avast! antivirus
Professional Edition **4**.8

Uživatelský manuál

OBSAH

Úvod

Vítejte v programu avast! antivirus Professional Edition verze 4.8.

avast! antivirus je soubor špičkových aplikací, které mají za úkol ochránit Váš počítač před virovou nákazou. S jeho pomocí můžete velmi podstatným způsobem snížit riziko napadení Vašeho počítače virem, a zamezit tak ztrátě dat.

avast! antivirus 4.8 zahrnuje prvky antispyware ochrany, certifikované procedurou Checkmark West Coast Lab, a antirootkit technologie zabudované přímo do programu avast! antivirus.

O firmě ALWIL Software a.s.

ALWIL Software je čistě česká firma, založená již v dubnu 1991. Od 1. Ledna 2007 se společnost ALWIL Software mění na akciovou společnost. Naše produkty jsou ale na trhu již od roku 1988. Specializujeme se na ochranu dat na počítačích kompatibilních s IBM PC s operačními systémy MSDOS, Windows a Novell.

Naše firma spolupracuje s řadou jiných firem a osobností z antivirové oblasti po celém světě. I díky tomu je kvalita našich programů velmi vysoká, podle nezávislých testů patří dlouhodobě ke světové špičce.

Naše firma je důkazem, že špičkové softwarové firmy se nevyskytují pouze v Silicon Valley, ale i v tak krásném městě, jako je Praha. Praha je nyní nejen romantickým a historickým městem, plným gotických a barokních památek, ale i místem vývoje kvalitního softwaru.

Více informací o našich produktech naleznete na webové stránce
http://www.avast.com/index_cze.html

Podpora produktů avast!

Pokud budete mít jakýkoliv problém s programem avast!, který se Vám nepodaří vyřešit ani po přečtení manuálu, obraťte se prosím na internetovou stránku naší podpory
http://support.avast.com

- V **Knowledgebase** si můžete prohlédnout tříděný seznam odpovědí na nejčastěji kladené otázky.

- Popřípadě využijte výhody českého fóra produktů avast! Zde můžete vyměnit svoje zkušenosti s dalšími uživateli programu a dozvědět se mnoho užitečných informací o problémech, které je provázejí. K využívání fóra je nejpreve nutné provést jednoduchou registraci. Více informací naleznete na adrese **http://forum.asw.cz/**

Pokud Váš problém i nadále přetrvává, můžete přímo "**Vytvořit případ**" týmu naší technické podpory. K tomu se budete muset znovu zaregistrovat. Prosím, přiložte ke zprávě co nejvíce informací vztahujících se k Vašemu případu.

Počítačové hrozby

Viry, spyware, rootkity a další formy škodlivého softwaru jsou souborně nazývány jako malware (zkratka pro malicious software); malware je také někdy označován za “badware”.

Co je to počítačový virus?

Počítačový virus je část softwaru, většinou škodlivého, který se sám šíří mezi jednotlivými počítači. Je schopen způsobit poškození systému, ztrátu důležitých dat, nebo může být využit k instalaci dalšího spyware, rootkitů nebo jiného malware.

Nejdůležitějším krokem k prevenci problémů je pravidelná aktualizace antiviru avast! na všech počítačích v síti. Také se doporučuje kontrolavat a provádět aktualizaci nejnovějších bezpečnostních balíků daného operačního systému. Uživatel by se měl vždy ujistit, zda může důvěřovat softwaru, který si z internetu stahuje. Spousta malware je do počítače instalováno spolu se softwarem, který navenek vypadá legitimně.

Co je spyware?

Spyware je software instalovaný na počítače za účelem sběru dat o uživateli bez jeho souhlasu a vědomí. To může vést až k úniku citlivých informací (například údaje o bankovních účtech a kartách) nebo úniku důležitých firemních dat.

V dnešní době se tvorbě spyware věnuje stále více dobře organizovaných kriminálních skupin, do počítače se dostává pomocí virů či jiného typu malware.

Co jsou rootkity?

Rootkity jsou programy, které se instalují na počítač zatímco jejich procesy, služby a registrační klíče zůstanou skryté a tím neviditelné pro uživatele. Představují riziko pro domácí a firemní sítě a je velmi těžké je najít a odstranit.

Rootkity se normálně šíří pomocí dalšího malware (jako např. Trojanů) a proto doporučujeme, aby si všichni uživatelé pravidelně aktualizovali avast!

Hlavní součásti programu avast! antivirus

avast! antvirus 4.8 je velkým skokem v pokroku technologie produktové řady avast! Zahrnuje přidání antispyware ochrany, certifikované procedurou Checkmark West Coast Lab, a antirootkit technologie přímo do programu. avast! 4.8 antivirus také přidává silnou sebeobranu, která znemožňuje útoky proti programu samotnému. Pravidelně získává ocenění Virus Bulletin 100% za detekci 100% "in the wild" virů šířící se volně mezi uživateli a je opakovaným vítězem ceny Secure Computing Award.

avast! antivirus je používán ve více než 60 miliónech domácností a kanceláří. Je speciálně navržen tak, aby zátěž na operační systém počítače byla co nejmenší a automatické aktualizace jak programu, tak virové databáze byly prováděny automaticky.

Avast! Antivirus představuje sbírku špičkových technologií, která Vám nabízí bezkonkurenční ochranu proti všem formám malware. Přehled hlavních součástí programu naleznete níže.

Hlavní součásti	Home Edition	Professional Edition
Antivirové jádro	**Ano**	**Ano**
Silná residentní ochrana	**Ano**	**Ano**
Antispyware ochrana zabudovaná v Antivirovém jádru	**Ano**	**Ano**
Rootkit ochrana zabudovaná v Antivirovém jádru	**Ano**	**Ano**
Sebeochranné mechanismy	**Ano**	**Ano**
Automatické inkrementální aktualizace	**Ano**	**Ano**
Virová truhla k ukládání podezřelých souborů	**Ano**	**Ano**
Integrace do systému	**Ano**	**Ano**
Integrovaný nástroj Virus Cleaner	**Ano**	**Ano**
Test z příkazové řádky	**Ne**	**Ano**
Script blocker	**Ne**	**Ano**
PUSH aktualizace	**Ne**	**Ano**
Rozšířené uživatelské rozhraní a možnost vytvářet a plánovat úlohy	**Ne**	**Ano**

Antivirové jádro

Antivirové jádro je základním prvkem programu. Poslední verze avast! Antivirus kernel kombinuje špičkový výkon s vynikající schopností detekce, čímž dosahuje 100% detekovaných "in the wild" virů a excelentní detekce Trojských koní s minimem falešných poplachů.

Antivirové jádro je držitelem certifikátu ICSA Labs; pravidelně se účastní testů časopisu Virus Bulletin, kde často získává prestižní ocenění VB100.

Residentní ochrana

Residentní ochrana (ochrana systému v reálném čase) je v dnešní době jednou z nejdůležitějších složek každého antivirového programu. Residentní ochrana avastu zahrnuje více částí jednotlivých poskytovatelů, kteří jsou schopni zachytit virus před tím, než by mohl infikovat Váš počítač.

Antispyware ochrana zabudovaná v Antivirovém jádru

avast! antivirus 4.8 zahrnuje nové prvky antispyware ochrany, certifikované procedurou Checkmark West Coast Lab, které zaručují ještě vyšší schopnost ochrany důležitých dat a programů.

Rootkit ochrana zabudovaná v Antivirovém jádru

Anti-rootkit technologie založená na špičkové technologii GMER je také obsažena v základní verzi. Pokud je rootkit objeven, avast! ho vypne a až poté, co nemůže poškodit běh počítače, je vymazán. Avast! Antivirus disponuje virovou databází, která se automaticky aktualizuje a poskytuje tak ochranu proti nejnovějším typům rootkitů.

Sebeochranné mechanismy

Některé viry se mohou pokusit vypnout Váš antivirový software. Proti těmto nejnovějším typům útoků avast! vyvinul velmi kvalitní a silné sebeochranné mechanismy. Jsou založeny na vysoce ceněné technologii avast! antivirus, která poskytuje další vrstvu ochrany dat a programů.

Automatické aktualizace

Automatické aktualizace jsou dalším klíčovým prvkem antivirové ochrany. Aktualizace programu i virové databáze mohou být prováděny automaticky. Jsou inkrementální, což znamená, že se stahují pouze nová či chybějící data, což významně snižuje čas potřebný k aktualizaci. Velikost aktualizací se v případě virové databáze pohybuje v řádu desítek KB a programu v řádu stovek KB.

Pokud máte pevné internetové připojení (jako např. Broadband), potom se aktualizace provádějí zcela automaticky v předem stanovených intervalech. Pokud se připojujete k internetu pouze příležitostně, avast! připojení sleduje a provede aktualizaci, když jste online. Tento proces je blíže popsán na straně 34.

Virová truhla

Virovou truhlu si můžete představit jako adresář na disku, který má speciální bezpečnostní vlastnosti, díky nimž dokáže izolovat potenciálně nebezpečné soubory. Se soubory v truhle lze pracovat, ale s určitými bezpečnostními omezeními.

Hlavním účelem virové truhly je izolace souborů od operačního systému. Tyto soubory nemohou být ovlivněny žádnými procesy zvenčí. Žádné nebezpečí nehrozí ani pokud do truhly uložíte infikované soubory. Virová truhla je také užitečná v případě tzv. falešných alarmů. Když se detekovaný soubor později ukáže jako falešný alarm a není infikovaný, můžete soubor přesunout zpět na své původní místo.

Více informací naleznete na **straně 45**

Integrace do systému

avast! antivirus je plně integrován do systému Vašeho počítače.

Testování lze provádět přímo z prostředí průzkumníka Windows kliknutím pravým tlačítkem myši na soubor či adresář a zvolením příslušné položky z nabídky.

Avast! také obsahuje speciální šetřič obrazovky, který při aktivaci spouští test disku. Můžete ho použít spolu s Vaším oblíbeným šetřičem obrazovky. Více informací o konfiguraci šetřiče obrazovky avast! antivirus naleznete na **straně 65**.

Ve 32-bitových verzích Windows NT/2000/XP/Vista avast! nabízí možnost Naplánovat úlohu po startu počítače tzv. “boot time scan”, což umožní scan po startu systému před tím, než by virus mohl počítač napadnout.

Integrovaný nástroj avast! Virus Cleaner

Hlavním cílem programu avast! je ochrana dat proti virové či jiné infekci. Primární je proto prevence, ne léčení virů. avast! ovšem nabízí i speciální nástroj na léčení virů Virus Cleaner, který umí odstranit některé běžné viry z infikovaných počítačů. Množství počítačových virů bohužel neustále stoupá a proto je někdy nutné vyhledat pomoc odborníka.

Více informací o nástroji Virus Cleaner naleznete na **straně 63**.

Test z příkazové řádky

Pro pokročilé uživatele avast! nabízí možnost testu z příkazové řádky. Příkazem ashCmd spustíte stejný test antivirového jádra jako z normálního grafického rozhraní. V příkazové řádce je dostupný speciální STDIN/STDOUT mód se širokou škálou různých parametrů. Tento mód je navržen pro BATCH programy, má stejné možnosti jako rozšířené uživatelské rozhraní (včetně reportů). Návod k příkazové řádce naleznete na **straně 91**.

Script blocker

Zabudovaný script blocker Vás chrání proti script virům schovaným uvnitř webových stránek. Takové skripty jsou normálně neškodné. Programy, které je spouštějí jim totiž zabrání v přístupu k jakýmkoliv souborům. Někdy se ale může objevit bezpečnostní díra, kterou viry využívají k infikování počítače. Avast! proto kontroluje potenciálně nebezpečné skripty webových stránek, které navštěvujete.

PUSH aktualizace

Další speciální složkou Professional Edition jsou PUSH aktualizace. Jde o velkou změnu v technologii aktualizací. Obvykle každý program sám zjišťuje dostupnost akualizací. V tomto případě jsou ale PUSH aktualizace vyvolány naším serverem, což má za nsledek velmi rychlou odezvu a zjednodušení celého procesu. Systém je založen na protokolu SMTP (stejný jako se používá pro emailové zprávy). Samotná aktualizace je poté kontrolována emailovými poskytovateli MS Outlook nebo Internet Mail. Celý system je chráněn asymetrickými čísly a je chránět proti případnému zneužití.

Rozšířené uživatelské rozhraní

avast! antivirus Professional Edition nabízí rozšířené uživatelské rozhraní, z kterého je možné naplánovat a vytvářet “Úlohy” podle svých potřeb. Například naplánovat úlohu na vybraný čas, v denních, týdenních či měsíčních intervalech. Nová “Seance” se vytvoří kdykoliv spustíte vybranou úlohu a uloží se v ní výsledky testu, které si poté můžete prohlédnout. Dále si můžete zvolit jakou akci avast! provede v případě, že detekuje virovou infekci a zvolit náhradní akci v případě, že první nebyla úspěšná. (např. Opravit soubor a pokud není úspěšné, tak Přesunout soubor do truhly). Více informací o rozšířeném rozhraní naleznete na **straně 49**.

Systémové požadavky

Pro počítač s operačním systémem Windows 95/98/Me: PC 486, 32 MB RAM, 50 MB volného místa na pevném disku

Pro počítač s operačním systémem Windows NT 4.0: PC 486, 24 MB RAM, 50 MB volného místa na pevném disku, Service Pack 3 nebo vyšší

Pro počítač s operačním systémem Windows 2000/XP Stanice (ne server): PC Pentium, 64 MB RAM (128 MB doporučeno), 50 MB volného místa na pevném disku

Pro počítač s operačním systémem Windows Vista: Pentium 4, 512MB RAM, 50 MB volného místa na pevném disku

Program samotný vyžaduje asi 20 MB volného místa na disku, zbytek je vyhrazen pro VRDB (databáze pro obnovu, známá též jako "databáze integrity" z předchozí verze).

Je vyžadována **funkční instalace MS Internet Explorer 4** nebo vyšší.

Tento produkt **nemůže být instalován na serverový operační systém** (rodiny Windows NT/2000/2003 Server).

Poznámka: Nedoporučujeme instalovat na Váš počítač více než jedno antivirové řešení. Pokud je takový program již nainstalován , prosím odstraňte ho spolu se všemy jeho zbytky ještě před instalací programu avast!.

Jak nainstalovat avast! antivirus Professional Edition

V této části se dozvíte jak avast! nainstalovat a jak ho poté aktivovat (vložit licenční klíč do programu). Snímky obrazovky na následujících stránkách jsou pořízeny na operačním systému Windows XP za použití prohlížeče Internet Explorer, mohou se tedy ve verzi Vašeho operačního systému nebo prohlížeče lišit.

avast! antivirus Professional Edition si můžete nahrát z webové stránky **www.avast.com**.

Před stahováním programu doporučujeme ukončit všechny ostatní běžící aplikace.

Klikněte na "ke stažení", poté "Programy" a zvolte verzi programu, kterou si chcete nahrát.

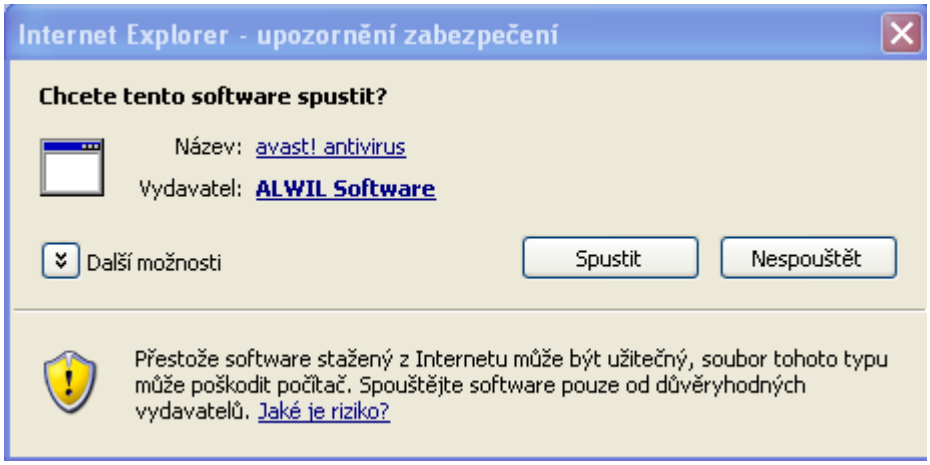
Ze seznamu v tabulce si vyberte jazykovou verzi, kterou potřebujete (viz. Níže) a klikněte na tlačítko "Download".

avast! 4 Professional Edition

Download avast! 4 Professional - **česká** verze (délka 26.27 MB)
Download avast! 4 Professional - **arabská** verze (délka 26.23 MB)
Download avast! 4 Professional - **anglická** verze (délka 26.43 MB)
Download avast! 4 Professional - **bulharská** verze (délka 26.27 MB)

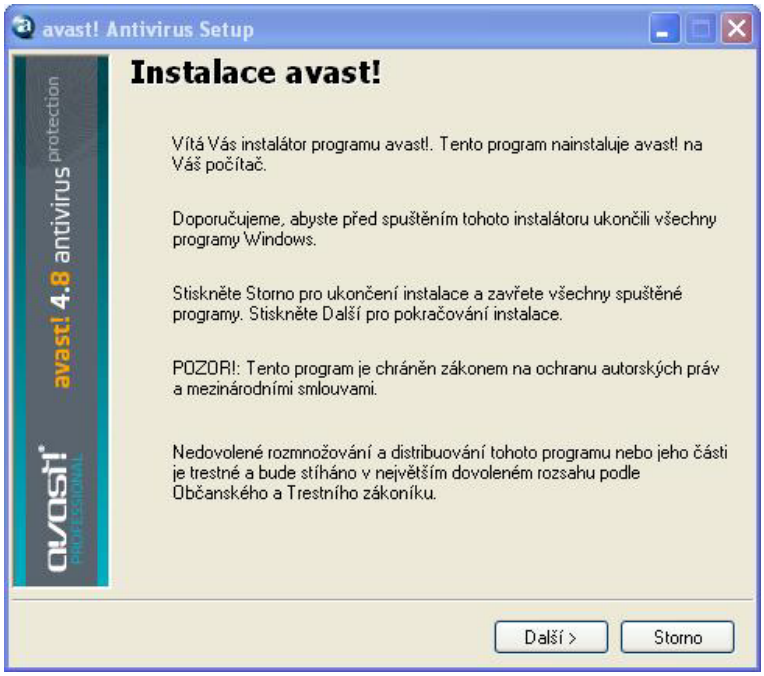
Klikněte buď na "Spustit" či "Uložit". Instalační soubor "setupczepro.exe" se začne nahrávat na Váš počítač.

Po skončení stahování se zobrazí toto okno:



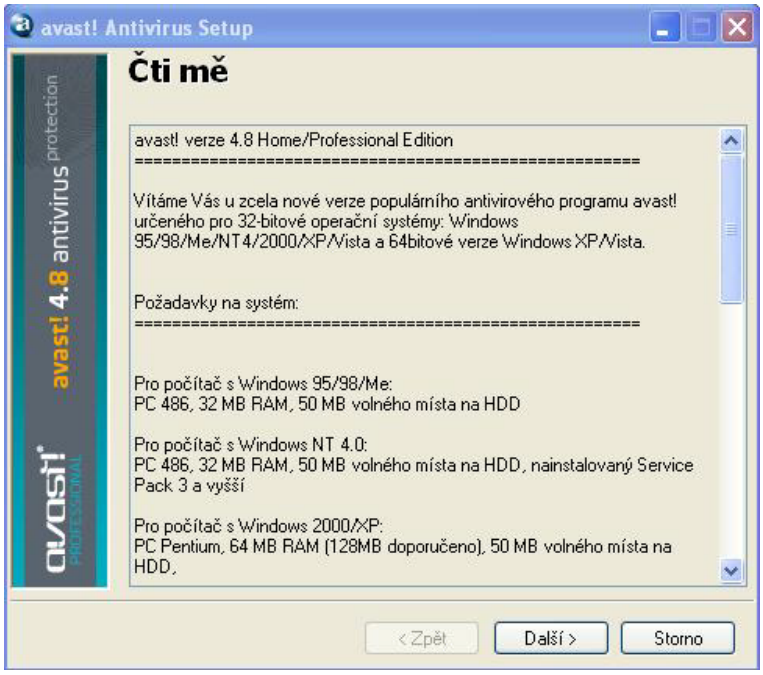
V ostatních webových prohlížečích může být pouze možnost "Uložit" soubor. Pokud kliknete na Uložit, soubor pouze uložíte a instalace se automaticky nespustí. Soubor proto po uložení na disk spusťte.

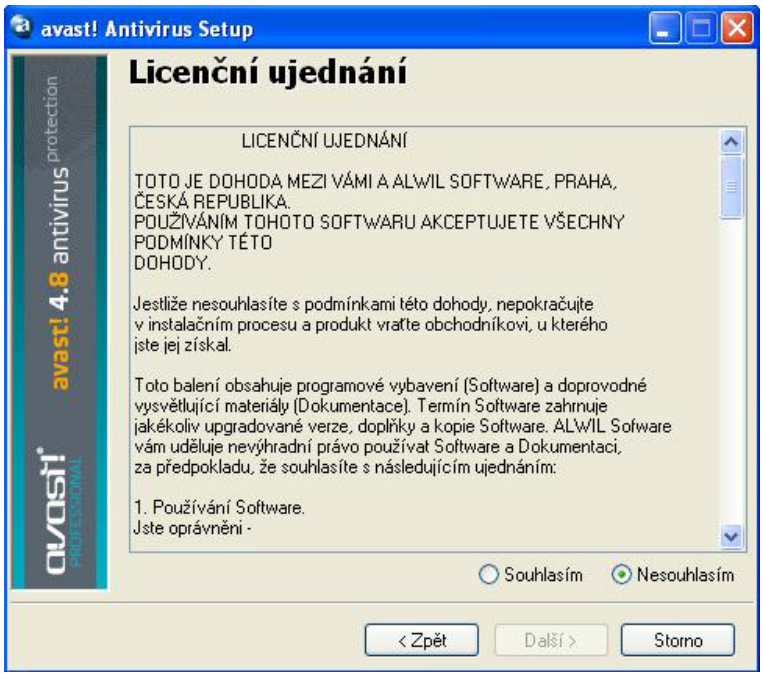
Kliknutím na tlačítko "Spustit" se dostanete do okna avast! Antivirus Setup:



Po kliknutí na tlačítko "Další" Vás instalační průvodce provede zbytkem procesu instalace.

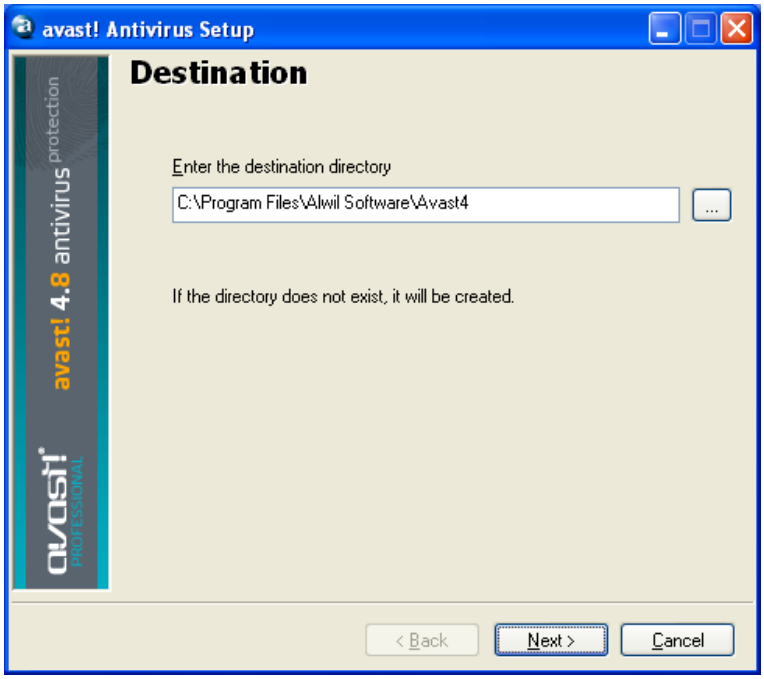
Nejprve se zobrazí okno s minimálními systémovými požadavky a poté budete požádáni o souhlas s licenční smlouvou pro koncového uživatele.





