaticky aktualizován každou hodinu. Ale možná je i ruční aktualizace, či změna časového intervalu pro automatickou aktualizaci (v modulu Aktualizace).

Slovníček

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 omezení;experti zabývající se bezpečností počítačů zrazují před jeho používáním na internetu.

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.

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, pokud ne, nemůžete instalovat Aktualizace.

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

Archiv

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

	Soubor, který obsahuje jeden nebo více souborů v komprimovaném formátu.
Boot sectorů	Sektor na začátku každého disku, který rozpozná architekturu disku (velikost sektoru, velikost clusteru atd.). U startovacích disků obsahuje zaváděcí sector rovněž program, který načítá operační systém.
Boot virus	Virus, který infikuje zaváděcí sector pevného nebo pružného disku. Pokus o zavádění z diskety infikované virem zaváděcího sektoru zapříčiní, že se virus v paměti zaktivizuje. Pokaždé, když zavedete systém z tohoto místa, budete mít aktivní virus v paměti.
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.
Cookie	V internetovém žargonu 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, cílovat 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.
Červ	Program, který se množí v síti a rozšiřuje, kudy projde. Neumí se připojit k jiným programům.
Definice viru	Binární vzorec viru, používaný antivirovým programem k odhalení a elminaci viru.
Disková mechanika	Je zařízení, které čte data a zapisuje je na disk.

	Mechanika hard disku čte a zapisuje do hard disků. Mechanika pružného disku slouží pro pružné disky. Diskové mechaniky mohou být buďto interní (umístněné uvnitř počítače), nebo externí (umístěné v oddělené krabici, která se připojuje k počítači).
E-mail	Elektronická pošta. Servis, který zasílá zprávy na počítače prostřednictvím místních nebo globálních sítí.
E-mailový klient	E-mailový klient je aplikace, která Vám umožňuje posílat a dostávat e-mail.
Falešná pozitivita	Objeví se, když skener identifikuje soubor jako infikovaný, ačkoliv ve skutečnosti není.
Heuristický	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 "falešné pozitivitě".
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 uživatelově zařízení (klient). Applety se v jednotlivých aplikacích liší, a jsou regulovány přísným bezpečnostním protokolem. Příklad: přestože jsou spouštěny u uživatele, nemohou přečíst nebo zapsat data z/na uživatelova/o zařízení. Applety jsou dále omezovány, takže mohou číst a psát data pouze na té doméně, z níž jsou poskytovány.

Macro 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 konat pokaždé, když je dokument otevřen.
Ne-heuristický	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.
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.
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.
Položky Startupu	Veškeré soubory uložené v této složce se otevřou, jakmile se spustí počítač. Na příklad, obrazovka při startu, zvukový soubor, který se přehraje, když je počítač poprvé spuštěn, kalendář s připomínkami, nebo aplikační programy. Obvykle je do této složky uložen alias souboru , a ne samotný soubor.
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.
Prohlížeč	Zkratka pro Webový browser, softwarovou aplikaci používanou pro lokalizaci a zobrazení webových stránek. Dva nejpopulárnější prohlížeče jsou Netscape Navigator 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-in.
Příkazový řádek	V příkazovém řádku píše uživatel příkazy do prostoru poskytnutého přímo na obrazovce.
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.
Script	Jiný termín pro makro nebo pro dávkový /batch/ soubor; script je seznam příkazů, které mohou být vykonány bez uživatelovy interakce.
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.
Spam	Jedná se o hromadné rozesílání nevyžádaných e-mailů.
Spyware	Jedná se o software, který tajně shromažďuje informace o uživateli prostřednictvím internetového připojení, které bývají využity zejména k reklamním účelům. Spywarové aplikace bývají často skrytou komponentou freeware nebo shareware programů, které se dají stáhnout z internetu. Pokud je spyware nainstalován, monitoruje aktivity uživatele na internetu a na pozadí posílá shromážděné informace třetí osobě. Spyware

shromažďuje také e-mailové adresy, hesla, čísla kreditních karet apod.

Nehledě na otázku etiky a porušování soukromí, spyware zabírá také paměť a systémové zdroje počítače, zneužívá připojení k internetu a zpomaluje tak chod dalších aplikací. Může vést až k nestabilitě a pádu systému.

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 servisu na vlastní počítač. Stahování může často odkázat na kopírování souboru ze síťového souborového serveru na počítač v síti.

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 na ikonu pro zobrazení a vstup do detailů a kontroly.

Tajný vchod

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

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 rutinním provozu.

Trójský 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 Trójského koně je program, který se domáhá vyčištění Vašeho počítače od virů, ale namísto toho do Vašeho 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 Trói.

Události

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

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, potože 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.

Zabalené programy

Soubor v komprimovaném formátu. Mnoho operačních systémů a aplikací obsahuje příkazy, které Vám umožní zapakovat soubory tak, aby zabíraly méně paměti. Na příklad 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.