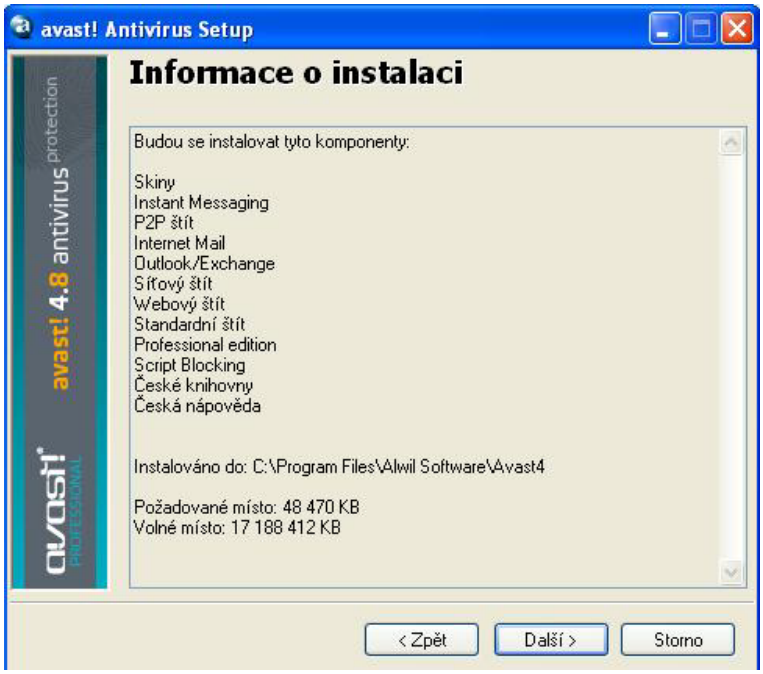
K úspěšnému pokračování je nutné kliknout na “Souhlasím” a poté “Další”.

Poté budete požádán o potvrzení cílového adresáře, kam se program uloží. Doporučujeme použít cílový adresář, který je původně přednastavený a kliknout na "Další".



V následujícím okně můžete zvolit nastavení komponent programu. Běžné nastavení je automaticky předkonfigurováno. Pokud nechcete žádnou položku změnit (např. jazykovou verzi), klikněte na tlačítko "Další".

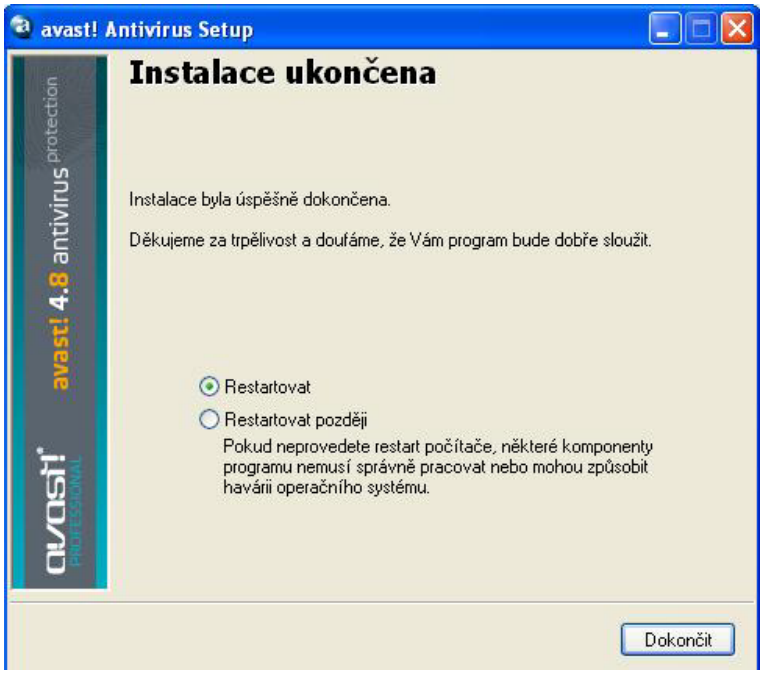
V dalším okně program potvrdí jaké komponenty bude kam instalovat. Znovu klikněte na tlačítko "Další".



Poté Vám bude nabídnuto naplánovat úlohu po startu systému – více informací naleznete na straně 35.

V posledním okně potvrdíte úspěšnou instalaci programu. K tomu je potřeba počítač restartovat.

Zvolte "Restartovat" a klikněte na tlačítko "Dokončit". Váš počítač bude automaticky restartován.



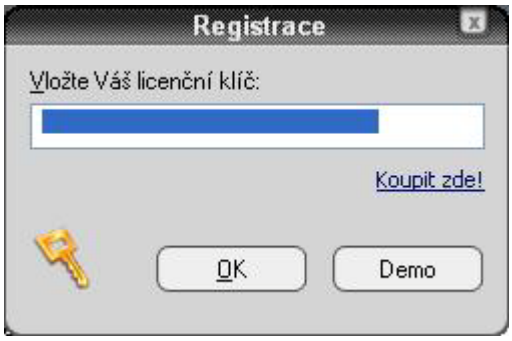
Nyní je instalace kompletně dokončena.

První kroky s programem

Po restartu počítače by se měla v systémové liště objevit modrá ikona avastu.

avast! Antivirus Professional Edition může být používán 60 dní jako zkušební verze, poté je nutno zakoupit licenční klíč.

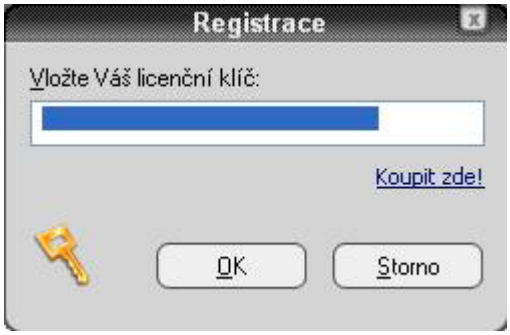
První okno, které se objeví po startu počítače vypadá takto:



Není nutné ihned do programu vkládat licenční klíč. Pokud chcete program použít jako zkušební verzi na 60 dní, klikněte na tlačítko "Demo". Nebo můžete přímo zažádat o licenční klíč k plné verzi, v tomto případě klikněte na "Koupit zde!".

Pokud jste se rozhodli pro spuštění demo verze, okno registrace se již znovu nezobrazí. Zaregistrovat program můžete ale kdykoliv. Další informace o registraci jsou uvedeny na následujících stránkách. Pokud si avast! nezaregistrujete ani ve zkušební lhůte 60 dnů, zobrazí se Vám varovná zpráva o vypršení licence. Při startu programu se pak zobrazí toto okno:

Po kliknutí na tlačítko "OK" budete moci znovu zadat licenční klíč do stejného registračního okna:



Následující stránky podrobně popisují proces získání a vložení licenčního klíče do programu.

Ochrana heslem

Pokud chcete změnit předem definované heslo k programu, klikněte pravým tlačítkem myši na modrou ikonu avast! v systémové liště a zvolte “Nastavit/změnit heslo”.

Jak zakoupit program avast! 4 Professional

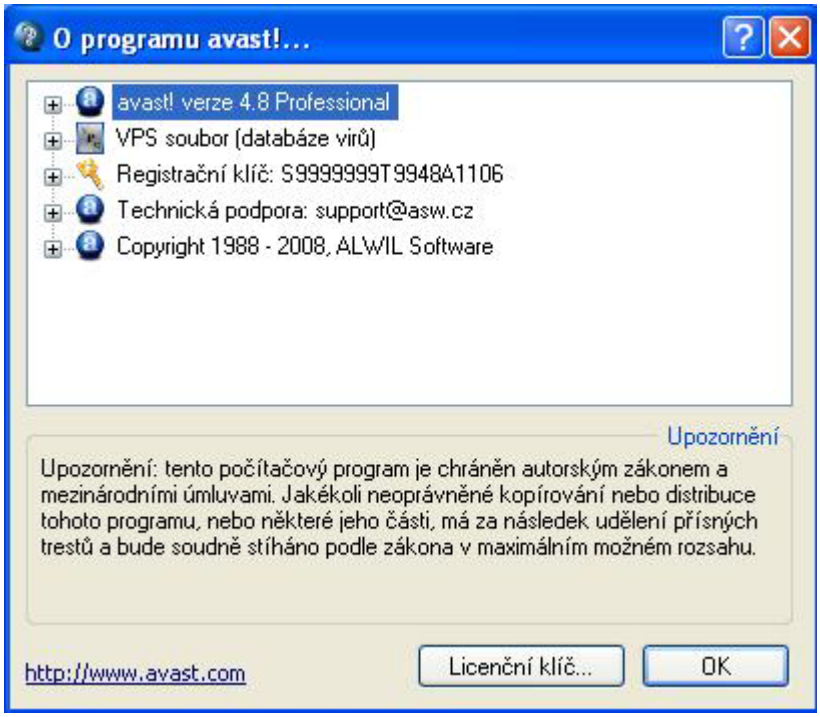
Pokud si přejete program používat i po zkušební době, je nutné zakoupit platný licenční klíč a vložit ho do programu. Licenční klíč pro avast! antivirus Professional Edition je nabízen na dobu 12, 24 nebo 36 měsíců.

avast! 4 Professional můžete v ČR zakoupit prostřednictvím firmy ALWIL Trade.

Více informací o všech produktech, platebních podmínkách a ceníkách naleznete na stránce www.alwil.com.

Licenční klíč Vám bude do 24h po koupi zaslán.

Jestliže už máte program nahraný a nainstalovaný, klikněte pravým talčítkem myši na modrou ikonu a v systémové liště a zvolte “O programu avast!...”



Klikněte na tlačítko Licenční klíč, zobrazí se Vám okno s možností Koupit zde!, která Vás zavede na naše webové stránky s informací, jak naše produkty zakoupit.

Vložení licenčního klíče

Poté co obdržíte licenční klíč, vložte ho do programu avast! .Tím ho zaktivujete. Atualizace se budou nadále provádět automaticky a přestanou se zobrazovat varovná okna.

Nezapoměňte, že před vkládáním licenčního klíče musí být program na počítači nainstalován.

Postupujte podle těchto kroků:

1. Označte licenční klíč v emailu, který jste od nás obdržel. Umístěte kurzor myši na začátek klíče a stiskněte levé tlačítko myši. Mějte ho stisknuté a táhněte přes celý klíč. Tím ho označíte. Na označený klíč klikněte pravým talčítkem myši a zvolte “Kopírovat”.

2. Klikněte pravým tlačítkem myši na modrou ikonu avastu v systémové liště a zvolte “O programu avast!...”

3. Klikněte na tlačítko "Licencční klíč..." vlevo dole.

4. Přesuňte kurzor do kolonky licenčního klíče, stiskněte pravé tlačítko myši a ze zobrazené nabídky vyberte “Vložit”. Licenční klíč je nyní vložen do programu.

5. Klikněte na tlačítko “OK” . avast! bude aktivován na 14, 26 či 38 měsíců ode dne jeho zakoupení. Po vypršení této lhůty bude třeba licenci znovu zakoupit a vložit nový klíč do programu.

Základy užívání programu avast! antivirus

avast! poskytuje ochranu proti všem typům malware. Obsahuje součásti, které lze od kvalitního, profesionálního antivirového programu očekávat. Samozřejmostí je rezidentní ochrana, která

sleduje všechny potencionálně nebezpečné operace prováděné při běžné práci s počítačem, jako je například spouštění souborů, a brání tak virové infekci.

Avast! poskytuje dva druhy ochrany proti virům, residentní ochranu a test na vyžádání. Residentní ochrana Vás chrání v reálném čase, je aktivována po instalaci programu. Test na vyžádání lze spustit ze samotného programu. Nejprve je třeba zvolit oblast, ve které bude avast! hledat viry. K tomu slouží tři tlačítka pro volbu oblastí – "Média", "Složky" a "Lokální pevné disky".

Avast! Antivirus také nabízí speciální šetřič obrazovky, který Váš počítač testuje vždy, když se zapne.

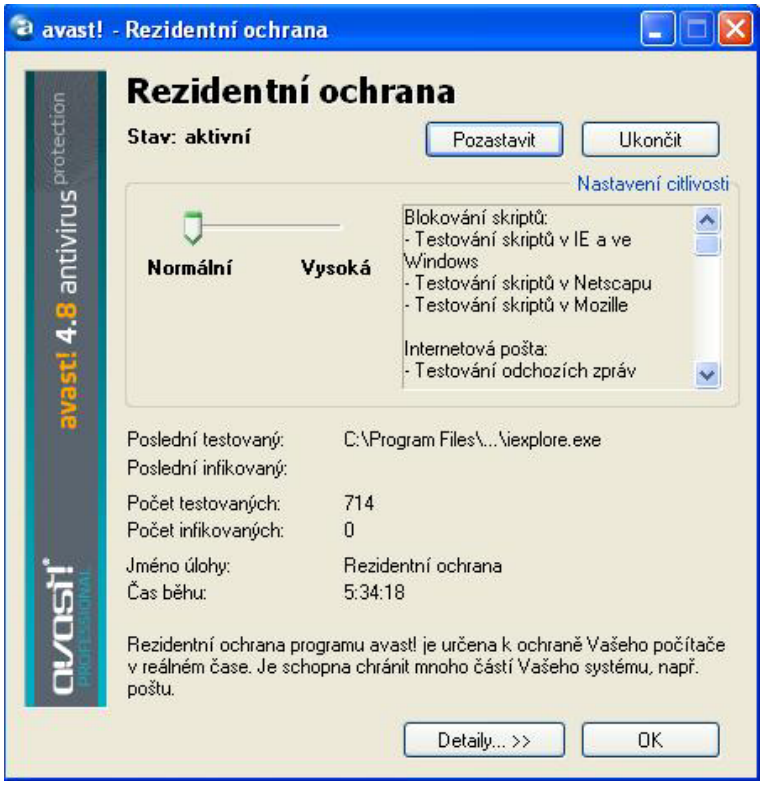
Residentní ochrana

Rezidentní ochrana je typ speciální úlohy, která sleduje (dle nastavení) všechny spouštěné aplikace či otvírané dokumenty, a účinně tak brání infikování počítače v reálném čase. Běží zcela nezávisle. Aktivuje se po startu počítače. Pokud funguje bez problémů, tak její běh vůbec nezaznamenáte.

Modrá "a" ikona v systémové liště ukazuje stav residentní ochrany. Přítomnost a ikony znamená, že tato ochrana je nainstalovaná, a že je funkční. Pokud ikonu překrývá červený pruh, residentní ochrana funkční není a Váš počítač není chráněn. Pokud je šedá, residentní ochrana byla pozastavena (viz. níže).

Pro nastavení residentní ochrany klikněte na modrou ikonu v systémové liště, nebo na ni klikněte pravým tlačítkem myši a zvolte "Zobrazit okno residentní ochrany".

Zobrazí se následující okno:



V tomto okně můžete residentní ochranu dočasně pozastavit či ukončit kiknutím na tlačítka "Pozastavit" nebo "Ukončit". Obě možnosti jsou stejné, po restartu bude residentní ochrana znovu aktivována. Počítač je tak chráněn proti nechtěnému vypnutí residentní ochrany.

Můžete zde i nastavit citlivost residentní ochrany pohnutím jezdce z Normální na Vysokou nebo naopak. Residentní ochrana se skládá z více poskytovatelů a každý z nich má na starosti něco jiného, viz. následující strana. Jakákoliv změna provedená v tomto okně bude aplikována na všechny poskytovatele.

Residentní ochrana se skládá z těchto poskytovatelů:

Poskytovatel **Instant Messaging** slouží k ochraně komunikačních programů (jako jsou např. ICQ, Skype či MSN messenger). Mnohé komunikační programy mají možnost posílat a přijímat soubory od jiných uživatelů. Tímto způsobem lze velice snadno získat infikovaný soubor a šířit jej dále. Některé viry se prostřednictvím těchto programů dokáží šířit i bez vědomí uživatele. Infekci počítače pak dokáže zamezit právě poskytovatel Instant Messaging, který kontroluje adresáře, v nichž se přijaté a odeslané soubory ukládají.

Poskytovatel **Internet Mail** slouží k ochraně elektronické pošty spravované jinými e-mailovými klienty, než jsou MS Outlook a MS Exchange.

Síťový štít chrání počítač před útoky Internetových červů (Blaster, Sasser, atd). Jeho činnost je velmi podobná jednoduchému firewallu, jejž však plně nenahrazuje. Síťový štít nevyžaduje interakci s uživatelem. Je k dispozici pouze na operačních systémech Windows NT (2000, XP, Vista nebo 2003).

Poskytovatel **Outlook/Exchange** se týká pouze poštovních klientů MS Outlook a MS Exchange. Nastavení ostatních poštovních klientů, jako je Outlook Express, Eudora apod., se provádějí konfigurací poskytovatele Internet Mail.

Poskytovatel **P2P štít** (Peer To Peer) slouží k ochraně programů pro sdílení souborů jako je CZDC++, uTorrernt atd. Riziko, že soubor získaný pomocí Peer-To-Peer služeb bude infikovaný, je poměrně vysoké.

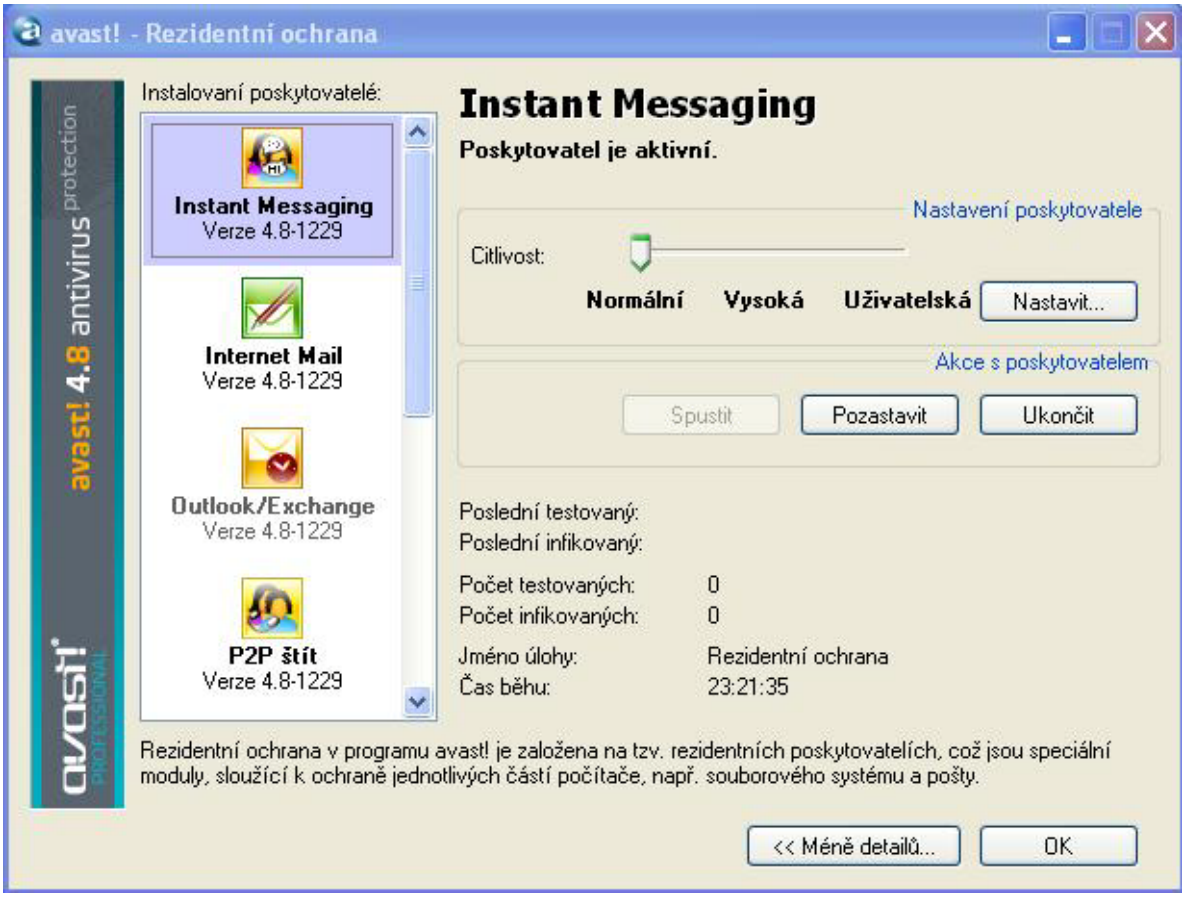
Poskytovatel **Script blocking** slouží k ochraně před skriptovými viry na internetových stránkách.

Standardní štít kontroluje programy, které spouštíte, a soubory, ke kterým přistupujete. Díky němu tedy není možné spustit infikovaný program (virus).

Poskytovatel **Webový štít** slouží k ochraně před viry, které by se do Vašeho počítače mohly dostat při běžné práci s Internetem, zejména při stahování nejrůznějších souborů z webových stránek.

Webový štít pracuje jako transparentní HTTP proxy a je kompatibilní s většinou internetových prohlížečů, včetně programů Microsoft Internet Explorer, Mozilla Firefox, Mozilla Suite a Opera. Na rozdíl od většiny obdobných řešení je dopad Webového štítu na rychlost prohlížení webu prakticky zanedbatelný. To je možné díky jedinečné vlastnosti zvané Inteligentní proudové testování, která umožňuje skenování objektů okamžitě při přístupu bez potřeby kešování. Proudové testování je prováděno v operační paměti (bez nutnosti ukládat obsah na disk), díky tomu je možné dosahovat vysokých datových toků.

Další možností je nastavit každého poskytovatele individuálně. Klikněte na tlačítko “Detaily…”, okno se rozšíří a zobrazí následující nabídku:



V rozšířeném okně jsou jednotliví poskytovatelé zobrazeni v levé části. Změnu citlivosti nastavení provedete posunutím jezdce na pravé straně v Nastavení poskytovatele, předtím ale vybraného poskytovatele označte v levé části okna. Také můžete dočasně pozastavit či ukončit poskytovatele kliknutím na tlačítko “Pozastavit” či “Ukončit”. Pozastavení poskytovatele automaticky zaktivuje po restartu počítatče. Pokud vyberete “Ukončit”, program Vás požádá o potvrzení Vaší volby(viz. strana 84). Když i poté kliknete na “Ano”, poskytovatel zůstane vypnut i po restartu počítače.

Kliknutím na “Nastavit” zobrazíte další širokou nabídku rozšířených nastavení (např. druh souborů, které budou testovány). Další informace o nastavení naleznete na straně 67 .

Jak spustit test na vyžádání v jednoduchém uživatelském rozhraní

Po spuštění programu se Vám avast! Zobrazí jako stříbrný rádio/CD přehrávač. Obsahuje všechny tlačítka pro definování, spuštění a zobrazení výsledků antivirového testu – viz. obrázek níže. Toto je základní, přednastavený vzhed, který může být změněn. Více naleznete na straně 28).

Před spuštěním programu se zobrazí informační okno jednoduchého rozhraní, které obsahuje pět bodů. Pro detailní zobrazení obsahu klikněte na "Více informací" u každého bodu. Zpět se vrátíte kliknutím na odkaz "Titulní stránka". Do titulního informačního okna jednoduchého rozhraní se můžete kdykoliv vrátit klinutím na tlačítko "Menu" a poté "Úvodní nápověda".

Textové okno jednoduchého rozhraní zobrazuje současný stav programu:

- ***Současná verze virové databáze*** – virová databáze obsahuje vzorky částí kódů všech známých virů a používá je k identifikaci všech podezřelých souborů.
- ***Residentní ochrana*** – zde můžete zkontrolovat nastavení citlivosti rezidentní ochrany.
- ***Datum posledního testu*** – Datum, kdy byl poslední antivirový test proveden.
- ***Databáze pro obnovu (VRDB)*** – Zobrazuje datum, kdy byla naposled vytvořena. Slouží k léčení napadených souborů.
- ***Automatická aktualizace*** – ukazuje nastavení aktualizací virové databáze a programu. Změnit se dá kliknutím na stav aktualizací (např. Pouze databáze). Více naleznete na straně 34.

Na každé straně okna jednoduchého rozhraní jsou umístěna tři tlačítka:

- **Vlevo nahoře –** zobrazí okno Virové truhly. Více informací o práci s virovou truhlou naleznete na straně 45.
- **Vlevo uprostřed** - zobrazí lištu s jezdcem, jehož posouváním můžete měnit úroveň rezidentní ochrany. Tyto úrovně jsou celkem tři: v levé poloze je rezidentní ochrana zcela **vypnuta**. **Standardní** úroveň je nastavena jako výchozí. avast! kontroluje všechny otevírané soubory. Je-li jezdec zcela vpravo, je úroveň rezidentní ochrany **důkladná**, což znamená, že jsou kontrolovány i všechny vytvářené a měněné soubory. Viz. strana 22

- **Vlevo dole** – Spustí se aktualizace virové databáze z Internetu (iAVS).
- **Pomocí tří tlačítek napravo vybíráte co chcete testovat.**
- **Tlačítko START**. Spustí prohledávání předem vybrané oblasti. Tlačítko se poté změní na **PAUSE.**
- **Tlačítko PAUZA**. Dočasně pozastaví prohledávání. (V toto tlačítko se změní tlačítko **START** po spuštění prohledávání).
- **Tlačítko STOP**. Ukončí prohledávání.

  Kliknutí na tlačítko vlevo nahoře ,vypadající jako tlačítko "***Eject***", zobrazí nabídku Menu jednoduchého rozhraní**.** Stejnou nabídku zobrazíte kliknutím pravým talčítkem myši kamkoliv v okně jednoduchého rozhraní.

  Pokud používáte program bez vzhledu (skinu – viz. strana 28), k nabídce jednoduchého rozhraní se dostanete přes "Nástroje" či "Nastavení" v horní liště.

  Některé z nabídky Menu mohou být zobrazeny přímo ze systémové lišty kliknutím pravým tlačítkem myši na modrou ikonu a.

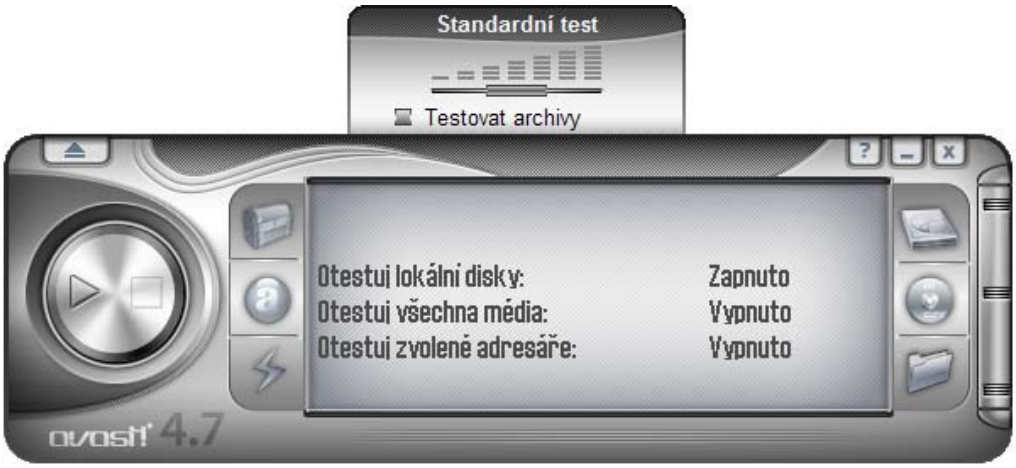
  Všechny dostupné nabídky programu jsou blíže popsány v tomto manuálu.

Volba oblasti testu na vyžádání.

Před spuštěním testu musíte zvolit, jaké soubory chcete testovat.

- ***Test lokálních pevných disků***

  Pokud chcete jednoduše otestovat vše na svém počítači (včetně všech hard-disků a souborů), klikněte na tlačítko vpravo nahoře. Informační okno jednoduchého rozhraní bude nahrazeno novým – viz. níže. Pro navrácení k původnímu oknu klikněte pravým tlačítkem myši kamkoliv a zvolte "Stav programu".



  V okně u Otestuj lokální disky se stav změní z "Vypnuto" na "Zapnuto".

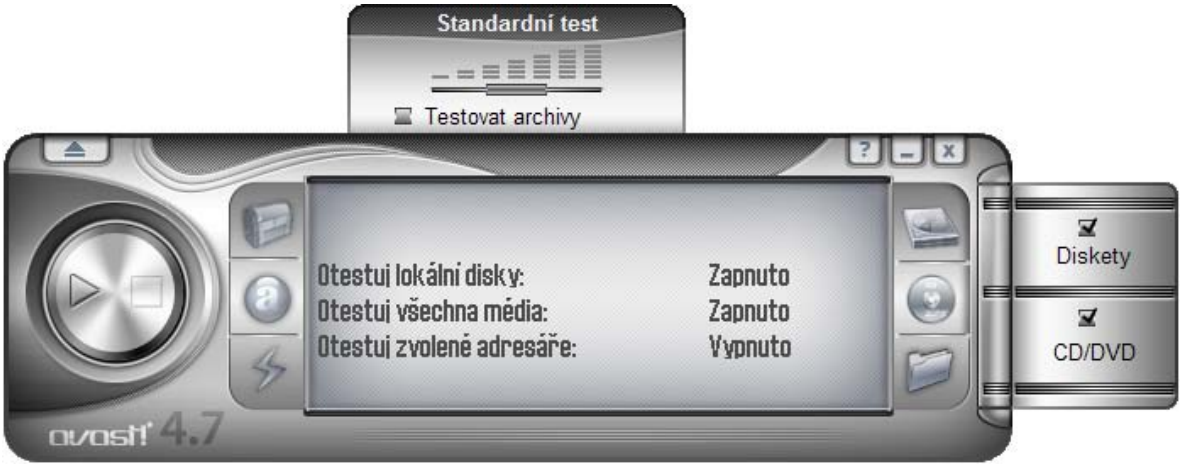
  Nad ním se objeví menší okno Standratního testu. Zde můžete nastavit citlivost testu, zobrazí se lišta s jezdcem. Změnou jeho polohy měníte úroveň testování. Tyto úrovně jsou celkem tři. Můžete zaškrtnout i možnost testu komprimovaných souborů. Tyto možnosti jsou blíže popsány na následujících stranách.

- ***Testování médií***

Tímto tlačítkem volíte, zda se budou testovat záznamová média v jednotkách CD-ROM, DVD-ROM nebo v disketových mechanikách (případně ve všech). Volbu provedete zatržením příslušné položky.

Stav testu všech médií se změní z "Vypnuto" na "Zapnuto".

Na pravé straně se znovu objeví další okno, ve kterém zvolíte jaký typ média chcete testovat.



- ***Volba adresáře***

  Poslední možností je tlačítko vpravo dole. Zde můžete vybrat přímo určitou složku (adresář). Zobrazí se stromová struktura, kde označíte jednu nebo více složek, které chcete kontrolovat. Rovněž je možné příslušný adresář s kompletní cestou k němu přímo vypsat do řádku v dolní části okna. Takto vypsané cesty ke složkám uzavřete uvozovkami. Je-li jich více, oddělte je středníkem. Např. **`"C:\Windows";"C:\Program Files"`**.

  Také je možné kombinovat více typů testu (např. všechny hard-disky spolu s testem médií).

Nastavení úrovně testování a spouštění testu

Při výběru testované oblasti můžete také nastavit úroveň testu a zvolit zda bude prohlížet i archivované soubory (zip, rar, atd.). Nejpre vyberte testovanou oblast a poté zaškrtněte položku "Testovat archivy". Citlivost testu ovlivní, jak důkladný bude. Vybrat si můžete z následujících možností:

- ***Rychlý test.*** Testují se pouze potencionálně nebezpečné soubory na základě jejich přípony. Kontrolují se tedy soubory s příponami EXE, SCR, COM, DOC apod. V takových souborech *avast!* hledá pouze odpovídající typ viru. To znamená, že např. v souborech EXE nehledá makroviry apod.

- ***Standardní test.*** Testují se pouze potencionálně nebezpečné soubory na základě jejich obsahu. Přípona souboru tedy nerozhoduje o tom, zda daný soubor bude či nebude zkontrolován. I zde *avast!* hledá pouze odpovídající typ viru.

- ***Důkladný test.*** Testují se všechny soubory na přítomnost všech typů virů. Tento test je vysoce spolehlivý, trvá daleko déle než předchozí testy.

Poté co označíte oblast testování, klikněte na "Play" tlačítko pro přehrávání, čímž se test spustí.

Jiná metoda

Klikněte na **Menu jednoduchého rozhraní** a zvolte první položku "Spustit test". I zde můžete volit typ testu a testovanou oblast, stejně jako v okně jednoduchého rozhraní.

Spouštění testu a zobrazování výsledků

Po výběru oblasti a nastavení úrovně testování spustíte samotné hledání pomocí tlačítka **START**. Toto tlačítko se po dobu testování změní na tlačítko **PAUZA**, kterým hledání pozastavíte. Tlačítkem **STOP** jej ukončíte úplně. Tento proces může zabrat hodně času, záleží hlavně na velikosti testovaných dat a na rychlosti Vašeho počítače.

Po spuštění antivirového testu můžete ve své prácí na počítači pokračovat. K tomu doporučujeme minimalizovat okno jednoduchého rozhraní. V opačném případě by se mohla rychlost počítače velmi zpomalit. Okno zpět vyvoláte jednoduše kliknutím na minimalizované okno na spodní liště.

Pokud antivirový test skončil a žádný virus nebyl nalezen, zobrazí se v jednoduchém rozhraní informace o skončeném testu (jako např. počet testovaných souborů/adresářů, celková doba testování, atd.).

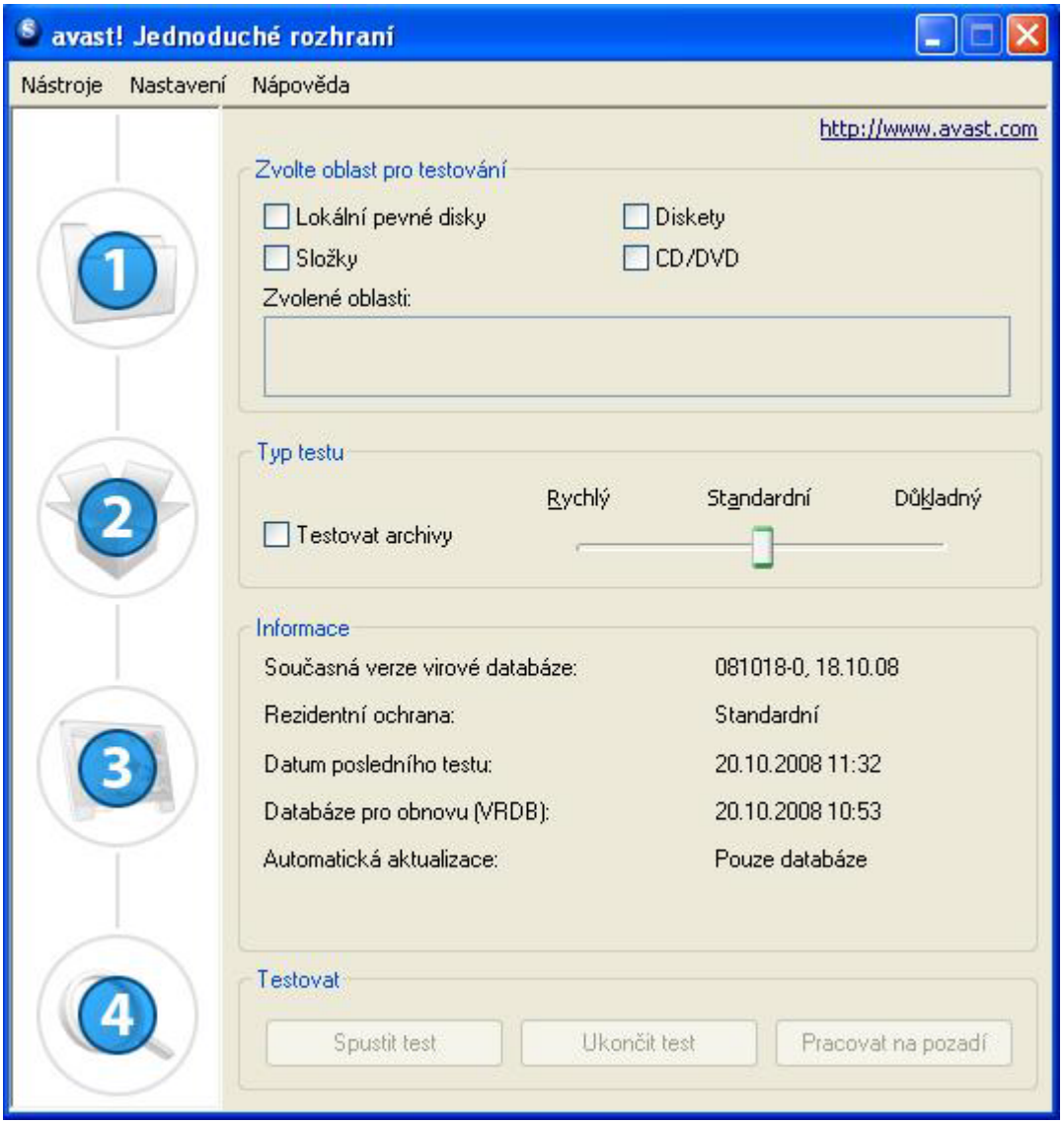
Pokud je nějaký virus nalezen, program se Vás zeptá, co s ním má udělat. Na výběr je několik možností, např. přesunout soubor do **Virové truhly**, smazat ho, přejmenovat nebo ho přesunout. Někdy je možné soubor i opravit. žádnou akci provádět nemusíte, ale může to vést k rozšíření infekce a způsobení dalších problémů. Všechny možnosti odstraňování virů jsou blíže popsány v další části "**Co dělat, pokud byl nalezen virus**".

Změna vzhledu v jednoduchém uživatelském rozhraní

V jednoduchém uživatelském rozhraní si můžete vybrat z množství jednotlivých vzhledů (skinů). Tři vzhledy jsou nabízeny v základní verzi, ostatní si můžete nahrát z Internetu – klikněte pravým tlačítkem myši kdekoliv v jednoduchém rozharní a z **Menu jednoduchého rozhraní**, vyberte "Změnit vzhled (skin)" a potom "Získejte více skinu z Internetu".

Další možností je použití programu zcela bez skinu. V tomto případě v "Nastavení" odšrtněte položku "Používat skiny pro Jednoduché rozhraní programu avast!". Pro obnovení původního nastavení klikněte na "Nastavení" v horní liště, potom znovu na "Nastavení" a zaškrtněte "Používat skiny pro Jednoduché rozhraní programu avast!". Skin se při dalším startu programu znovu objeví.

Vzhled jednoduchého uživatelského rozhraní bez skinu:



Oblast testování můžete zvolit zaškrtnutím příslušných polí pod položkami "Zvolte oblast pro testování". Citlivost testu změníte posunutím jezdce mezi možnostmi Rychlý, Standartní a Důkladný. Na stejném místě můžete také zaškrtnout možnost "Testovat archivy".

Po spuštění testu můžete pracovat i s dalšími aplikacemi na počítači. K tomu klikněte na tlačítko "Pracovat na pozadí".

K nastavení rezidentní ochrany přistoupíte kliknutím na tlačítko "Nastavení", a potom "Residentní ochrana". Jezdcem ji můžete přepínat z "Vysoké" na "Standartní" či "Nečinnou". Jak již bylo

zmíněno v předešlých kapitolách, toto nastavení bude aplikováno na všechny rezidentní poskytovatele současně. Nastavení jednotlivých poskytovatelů je blíže popsáno na **straně 22**.

K dalším částem programu, jako je např. Virová truhla, se dostanete kliknutím na "Nástroje" v horní liště a vybráním požadované položky. Ty jsou detailně popsány na následujících stranách manuálu.

Informace o stavu programu se nacházejí ve spodní polovině okna. Jsou blíže popsány v předchozí části.

Co dělat, pokud byl nalezen virus

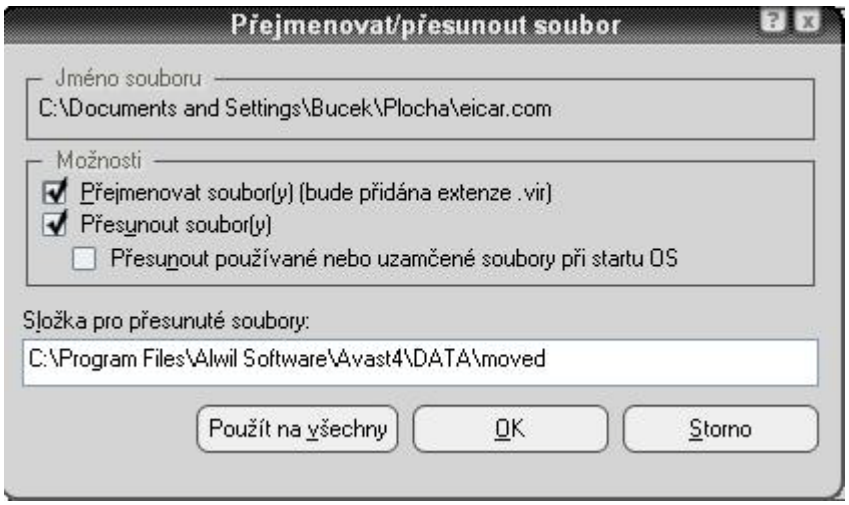
Pokud program najde podezřelý soubor, test se přeruší a objeví se okno s následující nabídkou:

Pokud kliknete na "Pokračovat", program neprovede nic. Vše bude zobrazeno na konci ve výsledcích testu – viz. **strana 33**. Kliknutím na "Ukončit" test ihned vypnete.

Pokud bude virus nalezen některým z residentních poskytovatelů, zobrazené okno bude trochu odlišné. Tlačítka "Pokračovat" a "Ukončit" jednoduše nahradí možnost "Žádná akce" (či "Přerušit spojení" v případě Webového štítu). Jestliže na tlačítko kliknete, infikovaný soubor zůstane na svém místě, ale nebude aktivován.

Máte na výběr ze čtyř dostupných akcí:

Možnost 1: Přesunout soubor na jiné místo na počítači. Soubor můžete i přejmenovat. Následující okno se objeví po kliknutí na tlačítko "Přesunout/přejmenovat".



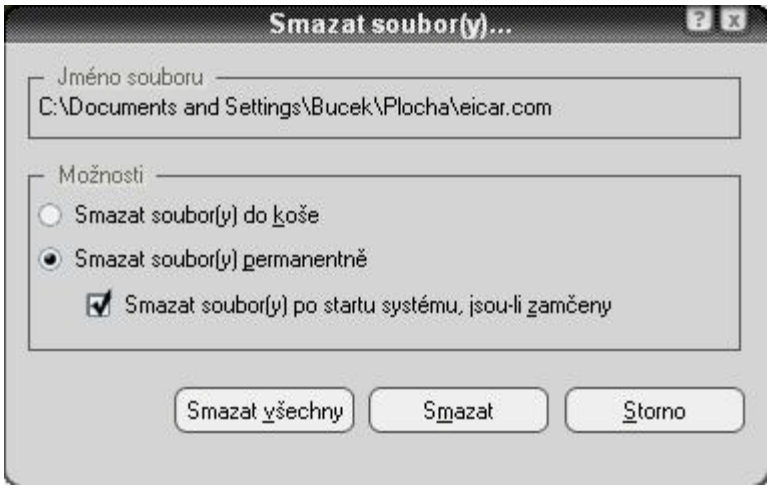
Do bílého okna můžete napsat složku, kam chcete přesouvaný soubor umístit. Program automaticky přednastaví výše uvedený podadresář.

Pokud zaškrtnete i "Přejmenovat soubor(y)", k souboru se přidá koncovka ".vir". To poslouží k lepší identifikaci souboru a předejití potencionálních problémů.

Pokud není možné soubor přesunout, např. protože je používán jiným procesem, můžete zaškrtnou možnost "Přesunout používané nebo uzamčené soubory při startu OS".

Poznámka - Přesouvání systémových nebo jinak důležitých soborů může vést k systémové chybě při příštím startu počítače. Pokud soubor přesunete do Virové truhly, bude pak možno v případě potřeby soubor znovu přesunout na jeho původní místo na disku. Více informací naleznete na straně 8.

Možnost 2: Smazat soubor – Po kliknutí na tlačítko "Smazat" se objeví následující okno:



Máte více možností virus smazat.

- ***Smazat soubor(y) do koše***

Soubory budou přesunuty do koše. Nebudou nenávratně smazány.

- ***Smazat všechny***

Smaže automaticky všechny nalezené soubory. Ty už později nemohou být obnoveny.

- ***Smazat soubor(y) pernamentně***

Smaže soubor z Vašeho počítače bez možnosti obnovení souboru. Smazán bude pouze infikovaný soubor. Může se stát, že vir vytvoří soubory, které vir neobsahují a program je jako podezřelé detekovat nebude. Tyto soubory budou pouze zabírat místo na hard disku, ale nepředstavují žádné nebezpečí.

Pokud bude moci program použít zabudovaný nástroj Virus Cleaner, objeví se další tlačítko – "Kompletně odstranit virus z počítače". Pokud je toto tlačítko dostupné, doporučujeme ho použít.

Jestliže není možné soubor smazat (např. protože je využíván jiným procesem), můžete zaškrtnout položku "Smazat soubor(y) po startu systému, jsou-li zamčeny", virus bude smazán při dalším startu počítače. K potvrzení akce potom klikněte znovu na tlačítko "Smazat".

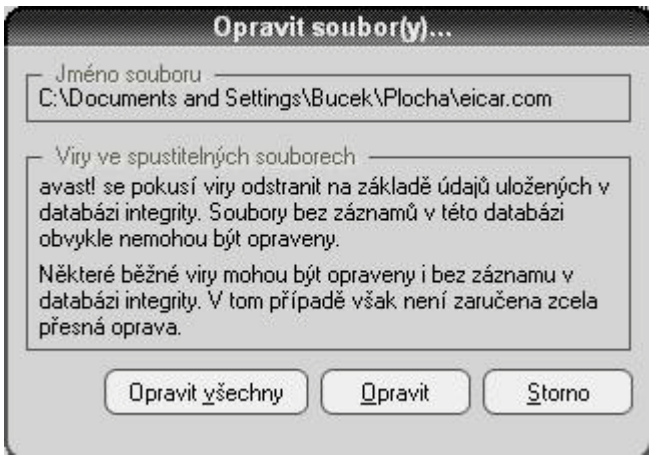
Poznámka – v případě infekce systémového souboru nebo důležitého programu se může stát, že systém či program nebude správně fungovat. Před odstraňováním souboru si musíte být jist, že není systémový nebo, že ho případně můžete obnovit ze zálohy.

Pokud si tím nejste jisti, doporučujeme Vám přesunout soubor do truhly. V truhle budou soubory odděleny od zbytku systému.

V případě infekce nemohou způsobit žádné poškození Vašemu počítači. Pokud zjistíte, že soubor škodlivý není, můžete ho přesunout zpět na své původní místo. Viz. strana 8.

Možnost 3: Opravit soubor(y).

Následující okno se objeví po kliknutí na tlačítko "Opravit":



Pokud kliknete znovu na "Opravit", program se pokusí soubor obnovit do původního stavu.

K této obnově používá tzv. databázi pro obnovu (VRDB). Pokud je v databázi dostatek informací o obnovaném souboru, může být většinou opraven. Mějte na paměti, že mohou být opraveny pouze soubory, které byly virem fyzicky měněny. Pokud vir vytvořil soubory nové, může je smazat pouze nástroj Virus Cleaner – viz. Možnost 2.

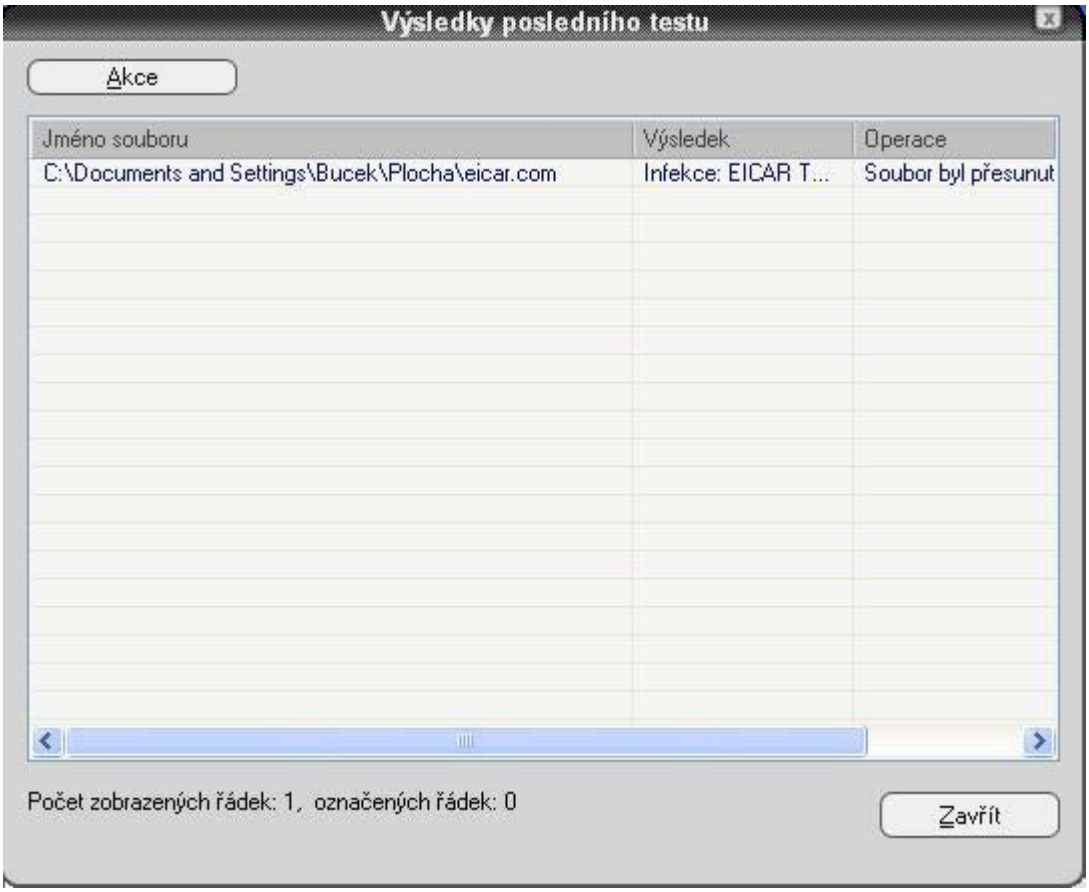
Pro aktualizaci VRDB klikněte pravým talčítkem myši na modrou ikonu "I" v systémové liště a zvolte "Spustit generování VRDB ihned". Databáze bude aktualizována s dalšími detaily o programech, které byly od poslední aktualizace instalovány.

Možnost 4: Přesunout soubor do truhly (MOŽNOST, KTEROU DOPORUČUJEME)

Poznámka - v případě infekce systémového souboru nebo důležitého programu se může stát, že systém či program nebude správně fungovat. Když ale soubor přesunete do Virové truhly, můžete ho přesunout zpět na své původní místo. Více informací naleznete na straně 8.

Výsledky posledního testu

Po tom, co zvolíte jakou akci má program při detekci viru provést, bude antivirový test dále pokračovat. V případě, že program znovu detekuje další soubor, zastaví se (v případě, že jako první akci nezvolíte "Smazat všechny"). Až test skončí, zobrazí se následující okno s výsledky testu a informacemi o nich.



Pokud zvolíte možnost neprovádět žádnou akci v průběhu testu, tyto soubory budou zobrazeny v seznamu, ale sloupec "Operace" bude prázdný.

I z tohoto okna můžete se souborem pracovat. Klikněte na něj, a potom na tlačítko "Akce" vlevo nahoře. Akci vyberte ze zobrazené nabídky, zobrazí se potom ve sloupci "Operace".

Pokud jste s výsledky testu spokojeni, klikněte na tlačítko "Zavřít". Pro vyvolání okna výslkedků posledního testu znovu jednoduše otevřte **Menu jednoduchého rozhraní** a zvolte "Výsledky posledního testu".

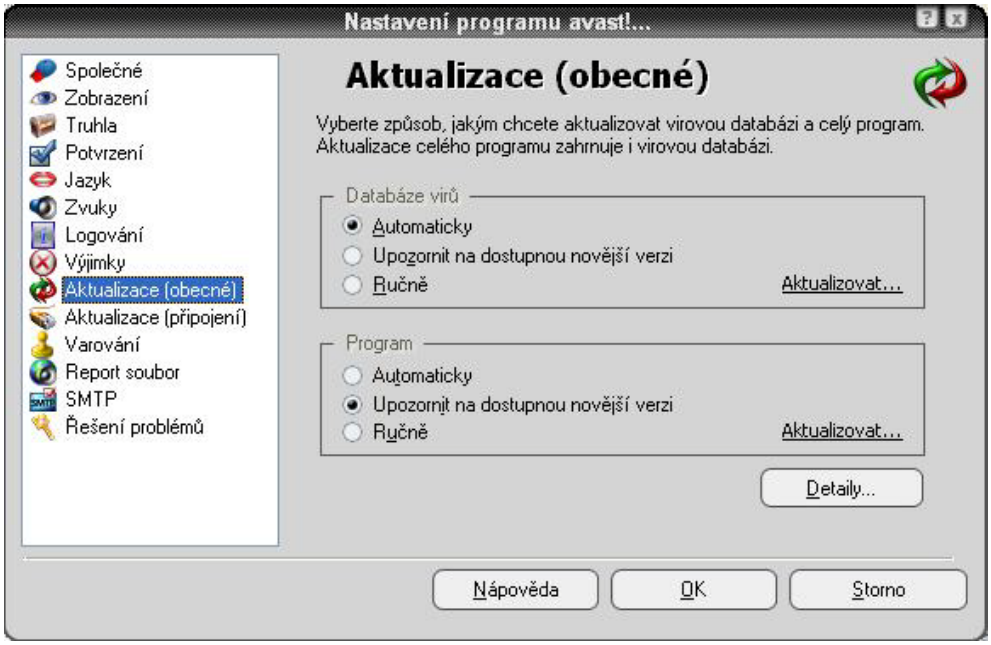
Poznámka: Pokud zavřete program avast!, výsledky posledního testu se již nezobrazí ani poté, co znovu program spustíte. Zobrazí se pouze v případě, že provedete test znovu. Informace o všech detekovaných virech a chybách jsou uloženy a mohou být zobrazeny v Prohlížeči log souborů – viz. **strana 47**.

Pokročilé části programu

Nastavení automatických akualizací

Výkonnost každého antivirového programu závisí na své vlastní databázi virů. Proto je velmi důležité aktualizovat jak virovou databázi, tak samotný program.

Můžete si zvolit, zda obojí chcete aktualizovat automaticky nebo ručně nebo nechat program pouze upozorňovat na dostupnou novější verzi. Změnu provedete buď rovnou z jednoduchého uživatelského rozhraní kliknutím na tlačítko "Pouze databáze" nebo otevřte nabídku Menu (viz. strana 24), zvolte "Nastavení" a klikněte na "Aktualizace (obecné)". Poté zvolte požadovanou položku pro Databázi virů a aktualizaci Programu, jak můžete vidět na obrázku níže.



Klikněte na "OK" a stav v okně přehrávače se změní následujícím způsobem:

- ***Zapnuto*** – pokud jste zvolili automatickou aktualizaci pro virovou databázi i program.
- ***Pouze program*** – pokud jste zvolili aktualizovat automaticky pouze program.
- ***Pouze databáze*** – pokud je automatická aktualizace zvolena pouze pro virovou databázi.
- ***Vypnuto*** – pokud automatická aktualizace není zvolena ani pro virovou databázi ani pro program.

Pokud chcete provést aktualizaci ručně, spusťte Menu jednoduchého rozhraní více na straně 24) a zvolte "Aktualizovat".

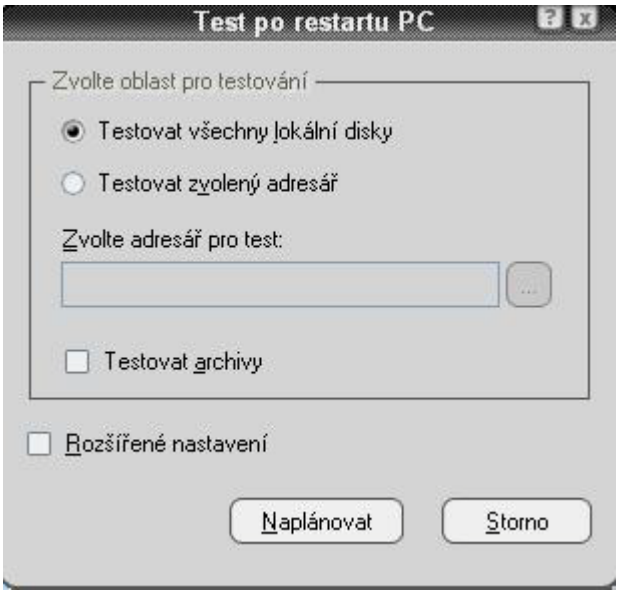
- Pro aktualizaci virové databáze zvolte **Aktualizace iAVS**.
- Druhou možností je **Aktualizace programu**.

Jak naplánovat test po restartu

(pouze pro 32 bitové verze Windows NT/2000/XP a Vista)

Další z možností je naplánovat antivirový test po restartu systému. Takový test se provede před tím, než je počítačový systém aktivní. Tento test je velmi dobrý, protože umožní virus detekovat před jeho aktivací. Virus nebude schopen způsobit žádnou škodu.

K naplánování testu po restaru spusťte **Menu jednoduchého rozhraní** (viz. **strana 24**) a klikněte na "Naplánovat test po restartu". Objeví se následující okno:



Zde si můžete zvolit z testování všech disků nebo zvolených adresářů. K testování adresářů klikněte na "Testovat zvolený adresář" a buď ho přímo ručně vepište do kolonky pro test, nebo klikněte na tlačítko napravo od kolonky a zvolte oblast pro testování. Až oblast naleznete a kliknete na ni, adresářová cesta se automaticky přenese do kolonky adresáře pro test.

Pokud do testu chcete zahrnout i archivované soubory, zaškrtněte položku "Testovat archivy".

Pokud zaškrtnete "Rozšířené nastavení", budete moci zvolit akci, kterou program provede po nalezení viru. Můžete zvolit z těchto možností:

- Smazat infikovaný soubor
- Přesunout infikovaný soubor
- Přesunout infikovaný soubor do truhly
- Ignorovat nalezení viru
- Opravit infikovaný soubor

Pokud zvolíte "Přesunout infikovaný soubor", soubor bude přesunut do složky C:/Program Files\Alwil Software\Avast4\DATA\moved. Program k souboru přidá koncovku ".vir", což slouží k lepší identifikaci souboru a předejití nechtěného spuštění viru.

Pokud zvolíte "Smazat nebo Přesunout infikovaný soubor", budete při detekci každého souboru dotázán, jakou akci má program provést.

Systémové soubory jsou soubory, které počítač používá k spouštění programů. Jejich smazání může mít negativní důsledky na chod systému. Při detekci se Vás proto program zeptá zda:

- Povolit smazání či přesunutí, nebo
- Ignorovat smazání či přesouvání systémových souborů

Volba "Ignorovat smazání či přesouvání systémových souborů" předchází problémům nechtěného smazání důležitých souborů, ale Váš počítač nemusí ochránit před možnou virovou nákazou. Doporučujeme proto přesunout všechny podezřelé soubory do truhly. Potom již nemohou představovat žádné nebezpečí. S nimi můžete naložit tak, jak je popsáno na straně 45 .

Až se rozhodnete jak naložit s infikovanými soubory, klikněte na "Naplánovat", zobrazí se následující okno:

Kliknutím na "Ano" restartujete počítač ihned. Když vyberete "Ne", test po startu systému se provede až při příštím startu počítače.

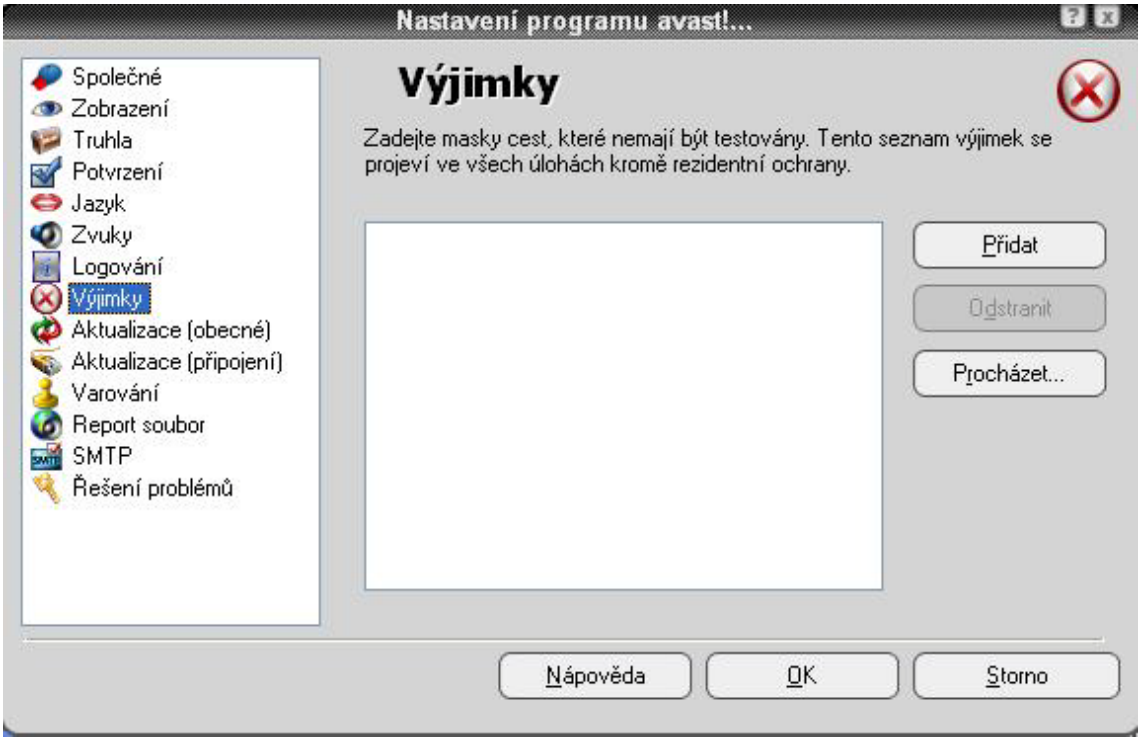
Vkládání souborů do vyjímek testu

Zde máte možnost vyjmout některé oblasti nebo jednotlivé soubory z antivirového testu. Soubory pak nebudou vyhledávány v průběhu žádného testu. To může být užitečné v několika případech:

- ***Předejití falešných alarmů***. Pokud program detekuje nějaký soubor a vy jste si jisti, že je to falešná detekce, můžete tento soubor přidat do vyjímek. Předejdete tak další falešné detekci souboru. V tomto případě prosím kontaktujte ALWIL software, aby mohl být problém co nejdříve vyřešen.

- ***Urychlení testu.*** Pokud máte na hard disku složky, které obsahují pouze obrázky, můžete takovou složku vložit do vyjímek. Doba testování tak bude snížena.

Mějte na paměti, že vkládání do vyjímek ovlivní všechny další antivirové testy, ale nezahrnuje residentní ochranu. Pro vložení souborů či složek do vyjímek residentní ochrany klikněte v **Menu jednoduchého rozhraní** na "Nastavení" a potom na "Vyjímky". Zobrazí se následující okno:



Pro přidání souboru klikněte na tlačítko "Procházet" a daný soubor zvolte. Nebo klikněte na "Přidat" a cestu k souboru či adesáři zadejte do zobrazené kolonky ručně. Pokud chcete do vyjímek přidat nějaký podadresář se všemi jeho soubory, je nutné přidat za jméno adresáře znak "*" (např. C:\Windows*). K vyjmutí souboru či adresáře ze seznamu na něj klikněte a poté klikněte na tlačítko „Odstranit".

Jak vytvořit report soubor výsledku testu

Stálý záznam výsledků každého testu provedete vytvořením reportu, který si budete moci později prohlédnout. Pro vytvoření reportu otevřete **Menu jednoduchého rozhraní**, jak je popsáno na **straně 24** a zvolte "Nastavení". Potom klikněte na Report soubor a v zobrazeném okně zaškrtněte "Vytvářet report soubor".

Pokud chcete vytvářet report soubor každého testu, ale nechcete si uchovávat všechny výsledky, zaškrtněte "Přepsat existující soubor". Jestliže tuto možnost necháte vypnutou, výsledky každého testu se přidají za výsledek předchozí zprávy.

Dále si můžete vybrat kam program report soubor zapíše. Přednastavena je "Standartní složka reportů", kterou změníte kliknutím na "Jiná složka" a zadáním Vámi zvolené cesty.

V "Zapisovat" si vyberete jaké informace budou zapsány v reportu:

- Spuštění úlohy – datum a čas, kdy byl test spuštěn
- Ukončení úlohy – datum a čas, kdy byl test ukončen
- OK soubory – soubory, které byly testovány bez shledání něčeho podezřelého. Pokud budete testovat celý hard disk a zaškrtnete tuto možnost, pravděpodobně bude report soubor velmi dlouhý (až několik tisíc řádků). Proto ji doporučujeme používat pouze při částečném testu a pouze když potřebujete zapsat výsledek všech infikovaných i čistých položek.
- Závažné chyby – vzniknou, pokud program detekuje něco neočekávaného. To obvykle vyžaduje další vyšetření problému.
- Lehké chyby – jsou méně závažné chyby. Většinou vznikají v důsledku nemožnosti testovat soubor (např. kůli využívání souboru jinou aplikací).
- Vynechané soubory – nemohou být testovány z důvodu nastavení testu. Např. v rychlém testu se soubory testují na základě jejich koncovek. Netestují se soubory s koncovkou,

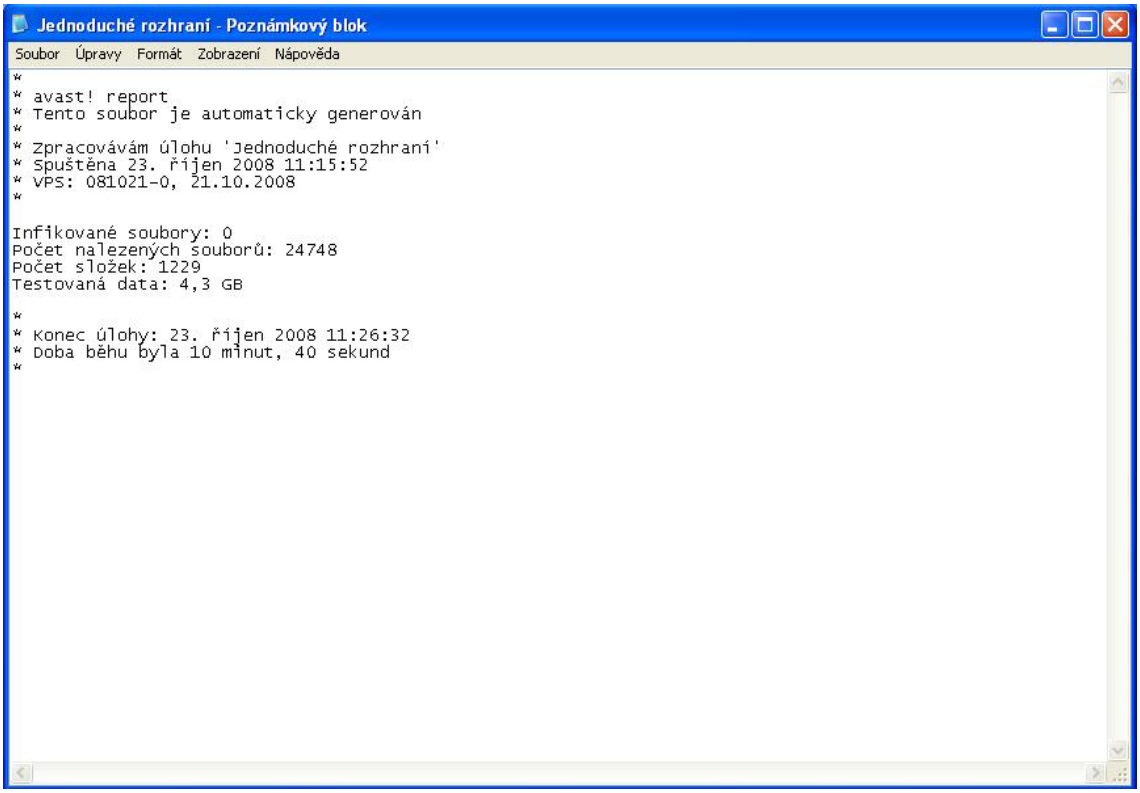
které jsou pokládány za bezpečné. Soubory ve vyjímkách budou také označeny jako vynechané.

- Infikované soubory – soubory, které mohou potencionálně obsahovat virus.

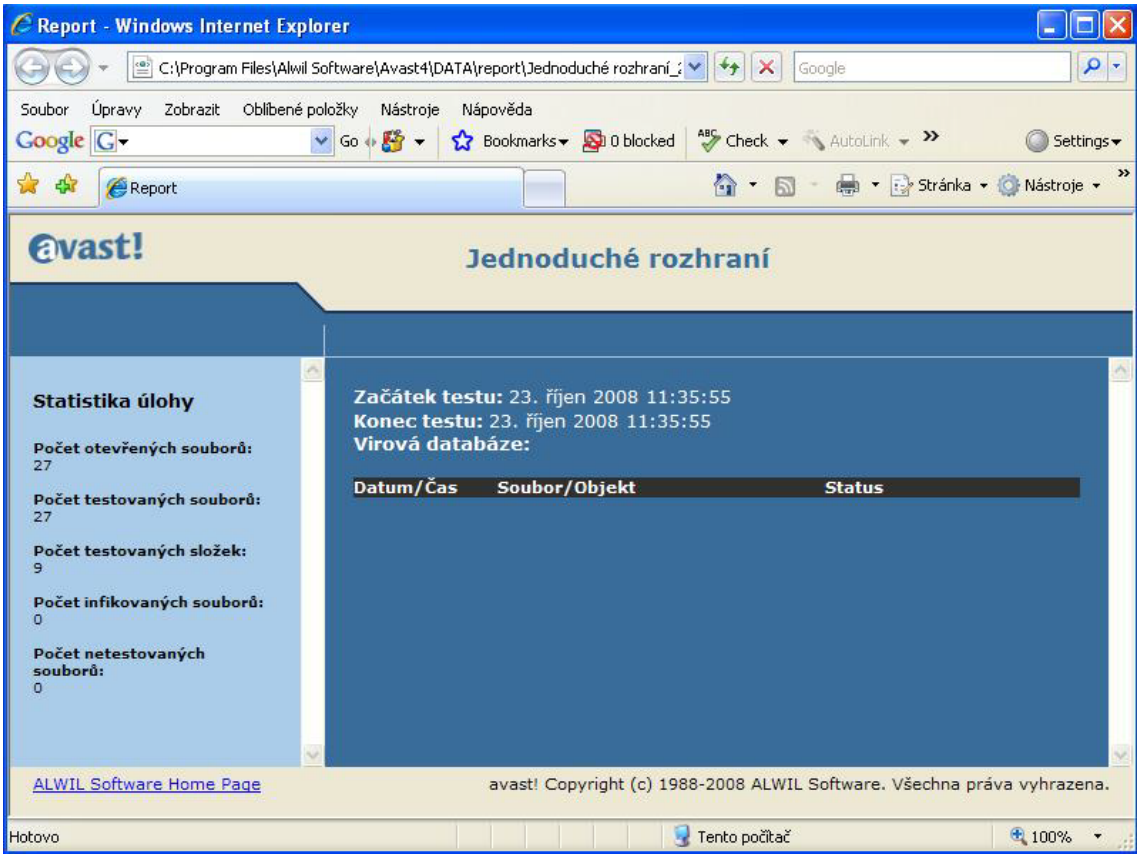
Nakonec zvolte typ souboru, který se vytvoří. Na výběr máte z textového nebo XML souboru. Po skončení testu se v okně jednoduchého rozhraní zobrazí další řádek – "Zobraz podrobný výpis posledního testu."

Po kliknutí na "Zobraz podrobný výpis posledního testu." se zobrazí výsledek testu ve zvoleném formátu. Stejného docílíte z **Menu jednoduchého rozhraní** kliknutím na "Zobrazit reporty testování...".

Report v textovém formátu:



Report ve formátu XML



Reporty předchozích testů jsou uloženy v přednastaveném adresáři nebo v adresáři uživatelem zvoleném – viz. předchozí strany.

Pokud zvolíte textový formát a nezašrtnete položku “Přepsat existující soubor”, uvidíte také výsledky předchozích reportů.

Jestliže již reporty vytvářet nechcete, klikněte na “Report soubor” v **Menu jednoduchého rozhraní** a odškrtněte položku “Vytvářet report soubor”.

Varování

avast! je také schopen zasílat varovné zprávy o virové detekci.

Z **Menu jednoduchého rozhraní** zvolte "Nastavení" a potom "Varování". Tato možnost je zvláště vhodná pro síťové administrátory, kteří tak budou ihned varování při detekci viru kdekoliv na síti.

Varování mohou být nastavena těmito způsoby:

- **WinPopup**
  Klikněte na "Přidat" a zvolte WinPopup. Poté zadejte IP adresu nebo síťové jméno počítače, na který chcete varování posílat. Také můžete kliknout na "Procházet" a adresu vybrat z nabídnutého seznamu.

- **MAPI**
  Varování bude odesláno emailem za použití MAPI protokolu. Do adresy virového varování vložte adresu, kam chcete varování posílat. Potom klikněte na tlačítko "MAPI..." dole pod oknem a vložte tam profil a heslo k příslušnému účtu.

- **SMTP**
  Varování se pošle emailem za použití protokolu SMTP. Pro vytvoření nového varování klikněte na tlačítko "Přidat" a zvolte SMTP. Do kolonky vložte emailovou adresu, kam chcete varování posílat. Je nutné vyplnit i další nastavení – viz. následující sekce "SMTP".

- **Tiskárny**
  Varování bude posláno na zadanou tiskárnu. Klikněte na "Přidat" a potom "Tiskárna". Do kolonky zadejte příslušnou tiskárnu nebo klikněte na "Procházet" a vyhledejte ji.

- **ICQ**
  Varování bude posláno zprávou po ICQ. Do kolonky zadejte číslo osoby, které chcete zprávu poslat.

- **Windows Messenger**
  Zadejte emailovou adresu, kterou používá příjemce zprávy jako login do služby Windows Messenger. Pro vytvoření nového varování klikněte na "Přidat", zvolte typ požadovaného varování a vložte výše zmíněné údaje.

Pokud chcete některé varování změnit či odstranit, klikněte na něj a poté klikněte na tlačítko "Změnit" nebo "Odstranit".

Kliknutím na tlačítko "Test" pošlete zprávu na zvolenou adresu. Kliknutí na "Test všech" pošle zprávu všem příjemcům v seznamu.

SMTP

Klikněte na Menu jednoduchého rozhraní, zvolte "Nastavení" a SMTP. V tomto okně můžete blíže uvést parametry Vašeho SMTP serveru. avast! toto nastavení používá při odesílání emilů zvláště když:

- Odesílá varovné zprávy po nalezení viru
- Odesílá soubory z Virové truhly do firmy ALWIL Software
- Odesílá zprávy o pádu programu do ALWIL Software

Do okna musíte vložit následující informace:

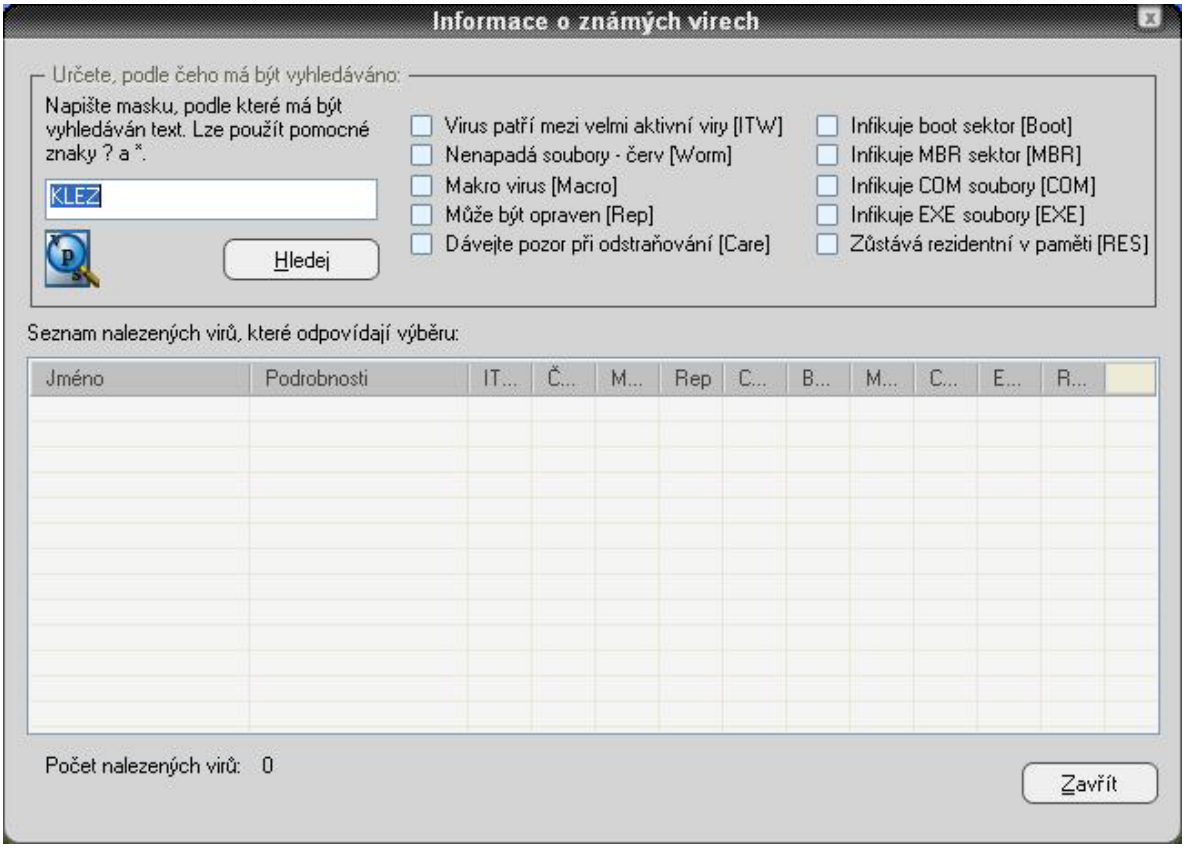
- Adresa serveru – adresa odchozího emailového serveru (např. smtp.server.com nebo 192.168.1.25).
- Port – číslo portu (přednastavený port je 25).
- Odesílatel – adresa odesílatele

Pokud SMTP server vyžaduje pro odhlášení autentifikaci, měl byste danou položku zaškrtnout a vyplnit kolonky pro jméno a heslo.

Informace o virech

Virová databáze obsahuje detailní informace o všech známých virech. Program ji používá při detekci potencionálních infekcí.

Pro otevření informace o virech otevřete **Menu jednoduchého rozhraní** a klikněte na "Informace o virech". Zobrazí se následující okno:



Viry ze seznamu můžete vyhledávat více způsoby. Pokud znáte přímo jméno celého viru, zadejte ho do kolonky a klikněte na tlačítko "Hledej". Pokud znáte pouze část jména, můžete místo neznámého znaku použít symbol "?" nebo "*" místo více neznámých znaků.

Příklad: Chcete najít informace o viru "Klez". Jeho přesné jméno v databázi je Win32:Klez-H [Wrm]. Do vyhledávání tedy napíšete *klez*. Program vyhledá všechny viry, které obsahují slovo „klez".

Pro zúžení výběru můžete také zaškrtnout políčko napravo, kde je seznam nabízených druhů virů. Na vybrané políčko klikněte dvakrát. Poté se zaškrtne a program budete hledat pouze daný druh. Při kliknutí na políčko jednou změníte jeho barvu. Pokud necháte položku zšedlou, hledaný virus ji nesmí obsahovat. Jestliže ji necháte barevnou, může ji obsahovat.

Významy vlastností virů:

- ***ITW - virus patří mezi velmi aktivní viry.***

  Viry označované jako ITW (z ang. "In The Wild" - "v divočině") jsou velmi rozšířené mezi uživateli po celém světě.

- ***Červ - nenapadá soubory***

  Jedná se o virus typu červ (z angl. "worm") tedy o virus, který provádí jiné činnosti než napadání souborů (např. se masově rozesílá, čímž zahlcuje mailové servery apod.).

- ***Macro virus***

  Virus využívající makrojazyka hlavně produktů firmy Microsoft (Word, Excel, ...).

- ***Rep - může být opraven.***

  U těchto virů dokáže avast! provést léčení, tzn. dokáže soubory napadené tímto virem vrátit do funkčního stavu před napadením.

- ***Care - dávejte pozor při odstraňování.***

  Takto jsou označeny viry, při jejichž odstraňování je nutné dodržovat speciální postupy (při jejich nedodržení lze mnohdy napáchat větší škodu než virus samotný!).

- ***Boot - infikuje boot sector.***

  Virus se zapisuje do spouštěcí oblasti pevného disku či diskety (tyto viry jsou v dnešní době vzácné).

- ***MBR - infikuje MBR sector.***

  Virus se zapisuje do master boot record sektoru pevného disku.

- ***COM - infikuje COM soubory.***

  Virus napadá spustitelné programy s příponou .com.

- ***EXE - infikuje EXE soubory.***

  Virus napadá spustitelné programy s příponou .exe.

- ***RES - zůstává rezidentní v paměti.***

  Tyto viry se po spuštění usídlí v paměti RAM a napadají spouštěné soubory.

Práce se soubory ve virové truhle

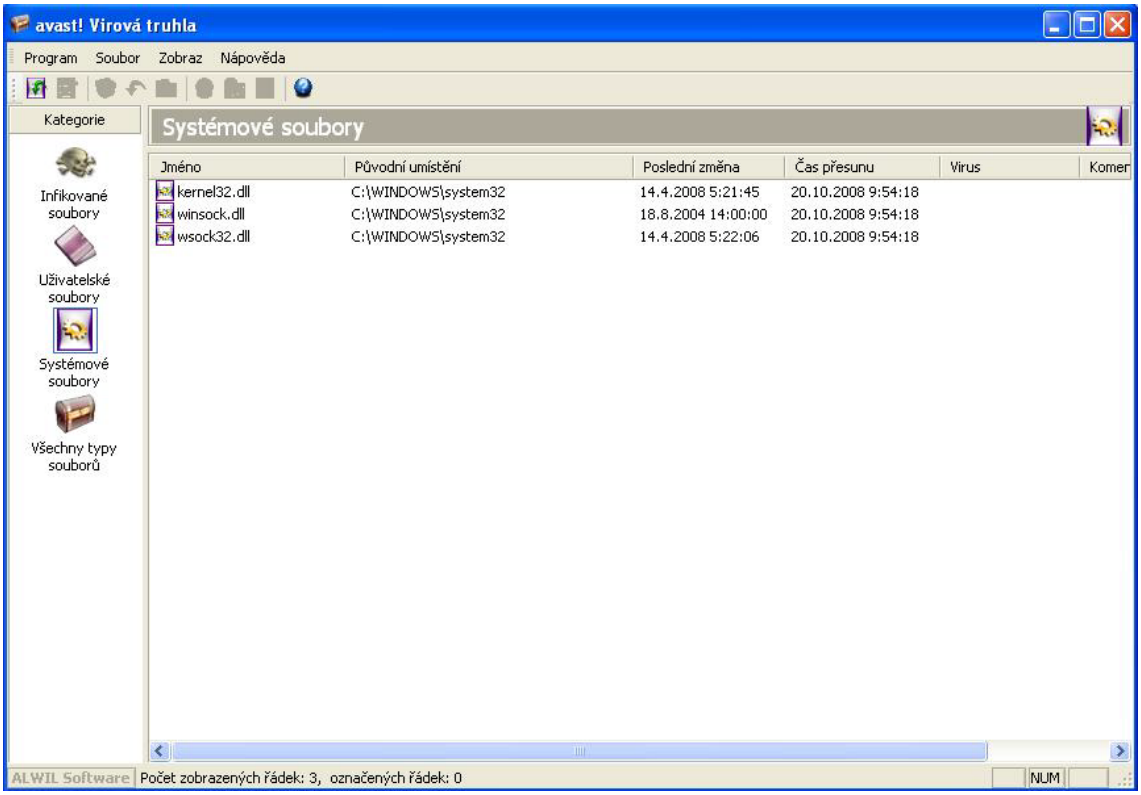
Virovou truhlu můžete spustit přímo z okna jednoduchého rozhraní nebo z nabídky Menu. Truhla se, díky svým vlastnostem, hodí k následujícím účelům:

- ***Ukládání virů.***

Pokud avast! nalezne virus a Vy se z nějakého důvodu rozhodnete jej nemazat, ale uložit, nabídne Vám avast! přesun právě do truhly, kde je zajištěno, že nebude spuštěn neopatrnou manipulací.

- ***Ukládání podezřelých souborů.***
  Každý podezřelý soubor (např. takový, který má dvě přípony) je vhodné pro případ pozdější analýzy uložit do truhly.

- ***Zálohování systémových souborů.***
  avast! při instalaci umístí do truhly, do kategorie "systémové soubory", některé důležité systémové soubory, jejichž eventuální napadení virem by mohlo způsobit pád operačního systému. Tyto soubory lze v případě potřeby z truhly obnovit na původní místo.



Aby jste se soubory v truhle mohly pracovat, klikněte na ně pravým tlačítkem myši nebo na soubor klikněte a vyberte z nabídky ikon v liště nahoře *(Poznámka: Pokud na soubor kliknete dvakrát, zobrazíte vlastnosti souboru. To Vás chrání před nechtěným spuštěním souboru).* Vyberte z následující nabídky:

- ***Obnovit soubory.***
  Zvolte, pokud chcete obnovit všechny soubory ze seznamu. Program je obnový automaticky, což můžete použít, pokud nechcete čekat.

- ***Přidání souboru.***
  Přidat soubor lze pouze do kategorie "uživatelské soubory".

- ***Smazání souboru.***

Soubory se odstraňují nenávratně, čili nepřemísťují se do koše! Ujistěte se, že nemažete některé systémové nebo jinak důležité soubory před použitím této operace.

- ***Obnovení souboru.***
  Tato funkce přesune soubor na jeho původní místo a zároveň jej odstraní z truhly.

- ***Extrahování souboru.***
  Zkopíruje soubor do zvolené složky.

- ***Testování souboru.***
  Prohledá soubor, zda neobsahuje virovou infekci.

- ***Zobrazení vlastností souboru.***
  Zobrazí vlastnosti souboru a umožní přidat k souboru komentář.

- ***Odeslání souboru do ALWIL Software.***
  Umožní zaslat vybraný soubor prostřednictvím e-mailu do ALWIL Software. Tuto možnost používejte ve výjimečných případech, zejména máte-li podezření, že se jedná o falešný poplach. K zasílanému souboru nezapomeňte vždy uvést maximum informací - důvod zaslání, verze virové databáze atp. Takto nám pomůžete stále zlepšovat naše služby a program.

Kliknutím na “Program”, “Nastavení” a potom “Truhla” změníte maximální velikost truhly a tím maximální velikost, kterou bude na hard disku zabírat. Také můžete změnit maximální velikost jednotlivých odesílaných souborů do truhly.

Prohlížeč log souborů

avast! při své práci vytváří různé log soubory, ve kterých jsou obsaženy informace o činnosti programu, o chybách či varováních, stejně jako zaznamenává průběh instalace a aktualizace programu i souborů virové databáze. Tyto záznamy lze pohodlně prohlížet pomocí vestavěného

prohlížeče log souborů (viz. strana 24). Spustíte ho z Menu jednoduchého rozhraní vybráním položky "Zobrazit log soubory".

Jednotlivé záznamy jsou rozděleny do těchto kategorií:

Informace	Informativní zpráva, vše je v pořádku.
Upozornění	Nějaká důležitá informace, ale stále je vše v pořádku. Obsahuje informace o aktualizaci programu a virové databáze.
Varování	Vyskytla se chyba, ale program může pracovat nebo chybu opravit.
Chyba	Vyskytla se chyba, program nemůže pracovat.
Kritická chyba	Kritický problém pro program, bude následovat jeho okamžité ukončení.
Poplach	Potenciálně nebezpečné pro celý počítač.
Fatální chyba	Nebezpečné pro celý počítač (bezpečnost, mazání systémových souborů).

Kliknutím na "Nastavení" a "Logování" z Menu jednoduchého rozhraní můžete změnit maximální velikost každého log souboru.

S informacemi obsaženými v log souborech lze pomocí vestavěného prohlížeče provádět některé základní operace. Můžete je např. řadit, filtrovat, vyhledávat či exportovat.

Hledání.

Chcete-li nalézt určitý záznam logu podle klíčového slova, stiskněte kombinaci kláves **CTRL+F**, nebo z nabídky zvolte **EDITOVAT → HLEDAT**, nebo v nástrojové liště klikněte na ikonu hledání. Také můžete v aktuálním výpisu kliknout pravým tlačítkem myši a po zobrazení místní nabídky zvolit **HLEDAT**. Zobrazí se okno, do jehož řádku napíšete klíčové slovo, např. "boot", a potvrdíte tlačítkem **OK**. Zobrazí se první nalezený záznam. Další můžete vyhledat opětovným stisknutím kláves **CTRL+F**.

Filtrování.

Filtrování se používá hlavně k zúžení výběru aktuálního výpisu podle zadaných kritérií. Z mnohařádkového logu lze tímto způsobem zobrazit nebo označit pouze malý počet řádků, které obsahují dané klíčové slovo. Filtrování spustíte stisknutím kombinace kláves **CTRL+R**, nebo stejnými způsoby jako hledání (viz. výše). Zobrazí se dialog, ve kterém určíte vlastnosti filtru:

Obsahuje.
Napište klíčové slovo, které musí být obsaženo v řádcích, které chcete zobrazit či vybrat. Můžete používat zástupné znaky *****. Pokud chcete zadat více klíčových slov, oddělte je středníkem.

A zároveň neobsahuje.
Zde napište klíčové slovo (slova), které nesmí být obsaženo v řádcích, které chcete zobrazit či označit.

Časové omezení.
Pokud chcete filtrovat logy pouze za určité časové období, nadefinujte je zde.

Zvolí se řádky, které odpovídají omezení.
Tato volba způsobí, že nalezené řádky, odpovídající danému filtru, budou zvoleny (označeny). Toto je výhodné v případě, že chcete výběr exportovat.

Zobrazí se pouze řádky, které odpovídají omezení.
Zvolíte-li tuto možnost, zobrazí se řádky odpovídající danému filtru a ostatní nikoliv.

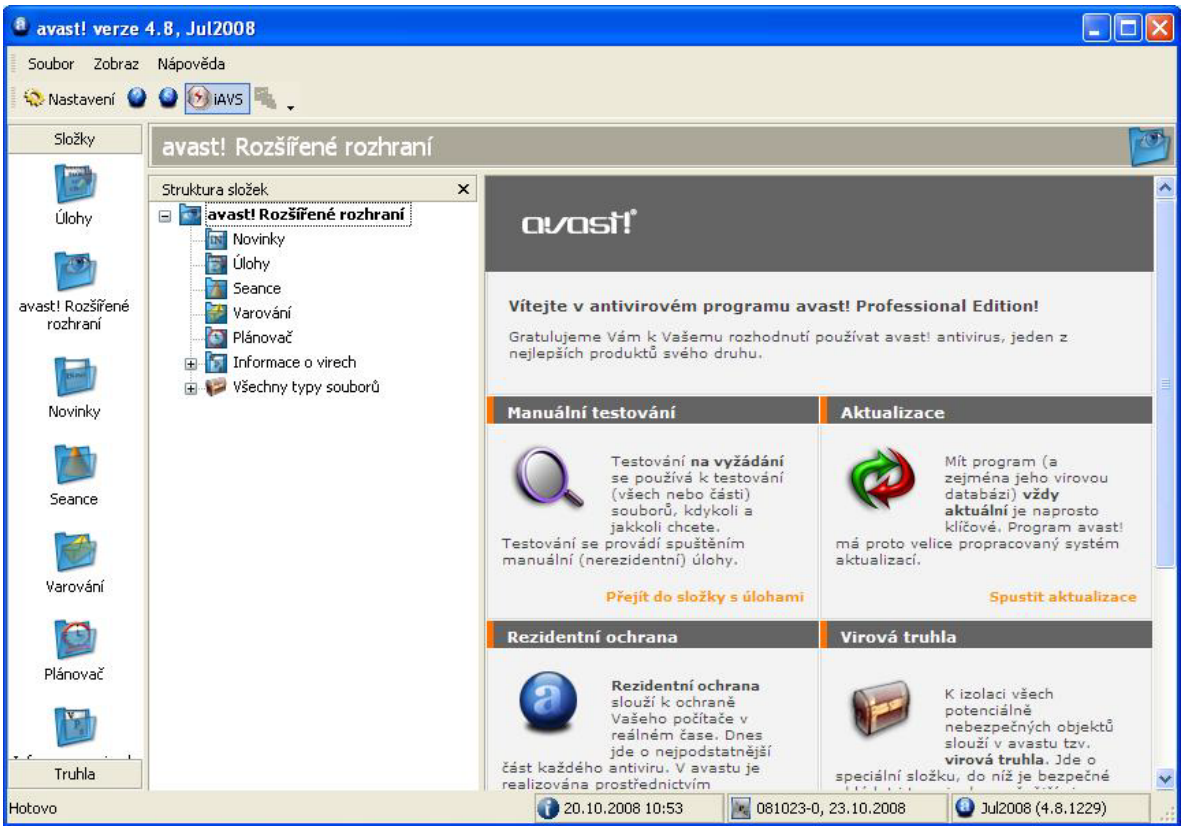
Řazení.
Pokud chcete současný výpis řadit, stačí kliknout levým tlačítkem na záhlaví příslušného sloupce. Položky budou setříděny. Provedete-li toto ještě jednou, řazení se změní ze vzestupného na sestupné a naopak.

Exportování.
Nalezené či vyfiltrované záznamy můžete exportovat do samostatných textových souborů, stejně jako můžete exportovat celé výpisy (např. výpis jedné z kategorií). Zvolte tedy řádky či celý výpis a v hlavní nabídce zvolte **SOUBOR → EXPORTOVAT SOUČASNÝ VÝPIS**, nebo pokud chcete exportovat pouze zvolené řádky, **SOUBOR → EXPORTOVAT ZVOLENÉ ŘÁDKY VÝPISU**. V okně, které se následně zobrazí, určete jméno exportovaného souboru a místo na Vašem počítači, kam si jej přejete uložit.

Práce s rozšířeným uživatelským rozhraním

Do rozšířeného rozhraní se přepnete z Menu jednoduchého rozhraní kliknutím na “Přepnout do rozšířeného rozhraní”. Pokud používáte jednoduché rozhraní bez skinu, klikněte na “Nástroje” a potom “Přepnout do rozšířeného rozhraní”.

Pro návrat do jednoduchého uživatelského rozhraní klikněte na “Zobraz” v horní liště a potom vyberte “Jednoduché rozhraní”.



Antivirový test se v rozšířeném rozhraní spouští vytvářením “Úlohy”. Úloha obsahuje informace o tom, co a jakým způsobem má avast! testovat. Např. jaké adresáře má prohledávat, jaké typy souborů, jak se má zachovat v případě nalezení viru, zdali má testovat také archivy a podobně. Úlohy lze vytvářet, měnit, mazat a kopírovat.

Jak pracovat s úlohami

Součástí programu jsou čtyři přednastavené úlohy. Pokud kliknete na "Úlohy" vlevo v seznamu složek nebo ve struktuře složek, zobrazí se v pravém okně. Po kliknutí na některou z úloh uvidíte v pravém spodním okně její popis.

Rezidentní ochrana.

Tato úloha sleduje (dle nastavení) všechny spouštěné aplikace či otevírané dokumenty, a účinně tak brání infikování počítače v reálném čase. Rezidentní ochrana se spouští automaticky při každém startu operačního systému a nedoporučuje se ji vypínat.

Ostatní úlohy se používají k testování určitých oblastí Vašeho počítače. Pro spuštění na ně dvakrát klikněte nebo na ně klikněte pravým tlačítkem myši a zvolte "Spustit".

Hledání: disketa A:

Spustí test diskety ve Vaší mechanice A: . U diskety bude zkontrolována i její systémová oblast, tedy boot sektor.

Hledání: lokální pevné disky
Úloha prohledá všechny spustitelné soubory a OLE dokumenty na všech lokálních pevných discích počítače. V případě, že program avast! nějaký virus nalezne, dá to najevo varovným hlášením o nálezu a zvukovým efektem (pokud je v počítači nainstalována zvuková karta). Úloha ohlásí každý nalezený virus. Kontrolovány budou i zkomprimované soubory a operační paměť počítače. U každého disku bude také zkontrolována systémová oblast. Nenajde-li úloha žádný virus, zobrazí hlášení, že úloha skončila a žádný virus nebyl nalezen.

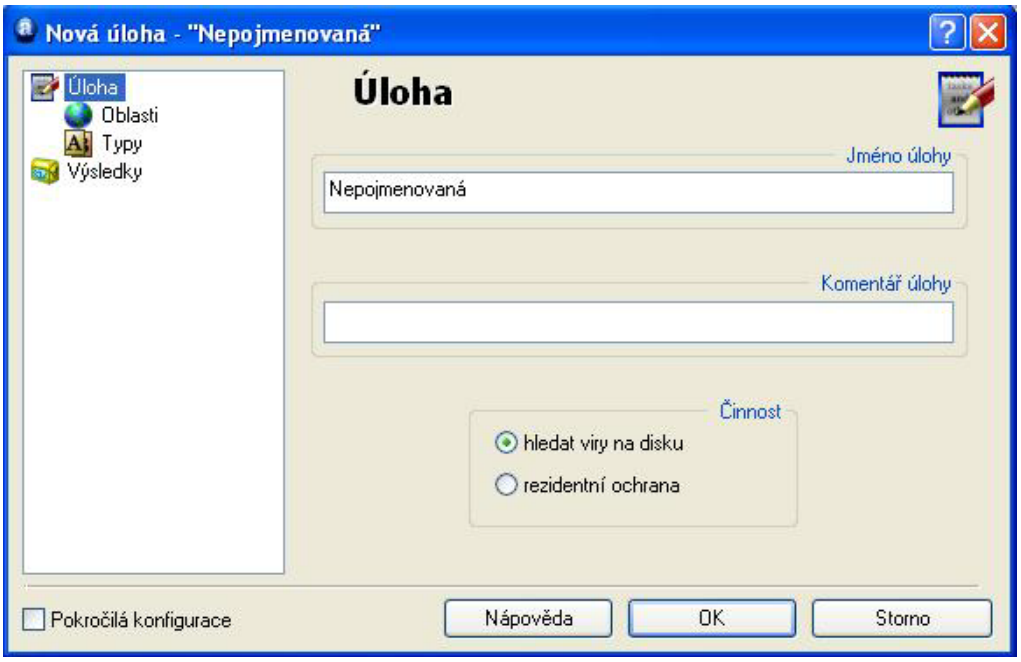
Hledání: zvolit složky
Úloha provede naprosto stejné kontroly na přítomnost virů jako předchozí úloha, ale před vlastní kontrolou bude mít uživatel možnost vybrat oblasti, které mají být zkontrolovány. Vybrat lze pochopitelně i více oblastí najednou.

Vytvoření a editace úlohy

Další možností je vytvoření vlastní úlohy, kterou poté můžete kdykoliv spustit. To je užitečné zvláště pro testování jednotlivých adresářů či souborů na disku nebo k naplánování úlohy ve Vámi zvolených časových intervalech.

Vytvoření nové úlohy zahrnuje spoustu kroků, z kterých si můžete zvolit např. oblasti testu, jaké soubory testovat a reporty. Po zvolení vlastnosti úlohy a potvrzení tlačítkem "OK" se nová úloha uloží. Pokud žádné nové nastavení nezvolíte, úloha se uloží v původním nastavení. Tu potom můžete měnit tlačítkem "Změnit" z horní lišty nebo kliknutím pravým tlačítkem myši na úlohu a zvolením "Vlastnosti". Úlohu můžete také odstranit tlačítkem "Smazat" z horní lišty.

Pro vytvoření nové úlohy nejdříve klikněte na "Úlohy" v horní liště nebo klikněte pravým tlačítkem myši na složku "Úlohy" na levé straně a zvolte "Vytvořit novou". Anebo klikněte na tlačítko "Nová" nahoře, zobrazí se následující obrazovka:

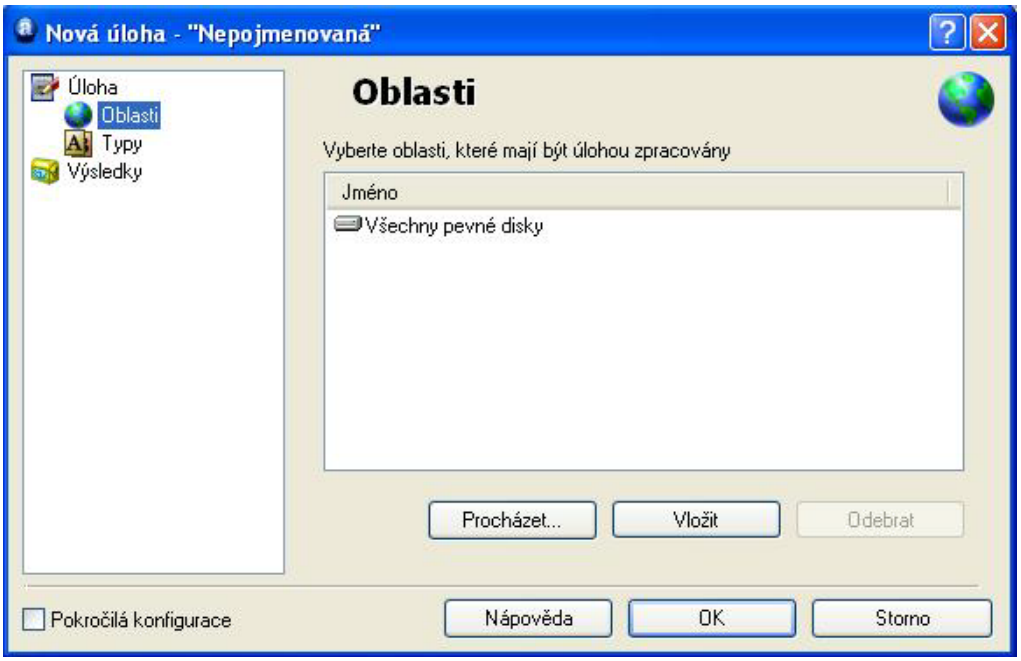


V této obrazovce si můžete zvolit jméno úlohy, které se později objeví v seznamu úloh v hlavním okně. Z názvu by tedy mělo být jasné, k čemu bude úloha sloužit (např. "Test: Moje dokumenty"). K úloze můžete také přidat nějaký užitečný komentář. Nakonec vyberte, zda se má úloha provádět pro test na vyžádání nebo pro rezidentní ochranu.

Vytváření úlohy test "na vyžádání"

- ***Oblasti***

Pokud máte pod položkou "Úloha" zvoleno "hledat viry na disku", klikněte na "Oblasti". Objeví se následující okno:



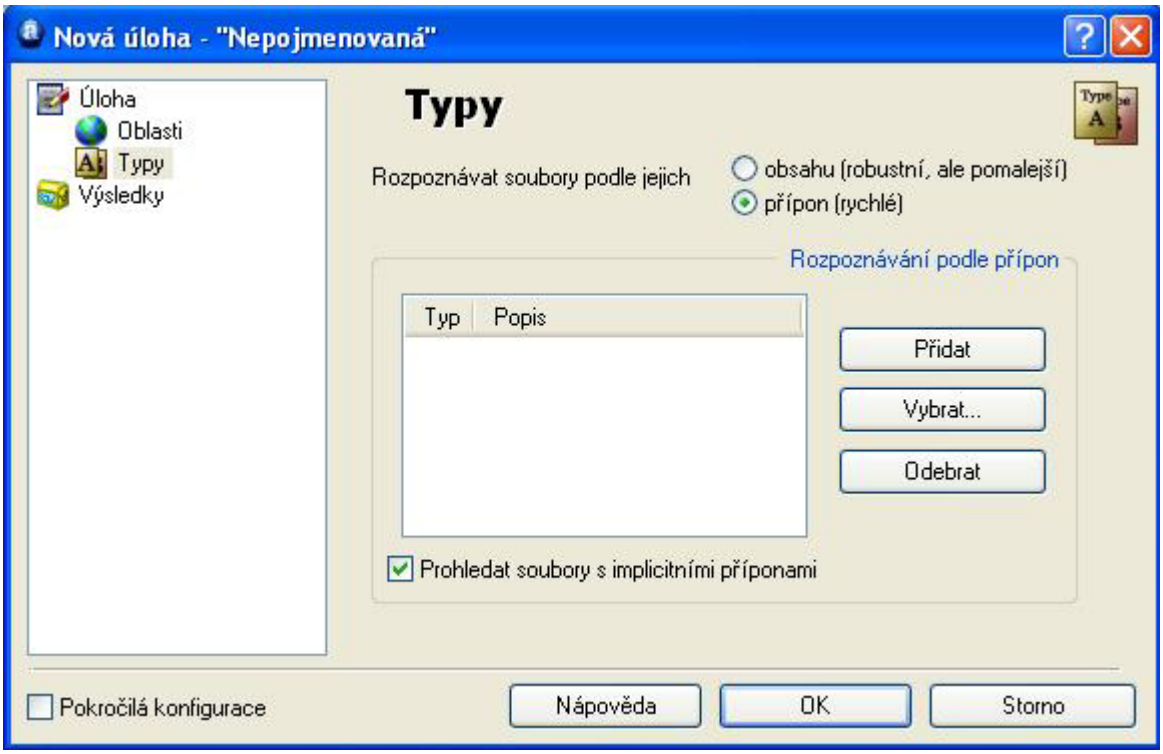
Zde vybíráte oblasti, které budou touto úlohou prohledávány. Implicitně je nastaveno "Všechny pevné disky". Oblastí můžete definovat více, může se jednat o celé adresáře nebo soubory. Pokud nechcete testovat všechny disky, klikněte na danou oblast a vyberte tlačítko "Odebrat". Potom můžete vybrat vlastní oblast kliknutím na "Procházet..." a zaškrtnutím požadovaných oblastí.

Po kliknutí na talčítko "Vložit" můžete zvolit z množství testovatelných oblastí. Položka "Zvolit po startu" znamená, že výběr oblasti k testování provedete vždy znovu při každém spuštění úlohy. Volbou "Jiná oblast" se do seznamu vepíše text "<napsat oblast>". Tento text nahraďte cestou k adresáři nebo souboru, který chcete testovat, tedy například "C:/Windows/System/soubor.exe".

- ***Typy***

Po zvolení testované oblasti klikněte na "Typy" a určete, jaké typy souborů bude avast! prohledávat. Mohou být rozpoznávány podle svého obsahu, což je důkladnější, ale pomalejší, nebo přípon.

Pokud zvolíte možnost rozpoznávat typy souborů podle jejich obsahu, máte na této stránce k dispozici už jen jednu volbu – "Prohledávat všechny soubory". To znamená, že se viry budou hledat i v souborech, v nichž se běžně nenacházejí, např. v textových souborech či v obrázcích. Pokud zvolíte možnost rozpoznávat typy souborů podle jejich přípony, zobrazí se následující dialogové okno, ve kterém určíte, jaké typy (tedy soubory s jakými příponami) chcete prohledávat.



Seznam přípon k testování se zobrazí po kliknutí na tlačítko "Vybrat...". Vybírat lze jeden či více odpovídajících typů souborů (pro výběr více položek lze použít klávesy CTRL a SHIFT). Vyberte požadovanou příponu a klikněte na "OK". Pokud přípona v seznamu není, můžete ji přidat ručně. Klikněte na "Přidat", příponu napište do pole a potvrďte znovu kliknutím na "Přidat". Jestliže některou příponu chcete ze seznamu vymazat, vyberte ji a klikněte na "Odebrat".

Pokud zaškrtnete kolonku “Prohledat soubory s implicitními příponami”, testovat se budou také všechny “nebezpečné” přípony.

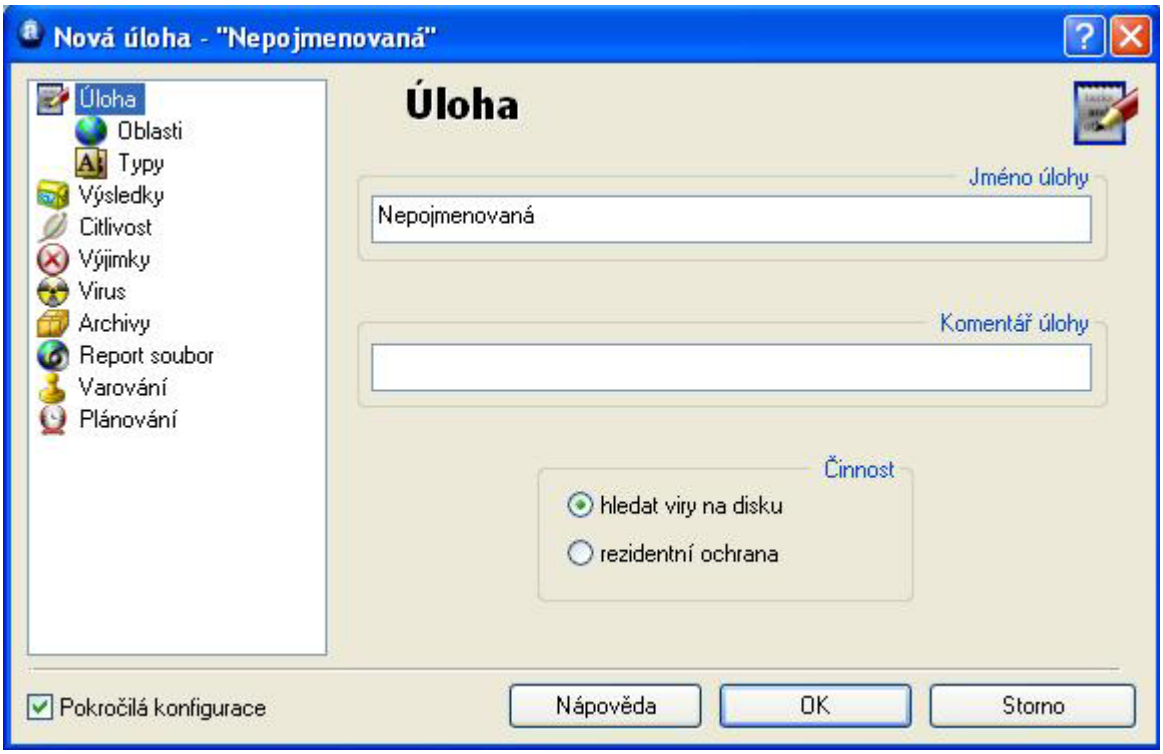
Všechny soubory s příponami, které nebyly zvoleny, budou reportovány jako “vynechané soubory”.

- ***Výsledky***

Po kliknutí na “Výsledky” lze pomocí zaškrtávacích políček zvolit, jaké výsledky budou úlohou uchovávány pro pozdější použití. Za normálních okolností postačí ukládat výsledky o infikovaných souborech. Na výběr máte také z ukládání souborů, na kterých se vyskytla těžká chyba, lehká chyba, vynechaných souborů nebo souborů vynechaných kůli nastavení vyjímek. Nedoporučujeme zaškrtnout políčko “OK soubory”, následkem by bylo vytvoření velmi velkého textového souboru.

Pokud nechcete uchovávat výsledky testu, vypněte tuto možnost ve spodní části obrazovky.

Jestliže zaškrtnete políčko “Pokročilá konfigurace”, zobrazí se následující okno s další nabídkou:



- ***Citlivost***

Zaškrtnutí políčka “Testovat celé soubory” určuje, zda se na přítomnost virů budou testovat celé soubory nebo jen ty části, do kterých se nejčastěji viry zapisují. Vychází se z toho, že drtivá většina virů buď přepíše začátek souboru, nebo se přidá na jeho konec. Zaškrtnutím této volby se tedy bude testovat celý soubor. Provádění úlohy se tak přirozeně poněkud zpomalí.

Zaškrtnutím volby “Ignorovat charakteristiky virů” zajistíte, že soubory budou testovány na přítomnost všech virů ve virové databázi. Není-li tato volba zvolena, jsou soubory testovány pouze na přítomnost těch virů, které napadají daný typ souboru. To znamená, že např. v souborech s příponou COM nebude avast! hledat viry, které napadají pouze soubory typu EXE.

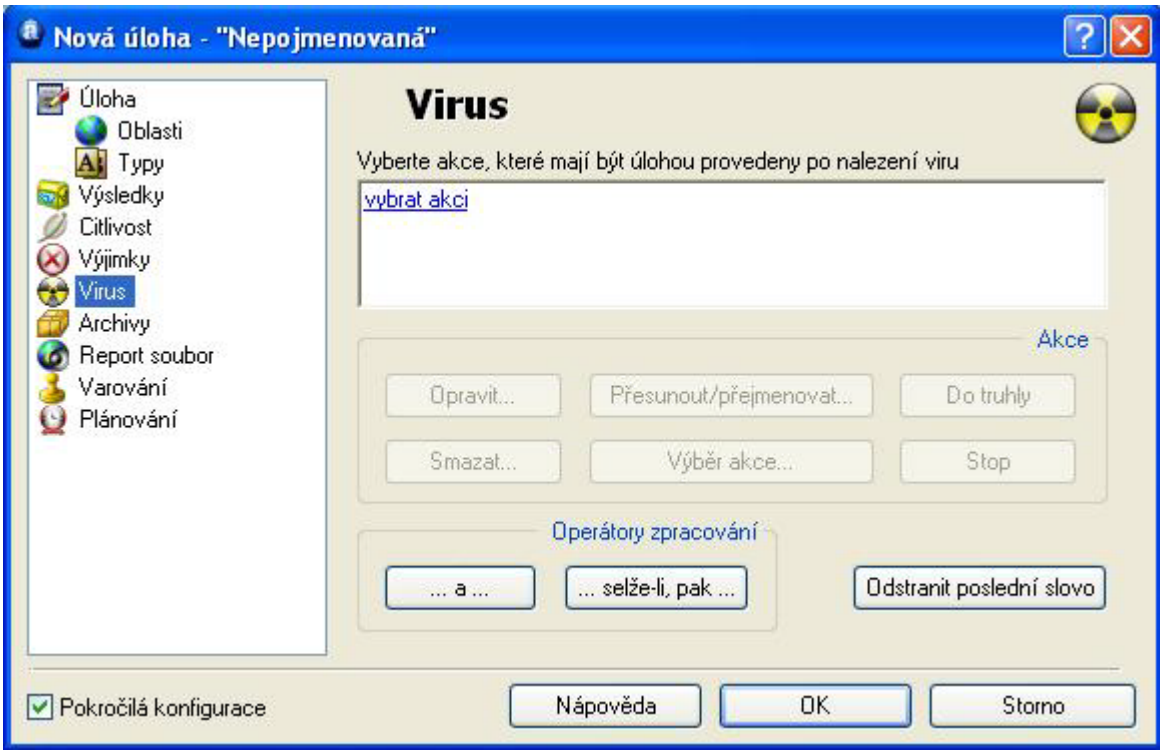
- ***Výjimky***

Zde je možno vyjmout určité oblasti nebo jen jednotlivé soubory z testování, takže se v nich nebudou hledat viry. Funguje to stejným způsobem, jak je popsáno na straně 37.

Vyjímky se ale aplikují pouze na jednotlivé úlohy. Soubory nebo adresáře, které jsou obsaženy ve výjimkách v Menu jednoduchého rozhraní budou automaticky vyjmuty ze všech testů a reportovány jako "vynechané soubory".

- ***Virus***

Po kliknutí na "Virus" se zobrazí toto okno:



Na této stránce lze určit, jaké operace budou provedeny v případě, že úloha nalezne virus. Přednastaveno je "vybrat akci". To je interaktivní akce.

Pokud tam přednastavenou akci necháte, po nalezení viru se provádění úlohy pozastaví a objeví se okno vyzývající Vás k vybrání akce.

Jaké akce budou v tomto okně k dispozici, můžete zvolit tak, že v seznamu akcí kliknete na "vybrat akci" a následně vyberete požadované možnosti. Danou akci můžete vybrat individuálně pro každý podezřelý soubor.

Po kliknutí na "vybrat akci" se zobrazí okno s interaktivním výběrem akce, tzn. Smazat, Opravit, Přesunout do truhly, Přesunout/Přejmenovat nebo Ukončit. Při detekci viru se zobrazí pouze ty volby, které zaškrtnete.

Všechny tyto volby jsou podrobně popsány na **straně 29** v části "Co dělat, pokud byl nalezen virus".

Pokud necháte zvolenu interaktivní akci, antivirový test se po detekci viru vždy zastavý. Jestliže budete plánovat úlohu a při jejím spuštění nebudete u počítače, doporučujeme Vám zvolit si více akcí. Jako např. "Přesunout do truhly".

Pro volbu jiné akce nejprve předchozí smažte kliknutím na tlačítko "Odstranit poslední slovo". Takto můžete odstranit všechny vybrané akce, čímž aktivujete šest možností ve středu okna. Kliknutím na některou z nich ji vložíte do akcí, které mají být úlohou provedeny po nalezení viru.

Smažete je znovu tlačítkem "Odstranit poslední slovo".

První čtyři akce jsou blíže popsány na **straně 29**.

Kliknutím na "Výběr akce" znovu zvolíte přednastavenou interaktivní akci. Kliknutím na "Stop" jednoduše test přerušíte ihned po nalezení podezřelého souboru.

Vybrat můžete více než jednu akci kliknutím na tlačítko "...a...". Například lze zvolit "Opravit" detekovaný soubor "...a..." potom "Přesunout/Přejmenovat".

Také můžete zvolit alternativní akci, která se provede, pokud původní selže. Například "Opravit" jako preferovaná akce. "...selže-li, pak..." a "Do truhly". Pokud selže oprava nějakého souboru, pošle se do truhly (viz. **strana 45**).

Poznámka – pokud zvolíte "Smazat", program se zeptá, zda chcete soubor smazat pernamentně nebo ho smazat do koše. Také můžete zvolit, zda se soubor smaže po dalším startu počítače zaškrtnutím "Smazat soubor(y) po startu systému, jsou-li zamčeny".

- ***Archivy***

Na této stránce lze zvolit, jaké typy archivů bude avast! při provádění úlohy testovat. Jako výchozí jsou vybrány pouze samorozbalovací spustitelné soubory. Volbou dalších archivů se samozřejmě prodlouží doba provádění seance. Zaškrtnutím volby všechny archivy se budou testovat všechny programu avast! známé archivy.

- ***Report soubor***

Zde můžete vygenerovat a uložit soubor obsahující informace o provedené seanci. Jedná se v podstatě o stejné informace jako ve výsledcích úlohy.

Další možnosti nastavování report souborů jsou blíže popsány na **straně 38**.

Poznámka: Standardně se report ukládá jako soubor *nazev_ulohy.rpt*. Soubor *.rpt je ve skutečnosti textový soubor, a lze jej tedy prohlížet a editovat běžným Poznámkovým blokem (Notepad).

- ***Varování***

Varování je buď obecné, které se rozešle vždy, když dojde k detekci podezřelého souboru nebo jednotlivé, vázající se k jednotlivé úloze, ke které je nastaveno.

Alerty, které mohou být přidány k jednotlivé úloze, jsou zobrazeny v kolonce “Dostupná varování”. Obecné varování se vytváří z “Nastavení” – “Varování” v Menu jednoduchého rozhraní. Blíže jsou popsány na **straně 41**. Tato varování nemohou být spojena s jednotlivou úlohou.

Pokud je v kolonce zobrazeno varování, které si přejete použít, klikněte na tlačítko “→”. Varování bude přesunuto do kolonky “Použitá varování”.

Pokud Vám zobrazené vyhovovat nebudou, klikněte na “Nové...” a vytvořte nové varování.

K varování můžete přidělit zvolené jméno, např. jméno, které je nějak spojeno s danou úlohou nebo můžete přidat komentář. Varování se vytváří úplně stejným způsobem, jak je popsáno na **straně 41** .

Poté co varování vytvoříte, klikněte na tlačítko “OK”. Automaticky se přesune do kolonky “Použitá varování”.

Z této kolonky varování přesunete zpět do dostupných varováních kliknutím na tlačítko “←”.

Pro změnu nebo smazání varování ho označte a klikněte na tlačítka “Upravit...” nebo “Odstranit”.

Pokud chcete vytvořit hlášení pomocí SMTP, nezapomeňte po vytvoření úlohy také vyplnit detaily SMTP kliknutím na “Nastavení” a “SMTP”.

Mějte na paměti, že varování, které jsou spojena s jednotlivými úlohami se odešlou pouze, pokud bude podezřelý soubor detekován právě touto úlohou. Pokud chcete odeslat varování, které je detekováno jakoukoliv úlohou, musíte vytvořit obecné varování. Více je vysvětleno na **straně 41**.

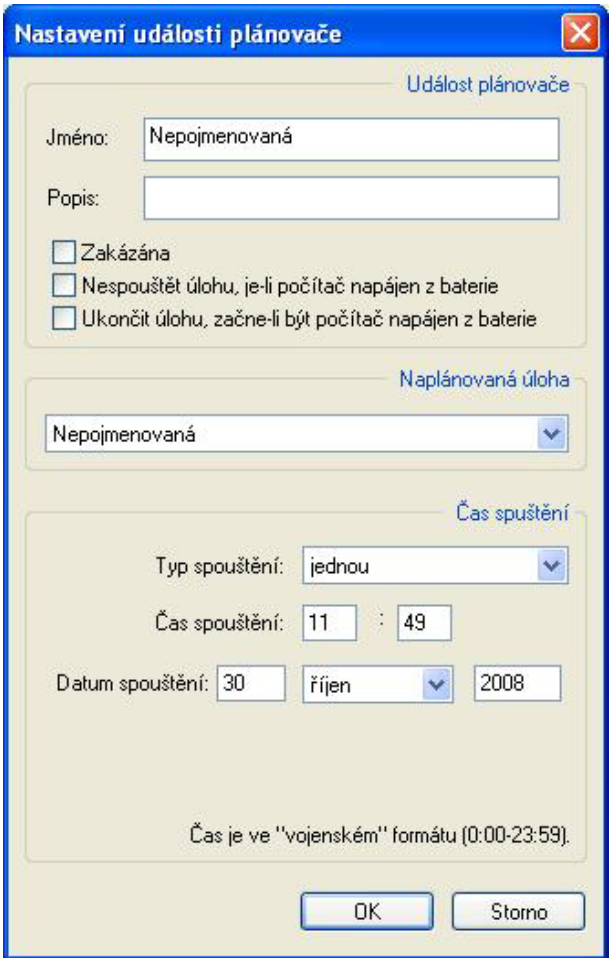
Tímto způsobem vytvořené alerty si můžete prohlédnout ve složce “Varování” v hlavním okně rozšířeného rozhraní. Také zde můžete vytvořit varování nové a později je použít při vytváření úloh. Klikněte na “Varování” v horní záložce a vyberte “Nové varování”.

Vytvořené varování smažete po jeho označení a kliknutí na “Varování” v horní liště a zvolte “Smazat varování”.

Plánování

Při vytváření úlohy si také můžete naplánovat, kdy chcete danou úlohu spouštět. Buď v určitý stanovený čas nebo v pravidelných intervalech (denně, týdně či měsíčně).

V okně "Plánování" klikněte na tlačítko "Přidat...". Objeví se nové okno "Nastavení události plánovače". Zvolte si jméno pro plánovanou úlohu, popřípadě ji popište v kolonce "Popis".



Pokud úlohu ještě nechcete aktivovat nebo ji chcete později zrušit a ne smazat, zaškrtněte políčko "Zakázána".

Další dvě možnosti poslouží zejména uživatelům notebooků. Pokud zaškrtnete "Nespouštět úlohu, je-li počítač napájen z baterie", úloha se při tomto chodu notebooku nespustí.

Položka "Ukončit úlohu, začne-li být počítač napájen z baterie" úlohu ukončí, pokud se přeruší napájení z elektrické sítě.

V kolonce "Naplánovaná úloha" zvolte její jméno. Poté pod položkou "Typ spouštění" blíže určete, zda chcete úlohu spustit pouze jednou nebo v pravidelných intervalech (denně, týdně nebo měsíčně). Podle toho se Vám objeví konfigurovatelné možnosti.

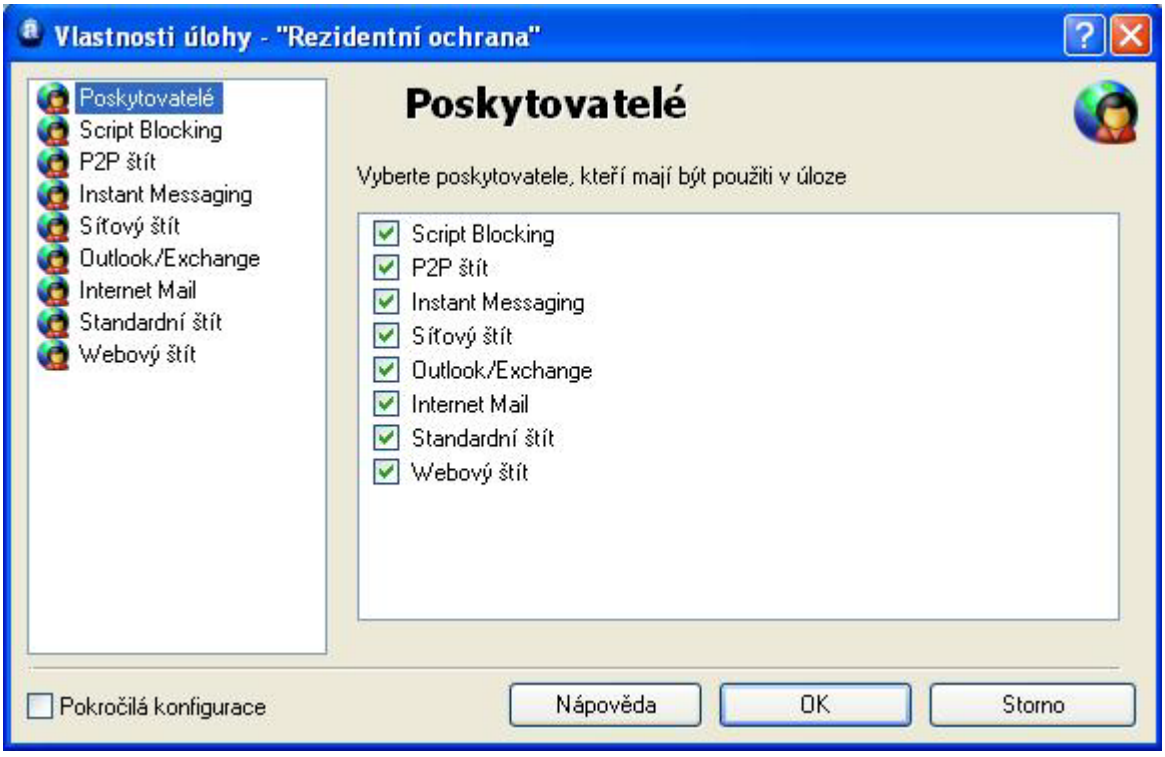
Jestliže chcete naplánovanou úlohu změnit nebo odstranit, klikněte na ni pravým tlačítkem myši a zvolte "Vlastnost" nebo "Odstranit".

Vytváření nové residentní úlohy

Pokud je přednastavená residentní ochrana aktivní, monitoruje všechny oblasti Vašeho počítače. Jestliže si přejete takové monitorování změnit, zastavte residentní ochranu a vytvořte novou úlohu s vlastním nastavením. To je lepší, než měnit standartní originální úlohu. Úlohu zastavíte kliknutím pravým tlačítkem myši na modrou ikonu "a" v systémové liště a vybráním "Zastavit residentní ochranu". Stejným způsobem se provádí změna v okně residentní ochrany, tak jak je popsáno na předchozích stranách uživatelského manuálu.

Spuštění jakékoliv residentní úlohy automaticky vypne ostatní residentní úlohy. Pokud vidíte modrou ikonou "a" v systémové liště, tak residentní ochrana právě běží. Pokud aktivní není, objeví se před ní přeškrtlé červené kolečko.

Pro vytvoření residentní úlohy spusťte novou úlohu a klikněte na "residentní ochrana", objeví se okno se seznamem všech poskytovatelů. Poté klikněte na "Poskytovatelé" a odškrtněte ty, které nechcete v úloze použít. Také můžete změnit nastavení každého poskytovatele, klikněte na něj a zvolte "Normální" nebo "Citlivé" nastavení.



Pokud zaškrtnete položku "Pokročilá konfigurace", budete moci vybrat z dalších možností. Například testovat pouze určité typy souborů nebo blíže určit, jakou akci program provede po detekování podezřelého souboru. Více informací naleznete v části nastavení Residentní ochrany, reportů a varování.

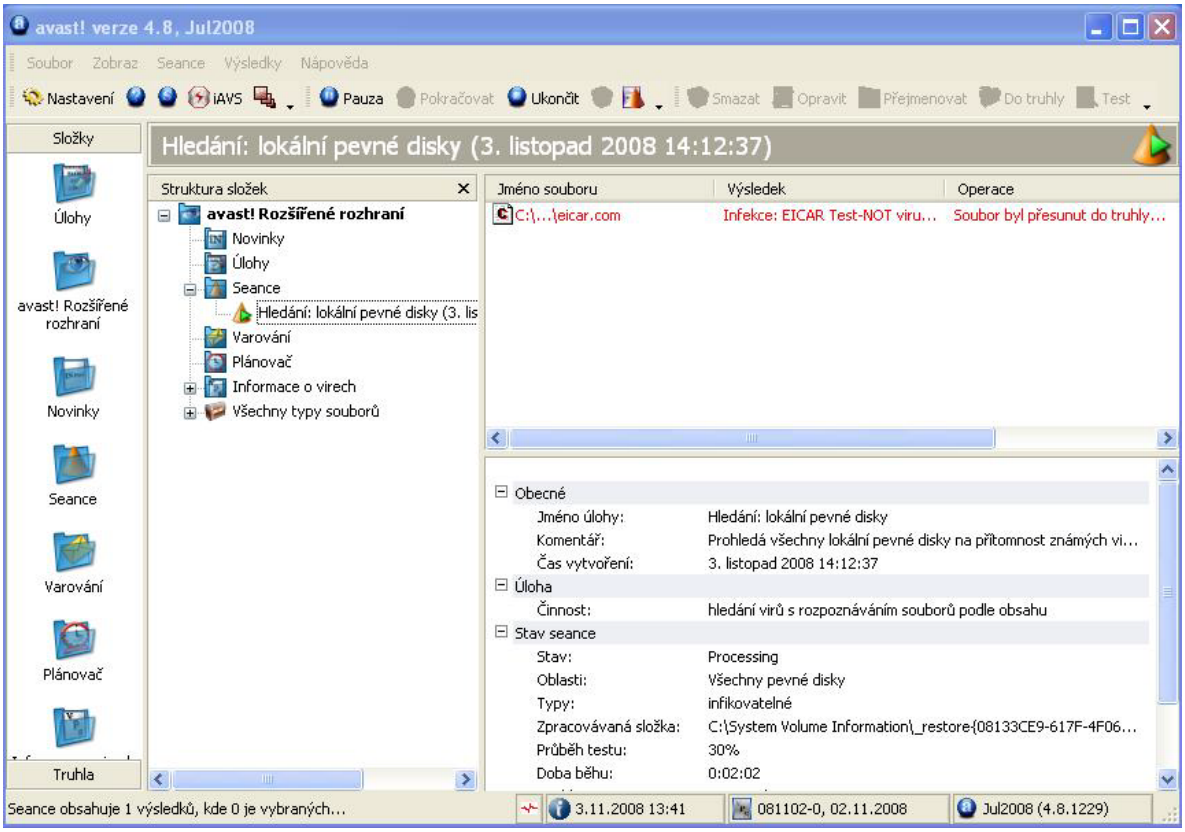
Seance: Spouštění testu "Na vyžádání"

Po kliknutí na jakoukoliv úlohu na následujícím obrázku se zobrazí popis této úlohy. Tu spustíte dvojitým kliknutím na úlohu nebo kliknutím pravým tlačítkem a vybráním "Spustit".

Seance je samotný proces zpracovávání úlohy. Neboli po spuštění úlohy začne probíhat seance. Lze ji pozastavovat, ukončovat, mazat nebo zobrazovat její výsledky. Seance se zaznamená pro každou spuštěnou úlohu, kliknutím na ni pak zobrazíte více informací. To můžete vidět na obrázku dole. Všechny detekované podezřelé soubory jsou vypsány v horním okně, celkové výsledky jsou zobrazeny v okně spodním.

Akci, kterou program provedl můžete vidět popsanou ve sloupci "Operace". Pokud jste při vytváření úlohy vybrali nějakou automatickou akci, objeví se zde potvrzení, zda byla úspěšná. Jestliže jste vybrali akci "Interaktivní", objeví se varování detekce viru a program se Vás zeptá, jakou akci má provést – viz. strana 29.

Požadovanou akci můžete vybrat hned nebo ji ignoravat a rozhodnutí provést později. Kliknutím na podezřelý soubor zobrazíte v horním okně dostupnou nabídku. Jakákoliv ruční akce, kterou provedete, budete také zobrazena ve sloupci "Operace".

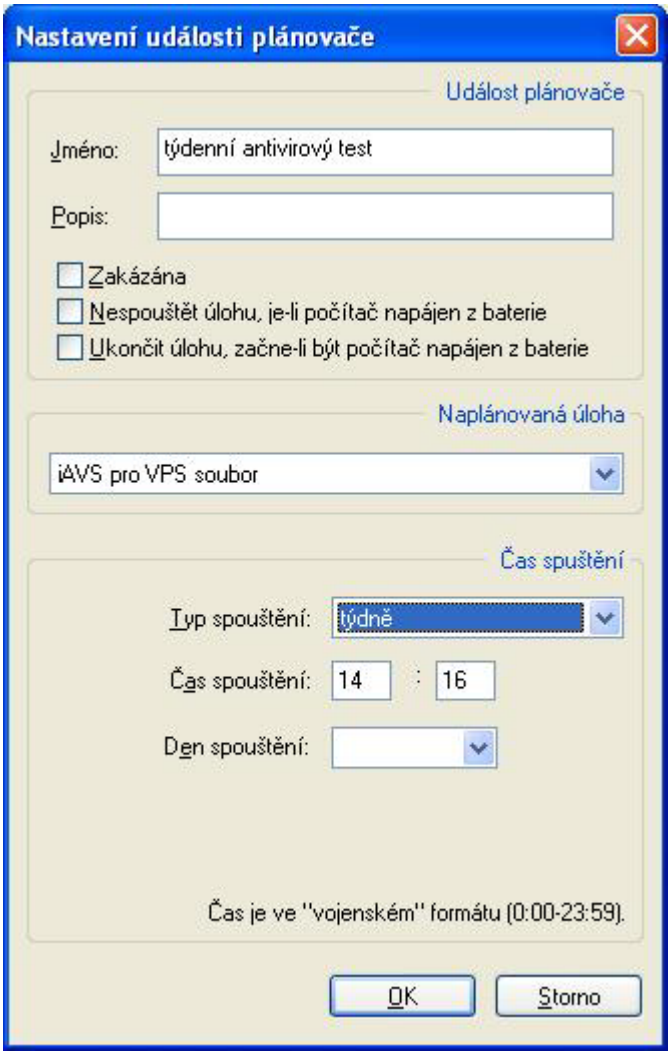


Pokud bylo při vytváření úlohy použito reportování, můžete si výsledky prohlédnout kliknutím na "Seance" v horní liště a potom kliknutím na "Zobraz report soubor".

Plánování vytvořených úloh/aktualizace

V rozšířeném rozhraní můžete naplánovat jakoukoliv vytvořenou úlohu nebo aktualizaci programu a virové databáze.

Pokud chcete naplánovat úlohu (např. aktualizaci virové databáze), klikněte na adresář "Plánovač". Poté klikněte na "Nová" v horní liště nebo "Plánovač" v horní liště a vyberte "Nová událost". Do zobrazeného okna vpište jméno požadované události, popřípadě také její popis. Tři možnosti k zaškrtnutí byly vysvětleny v kapitole "Vytváření nové Úlohy na vyžádání". Ze seznamu naplánovaných úloh si zvolte, kterou chcete naplánovat. Viz. obrázek na následující stránce.



Nakonec zvolte interval a čas spouštěné úlohy. Vše je také vysvětleno v předchozí kapitole. Potom klikněte na tlačítko "Ok".

Úloha je teď naplánována a zobrazí se, kdykoliv kliknete na "Plánovač" v seznamu adresářů. Pokud ji spustíte, vytvoří se nová seance. Výsledky seance si budete moci prohlédnout po kliknutí na adresář "Seance".

Chcete-li naplánovanou událost změnit, klikněte na ni pravým tlačítkem myši a zvolte "Vlastnosti". K odebrání úlohy zvolte "Smazat".

Při plánování testu mějte na paměti, že zvolení "Interaktivní" možnosti test zastaví vždy, když bude detekován podezřelý soubor.

Více informací naleznete na **straně 54**. V tomto případě doporučujeme vytvořit a naplánovat další úlohu, která se provede v případě, že je virus detekován (jako např. přesunout virus do truhly).

Poznámka – Virovou databázi nebo program můžete kdykoliv aktualizovat z horní lišty kliknutím na "Soubor" a "Aktualizace programu" nebo "Aktualizace iAVS" (tu můžete aktualizovat i kliknutím na iAVS v horní liště).

Plánování testu po restartu

Pro naplánování testu po restartu nejdříve klikněte na adresář "Plánovač". Potom klikněte na "Plánovač" v horní liště a zvolte "Plánování startu po restartu" nebo klikněte na ikonu horní lišty, která představuje tužku pod zeleným trojúhelníkem. Ve středu obrazovky se objeví nové okno, popsané blíže na **straně 35**.

Virová truhla

Všechny soubory v truhle můžete zobrazit kliknutím na tlačítko "Truhla vlevo dole" a potom na složku "Všechny typy souborů".

Jakoukoliv operaci se souborem je možné provést třemi způsoby: příslušný soubor označíte a požadovanou operaci zvolíte buď z nástrojové lišty kliknutím na odpovídající ikonu, nebo zvolíte objekt a z nabídky vyberete činnost anebo na soubor kliknete pravým tlačítkem myši a z kontextové nabídky zvolíte požadovanou operaci.

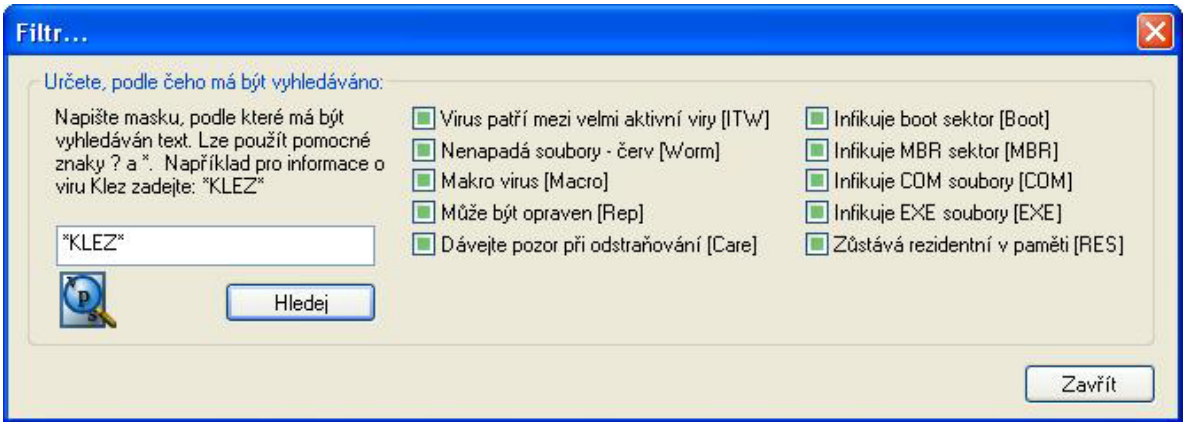
Pro použití možnosti "Obnovit" nebo "Přidat" musíte nejdříve kliknout na okno, v kterém jsou soubory obsaženy.

Vyhledávání ve virové databázi

Do virové databáze se dostanete kliknutím na složku “Informace o virech”.

Drhuhy virů zaškrtnete kolonkami vedle každého popsaného typu viru. Jedlotlivé druhy jsou bíže popsány na **straně 43**.

Pokud chcete vyhledat nějaký konkrétní virus, klikněte na “Informace o virech” a potom na “Filtr” v horní liště. Zobrazí se následující okno:



Viry ze seznamu můžete vyhledávat více způsoby. Pokud znáte přímo jméno celého viru, zadejte ho do kolonky a klikněte na tlačítko “Hledej”. Pokud znáte pouze část jména, můžete místo neznámého znaku použít symbol “?” nebo “*” místo více neznámých znaků.

Příklad: Chcete najít informace o viru “Klez”. Jeho přesné jméno v databázi je Win32:Klez-H [Wrm]. Do vyhledávání tedy napíšete *klez*. Program vyhledá všechny viry, které obsahují slovo „klez”.

Pro zůžení výběru můžete také zaškrtnout políčko napravo, kde je seznam nabízených druhů virů. Na vybrané políčko klikněte dvakrát. Poté se zaškrtne a program budete hledat pouze daný druh. Při kliknutí na políčko jednou změníte jeho barvu. Pokud necháte položku zšedlou, hledaný virus ji nesmí obsahovat. Jestliže ji necháte barevnou, může ji obsahovat.

Prohlížeč log souborů

Informace o Prohlížeči log souborů a jeho použití naleznete na **straně 47**.

Z rozšířeného uživatelského rozhraní ho spustíte kliknutím na “Zobraz” v horní liště a potom kliknutím na “Zobrazit log soubory”.

Virus cleaner

avast! Virus Cleaner je nástrojem k léčení souborů. To znamená, že dokáže opravit soubory napadené virem, aniž by je bylo nutné smazat a obnovit ze zálohy, či dotyčný software reinstalovat. Odstraňuje i virem přidané položky do systémového registru a soubory virem vytvořené (které samy o sobě neobsahují virový kód a nejsou tedy programem avast! detekovány). Jednoduše řečeno, avast! Virus Cleaner odstraňuje veškeré možné stopy po virové infekci. Není nutné spouštět jej v tzv. Nouzovém režimu Windows - je-li v paměti nalezen aktivní virus, je nejprve deaktivován.

avast! Virus Cleaner je přímo součástí antivirového programu avast!. Pokud avast! nalezne na počítači virus, který je vhodné odstranit pomocí avast! Virus Cleaneru, zobrazí se nabídka na spuštění a použití nástroje přímo v okně "Byl nalezen virus" jako samostatné tlačítko (nadepsané "Úplně odstranit virus z celého systému"), podobně jako tlačítka s možností smazání, přejmenování či přesunutí viru. Je-li nabídka ke spuštění avast! Virus Cleaneru aktivní, doporučujeme ji vždy použít!

Virus Cleaner můžete spustit přímo z rozšířeného uživatelského rozhraní kliknutím na “Soubor” a potom “Spustit avast! Virus Cleaner”. Po spuštění se provedou následující akce:

- Otestuje se paměť operačního systému, a je-li nalezen známý virus, jeho proces je ukončen. Tak se zabrání jeho dalšímu šíření. Pokud není možné virový proces ukončit (což se může stát - například červ Nimda používá falešnou systémovou knihovnu ke spouštění virového kódu uvnitř jiných procesů), je virus deaktivován - upraven tak, aby se dále nešířil.
- Jsou otestovány všechny lokální disky.
- Je prohledán systémový registr a všechna místa, odkud by se mohly automaticky spouštět programy. Je-li nalezen odkaz na virus zjištěný v paměti nebo na disku, záznam se opraví nebo odstraní.
- Infikované soubory, zjištěné při antivirovém testu, jsou odstraněny nebo opraveny (podle potřeby).
- Jsou smazány pracovní soubory vytvořené nalezenými viry.

Pokud je pro dokončení desinfekce potřeba restartovat počítač (například pokud virový soubor nemohl být smazán, neboť se stále používá, nebo pokud je deaktivovaný virus stále přítomen v paměti), uživatel je informován a dotázán, zda chce provést restart okamžitě.

Důrazně doporučujeme, abyste v průběhu testování nespouštěli žádné další aplikace. Mnohé viry se startují automaticky při spuštění jakékoliv jiné aplikace. Běžící virové procesy jsou ukončovány nebo deaktivovány pouze během první fáze procesu desinfekce; pokud virus znovu aktivujete uprostřed procesu testování (tím, že spustíte nějakou aplikaci, jako třeba Průzkumník nebo Poznámkový blok), virus pravděpodobně z Vašeho počítače nebude odstraněn!

Aby avast! Virus Cleaner mohl spolehlivě odstranit infekci z Vašeho počítače, je ho nutné spustit s administrátorskými privilegii (pokud je spouštěn pod Windows NT/2000/XP/2003/Vista). Pokud tato podmínka není splněna, některé viry nemusí být detekovány nebo správně odstraněny!

Tichá instalace

Tato možnost je určena zvláště správcům sítí. Umožňuje nainstalovat avast! na libovolný počet počítačů bez zásahu uživatele. Instalace může obsahovat předdefinované nastavení programu a úloh.

Při vytváření Tiché instalace postupujte následujícím způsobem:

- Na jeden počítač nainstalujte avast!.
- Nastavte jej tak, jak si přejete, aby byl nastaven na všech ostatních stanicích.
- Nastavte parametry úloh.
- Chcete-li, nastavte heslo pro přístup k nastavení a ukončení rezidentní ochrany.
- V Rozšířeném rozhraní zvolte “Soubor” a potom “Vytvořit tichou instalaci”.

A nastavte parametry tiché instalace:

- **Tichý režim** - Při instalaci na klientských počítačích se uživatelům budou zobrazovat pouze možná chybová hlášení.
- **Velmi tichý režim** - Při instalaci na klientských počítačích se uživatelům nebudou zobrazovat žádná hlášení.
- **Instalační složka** - Určete, do jakého adresáře se má avast! nainstalovat (standartně %PRGFILES%\Alwil Software\Avast4).
- **Žádný restart** - avast! po své instalaci potřebuje restartovat počítač. Touto volbou zajistíte, že restart nebude vyžadován.
- **Zeptat se na restart** - Po dokončení instalace bude uživatel vyzván k restartu.
- Pokud není zvoleno **Žádný restart** ani **Zeptat se na restart**, počítač bude po ukončení instalace restartován automaticky.

Klikněte na tlačítko **Vytvořit**.

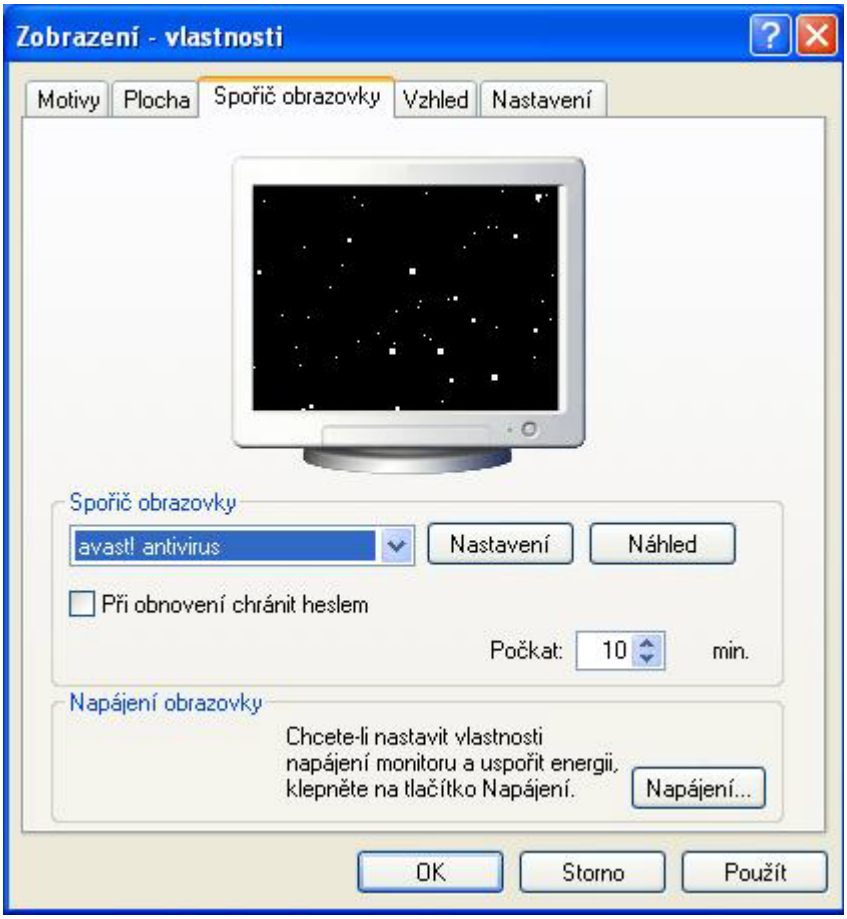
Nakonec určete, do které složky mají být uloženy soubory nezbytné pro tichou instalaci. Umístí se tam soubory admin.ini a tasks.xml . Soubor admin.ini obsahuje nastavení programu avast!, soubor tasks.xml obsahuje nastavení jednotlivých úloh. V případě, že bylo nastaveno heslo pro rezidentní ochranu, naleznete v adresáři také soubor **aswResp.dat**, který obsahuje šifrované heslo pro přístup k nastavení a ukončení rezidentní ochrany.

Do tohoto adresáře by měl být umístěn i instalační soubor programu. Nezapomeňte, že by složka měla být sdílená, tak aby ji bylo možné spustit na každé cílové stanici.

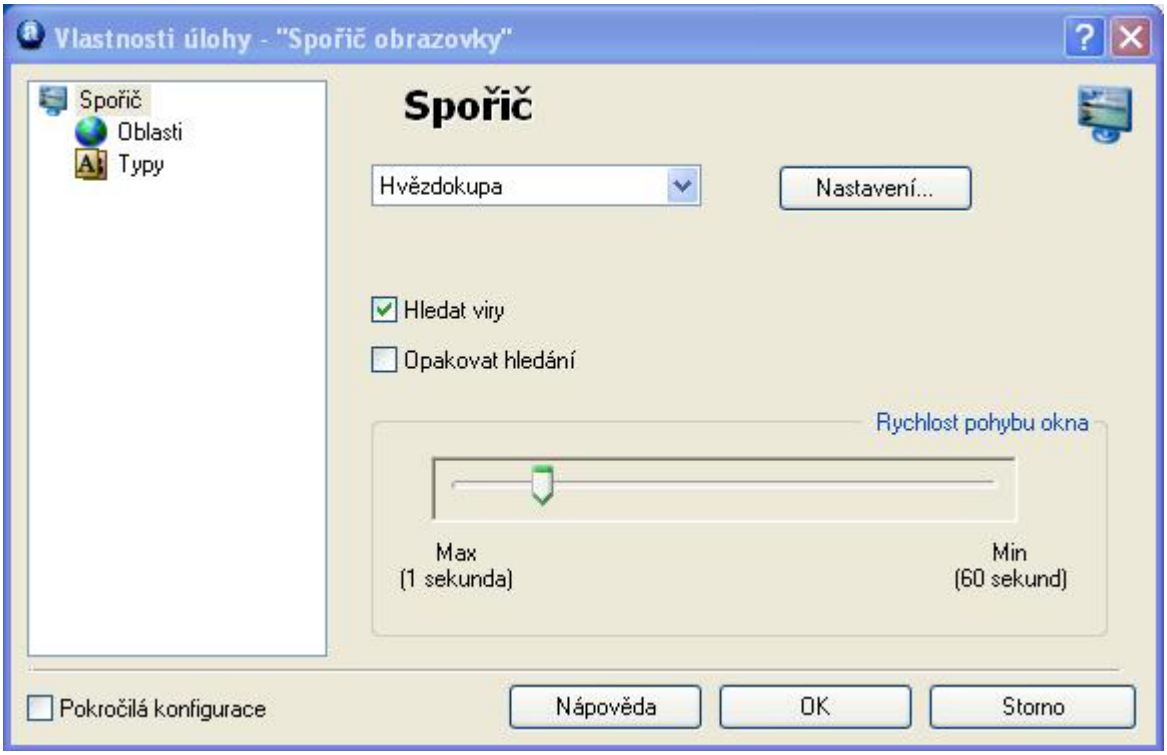
Jak používat spořič obrazovky programu avast! antivirus

avast! umožňuje provádět kontrolu souborů i v okamžiku, kdy se na počítači nepracuje a je spuštěn spořič obrazovky. Ve Vašem oblíbeném spořiči obrazovky se tak objeví ještě jedno malé okno programu avast! informující o jeho činnosti.

Chcete-li zapnout spořič obrazovky programu avast! antivirus, klikněte na tlačítko "Start" vlevo dole, vyberte "Ovládací panely" a klikněte na "Zobrazení". V okně Zobrazení-vlastnosti vyberte záložku "Spořič obrazovky". Pod kolonkou "Motiv" vyberte možnost "avast! antivirus". Ke zvolení máte i další běžně konfigurovatelné možnosti jako je doba čekání spořiče či ochrana heslem při obnovení.



Po kliknutí na tlačítko "Nastavení" se objeví následující okno, ve kterém budete moci spořič nakonfigurovat.



Pokud chcete provést test počítače na viry vždy, když se spořič obrazovky aktivuje, zašrtněte položku "Hledat viry". Jestliže tato položka zaškrtnutá není, spořič obrazovky programu avast! bude fungovat jako klasický spořič obrazovky.

Zaškrtnutím položky "Opakovat hledání" se ujistíte, že se test provede znovu poté, co prohledal všechny definované oblasti.

Jezdec v části "Rychlost pohybu okna" mění frekvenci zobrazovaného okna o průběhu testu.

Kliknutím na "Nastavení" budete moci znovu nastavit bežný spořič obrazovky.

Po kliknutí na "**Oblasti**" a "**Typy**" v levé části nastavíte další možnosti testu, jak je blíže vysvětleno na **straně 51**.

Pokud zaškrtnete políčko "Pokročilá konfigurace", objevý se další nabídka. Více je vysvětleno v části **Vytváření úlohy "test na vyžádání"**.

Nastavení residentní ochrany

1. Instant Messaging

Programy

Zde můžete blíže určit, pro jaké IM programy budou soubory testovány.

Pokud používáte Windows 95/98/ME a chcete zajistit ochranu programu Trillian, musíte danou adresářovou cestu zadat přímo do jeho konfiguračního souboru talk.ini . Některé programy lze chránit pouze při použití operačních systémů Windows NT, 2000, XP, 2003, Vista nebo 2008.

Archivy

Tato strana se zobrazí pouze pokud nastavujete residentní ochranu pomocí vlastnosti úlohy z Rozšířeného rozhraní, jak je blíže popsáno na **straně 55**.

Virus

Zde můžete blíže specifikovat, jakou akci program provede po nalezení viru. Také sem se můžete přepnout pouze při konfiguraci úlohy z Rozšířeného rozhraní. Viz. **strana 54**.

2. Internet Mail

Na stranách “POP”, “SMTP”, “IMAP” a “NNTP” můžete nastavit testování odchozích emailů, příchozích emailů a zpráv. Po případné detekci viru bude k emailové zprávě přidána příslušná informace. Další možností je přidávání čistých zpráv k emailům bez infekce.

Přesměrování

Tato část umožňuje nastavit transparentní testování emailů. Testovány budou emaily, které chodí přes nastavené porty. Funkce je dostupná pouze pod operačními systémy Windows NT/2000/XP/2003/Vista/2008.

- Přesměrované porty.

  Přednastavené jsou čtyři porty pro základní emailové protokoly. Pokud používáte porty odlišné, měly byste je sem vepsat. Jestliže je jich více, oddělte je čárkou.

- Ignorované adresy.

  Zde můžete zadat adresu buď mailového serveru nebo portu, kterou chcete vyjmout z antivirového testu. To je užitečné, pokud chcete testovat pouze zprávy z určitého účtu (a ignorovat ostatní). Když například zadáte smtp.server.com, avast! nebude testovat odchozí (SMTP) zprávy pro příslušný účet.

- Ignorovat lokální komunikaci

  Tato možnost by měla být normálně zaškrtnutá. Pokud není, avast! bude testovat i komunikaci lokální, která je obyčejně bezpečná. To povede ke zpomalení počítače. Poznámka: Do přesměrovaných portů zadávejte pouze porty, které opravdu používáte. V opačném případě by mohlo dojít k neočekávaným problémům.

Pokročilé

- Zobrazovat informace o činnosti

  Pokud je položka zaškrtlá, program bude v pravé dolní části obrazovky ukazovat soubory, které se právě testují.

- Tichý režim.

  Přednastavená akce po detekování podezřelého souboru je akce interaktivní. Pokud je zvolen také tichý režim, program se se všemi infikovanými soubory vypořádá podle následujícího pravidla:

  > Jestiže je zapnuto “s odpovědí Ano” všechny infikované soubory přiložené k emailové zprávě budou automaticky smazány.

  > Pokud je zvoleno “s odpovědí Ne”, infikovaný soubor bude automaticky přesunut do virové truhly.

  Při přednastavené akci po detekování podezřelého souboru a vypnutém tichém režimu se zobrazí normální okno nalezení podezřelého souboru a program se Vás zeptá, jakou akci chete s infikovaným souborem provést.

  Jestliže je zapnutá jakákoliv jiná akce než akce interaktivní, zaškrtnutí položky “Tichý režim” nebude mít na zvolenou akci žádný efekt.

  Mějte na paměti, že pokud nastavíte jinou akci pro poskytovatele Standartní štít, toto nastavení bude platit i pro poskytovatele Internet Mail a nahradí jeho stávající nastavení.

- Délka čekání na odpověď z Internetu.

  Přestavuje čas v sekundách, po který bude program čekat na odpověď z mailového serveru. Dále můžete zvolit, zda se po překročení této doby má ukončit spojení nebo se program zeptá na další potvrzení z Vaší strany.

- Zobrazit ikonu na liště při testování pošty

  Po zaškrtnutí této možnosti se při testování pošty zobrazí v systémové liště malá modrá ikona programu avast!

Heuristika

avast! umožňuje hledat v příchozích zprávách nejen známé viry, ale dokáže také kontrolovat zprávy heuristickou analýzou a případně tak odhalit virus, který v daný okamžik ještě nemá ve své virové databázi. Na této stránce lze tuto heuristickou analýzu modifikovat.

- Citlivost - Nízká.

  > Základní kontrola příloh.

    Kontrolují se přílohy podle jména a podle typu obsahu. To znamená, že avast! hlídá, zda příloha připojená ke zprávě nemá název složený ze dvou přípon a zda druhá přípona není "nebezpečná". Například, bude-li příloha mít název "Patch.jpg.exe", bude ji avast! chápat jako potencionálně nebezpečnou a zobrazí upozornění. Zároveň se kontroluje, jestli přípona přílohy odpovídá skutečnému typu souboru. Pokud ne, bude opět zobrazeno varovné hlášení. Například pokud soubor "Pamela.jpg" není obrázek (jak by se podle přípony JPG mohlo zdát), ale přejmenovaný COM soubor.

  > Kontrola sekvence bílých znaků.

    Některé viry využívají trik, při kterém za jednu příponu infikovaného souboru vloží velký počet mezer (nebo jiných nezobrazitelných, "bílých" znaků) a teprve potom druhou, skutečnou příponu, která bývá "nebezpečná". Uživatel tak onu druhou příponu vůbec nevidí (je např. o několik řádků níže nebo se nevejde do okna, ve kterém jsou názvy příloh zobrazovány). Heuristická analýza avastu tento trik dokáže odhalit a upozornit na to uživatele. Jako výchozí povolená sekvence těchto znaků je pět. Pokud tedy mezi dvěma příponami bude více než pět bílých znaků, zobrazí se upozornění.

- Citlivost – Střední (navíc k nízké citlivosti).

  > Rozšířená kontrola příloh.

    Pokud příloha připojená ke zprávě má spustitelnou příponu (EXE, COM, BAT atp.), bude zobrazeno varovné hlášení. Ne všechny sobory s takovými příponami

jsou nebezpečné, což bude mít za následek větší množství falešných detekcí, než při zvolení citlivosti nízké.

- Citlivost - Vysoká. (navíc k předcházejícím)

  > Kontrola HTML části zprávy.

  Viry využívají chyb některých e-mailových klientů (zejména nezabezpečených programů MS Outlook a Outlook Express) k tomu, aby se spustily pouhým prohlížením zprávy v náhledovém okně. avast! kontroluje, zda HTML část zprávy neobsahuje tag, který by toto umožňoval. Pokud ano, zobrazí varovné hlášení.

  > Odchozí pošta – kontrola v čase.

  Většina moderních virů se šíří e-mailem a samy sebe rozesílají na adresy uložené v adresáři Windows. Toto rozesílání je typické několika příznaky - ve velmi krátkém čase se odesílají zprávy na velký počet adres, přičemž tyto zprávy mívají stejný subjekt anebo stejnou přílohu. Tyto příznaky avast! sleduje a umí na ně upozornit. Více informací a možnosti nastavení jsou popsány na stránce **Heuristika – rozšířené**.

  > Outbound messages - Mass messages.

  Kromě příznaků popsaných výše, kdy se virus rozesílá v mnoha zprávách odesílaných rychle za sebou, existuje druhý podobný způsob: virus se rozešle jednou zprávou více (mnoha) příjemcům. Dostupný počet příjemců se může nastavit na straně "Heuristika (Pokročilé)".

- Citlivost - Vlastní

  Heuristickou analýzu si můžete touto volbou nastavit podle Vašich představ - pomocí tlačítka "**Upřesnit"**. Zvolte, které součásti heuristické analýzy popsané výše se mají používat.

  Dále můžete zvolit kontrolu struktury subjektu. avast! kontroluje, zda v poli "**Předmět"** není větší množství nesmyslných znaků, což je vždy podezřelé. Pokud např. bude v poli předmět sled znaků " <?*&$^*(^%#$%*_( )", bude zobrazeno varovné hlášení.

- Povolené URL

  Kliknutím na položku "Povolené URL" můžete zadat bezpečné URL, které bude heuristická analýza ignorovat. Pokud chcete URL přidat, klikněte na tlačítko "Přidat" a URL ručně vpište do zobrazené kolonky. Pro odstranění URL ho označte a poté klikněte na tlačítko "Odebrat".

- Tichý režim

  Na této stránce můžete také určit, jakou akci má program provést v případě detekování infikované zprávy.

Heuristika (Rozšířené)

Na této stránce můžete upravit vlastnosti heuristické analýzy týkající se odchozí pošty. Nastavení se použije pouze v případě, že na stránce "Heuristika" máte nastavenu citlivost na **vysokou** nebo **vlastní** . Pouze při zvolené **vlastní** citlivosti je možné toto nastavení měnit.

- Kontrolovaný čas.

  Zadejte čas v sekundách, během něhož bude avast! počítat odesílané zprávy. Jako výchozí je hodnota nastavena na 30 sekund. To znamená, že pokud bude během půl minuty odesláno více než 5 (rovněž výchozí hodnota) zpráv, které mají stejný předmět a/nebo obsahují stejnou přílohu, zobrazí avast upozornění.

- Limitní počet emailů.

  Tato položka určuje počet e-mailových zpráv, které avast! nechá bez povšimnutí odeslat, i když obsahují stejnou přílohu anebo mají stejný předmět. Po překročení tohoto počtu zobrazí avast! varovné hlášení.

- Kontrola podle subjektu (předmětu).

  Je-li tato možnost zvolena, bude avast! zohledňovat text v poli "Předmět" při své heuristické analýze.

- Kontrola podle příloh.

  Při zvolení této možnosti bude avast! při své heuristické analýze zohledňovat přílohy přikládané k odchozím zprávám.

- Absolutní počet.

  Tato hodnota, která je standardně nastavena na 10, určuje počet příjemců jedné odesílané zprávy, po jehož překročení bude zobrazeno varovné hlášení.

Archivy

Tato strana se zobrazí pouze pokud nastavujete residentní ochranu pomocí vlastnosti úlohy z Rozšířeného rozhraní, jak je blíže popsáno na **straně 55**.

Virus

Zde můžete blíže specifikovat, jakou akci program provede po nalezení viru. Také sem se můžete přepnout pouze při konfiguraci úlohy z Rozšířeného rozhraní. Viz. **strana 54**.

3. Network Shield (Síťový štít)

Tento poskytovatel chrání počítač před útoky Internetových červů. Jeho činnost je velmi podobná jednoduchému firewallu, jejž však plně nenahrazuje.

Nastavení

- Zobrazovat varovná hlášení

  Pokud je tato možnost zapnuta, bude se v malém proužku při pokusu o útok síťového červa zobrazovat varovné textové hlášení nad systémovou oblastí (nad hodinami).

- Logování

  Veškeré útoky se budou zapisovat do logovacího souboru, takže budete mít možnost sledovat jejich četnost, historii atd. Poslední zaznamenané útoky budou zobrazeny na následující stránce “Poslední útoky”. Tuto stránku můžete zobrazit pouze z nastavení residentní ochrany po kliknutí na ikonu “a” v systémové liště a zvolení poskytovatele Síťový štít. Poté klikněte na tlačítko “Nastavení” a zvolte záložku “Poslední útoky”.

Poslední útoky

Na této stránce se zobrazuje posledních 10 útoků síťových červů. Informace obsahuje datum a čas útoku, způsob útoku a IP adresu spolu s portem, odkud útok přišel.

4. Outlook/Exchange

Testování

Zde můžete určit typ testované zprávy, testování příloh a těla zpráv.

Příchozí pošta

Na této stránce může nastavit, jak avast! zareaguje na příchozí zprávu, která bude obsahovat virus. Zároveň zde lze zajistit, aby avast! vkládal do příchozích zpráv krátkou poznámku informující o tom, zda zpráva obsahuje či neobsahuje virus (ve formátu TXT nebo HTML). Se všemi infikovanými zprávy bude nakládáno tak, jak je popsáno v nastavení na stránkách “Ukládání virů” a “Upřesnit”.

Odchozí pošta

Zde můžete určit, jestli bude informace o čisté zprávě vkládána k emailu a určit formát zprávy stejně jako v předchozím případě. Infikované zprávy se neodešlou. Můžete také nastavit, aby přílohy, které vkládáte do odchozí zprávy, byly kontrolovány na přítomnost virů už při samotném vkládání a ne až při pokusu o odeslání takové zprávy.

Signatury

Použitím signatur lze výrazným způsobem snížit počet zpráv, které je nutno testovat. Signatury jsou malé "nálepky", které avast! může (je-li to tak nastaveno) do zpráv vkládat v případě, že neobsahují viry. Každá signatura obsahuje datum a čas.

Podstatné je, že signatury poskytovatele MS Outlook/Exchange jsou plně kompatibilní např. se signaturami programu avast!, Exchange Server Edition. Máte-li tedy Exchange

server a na něm provozujete avast!, mělo by ještě dojít k dalšímu podstatnému zrychlení, neboť např. zprávy otestované na serveru poskytovatelem MS Exchange Server již nebudou na klientu poskytovatelem MS Outlook/Exchange znovu testovány.

- **Vkládat signatury do čistých zpráv**.

  Zaškrtnutím tohoto pole zapnete podepisování zpráv. Bude-li toto pole vypnuté, nebude do žádné zprávy signatura zapsána.

- **Věřit všem signaturám**.

  Volba tohoto pole způsobí, že je-li zpráva opatřena platnou signaturou, bude ji poskytovatel důvěřovat bez ohledu na její stáří (alespoň není-li zaškrtnuto další pole "Vždy ignorovat signatury starší než aktuální virová databáze") a testování zprávy neprovede.

- **Nevěřit signaturám starším než**.

  Pomocí tohoto pole můžete nastavit maximální stáří signatur, kterým bude ještě důvěřováno. Hodnotu zde uvedenou může vždy zastínit zaškrtnutí pole "Vždy ignorovat signatury starší než aktuální virová databáze".

- **Nevěřit žádným signaturám.**

  Volba tohoto pole způsobí, že poskytovatel nebude důvěřovat žádným signaturám, a tudíž bude každou zprávu vždy nepodmíněně testovat.

- **Vždy ignorovat signatury starší než aktuální virová databáze**.

  Pomocí tohoto zaškrtávacího pole lze zajistit, aby poskytovatel vždy testoval i zprávy, které sice jsou opatřeny platnou signaturou, avšak datum a čas této signatury jsou starší než právě používaná virová databáze avastu. To může být užitečné, neboť teoreticky je možné, že v mezidobí - mezi původním testováním zprávy a dneškem - přibyl do virové databáze nový vzorek, který je právě obsažen v dané zprávě.

Ukládání virů

Pomocí polí na této stránce lze nakonfigurovat, zda má avast! v případě nalezení viru infikované soubory zálohovat na disk. Po kliknutí na tlačítko “Procházet” můžete určit, do jaké složky se infikovaný objekt uloží. Pokud zaškrtnete políčko “Přepisovat případné existující soubory”, všechny soubory se stejným jménem budou nahrazeny souborem novým.

Upřesnit

- Tichý režim

  Pokud je na stránce Virus přednastavena interaktivní akce, tak se po zaškrtnutí této položky infikovaný soubor přesune přímo do truhly.

  Jestliže je zapnutá jakákoliv jiná akce než akce interaktivní, zaškrtnutí položky "Tichý režim" nebude mít na zvolenou akci žádný efekt.

- Zobrazovat detailní informace o činnosti.

  Toto zaškrtávací pole určuje, zda bude poskytovatel při své činnosti zobrazovat detailní informace o své činnosti. Informace jsou zobrazovány v pravé dolní části obrazovky. Např. pro každý testovaný objekt.

- Při testování pošty zobrazovat ikonu na liště.

  Je-li toto pole zaškrtnuto, bude avast! při každé své činnosti se zprávou zobrazovat na na systémové liště v pravém dolním rohu malou ikonku, která symbolizuje, že poskytovatel právě něco dělá.

- Při spouštění zobrazovat úvodní obrázek.

  Pomocí tohoto zaškrtávací pole můžete nastavit, aby poskytovatel zobrazoval při spouštění podporovaného poštovního programu své logo.

Nakonec můžete určit MAPI profil a heslo, které se použijí při procházení složkami po kliknutí na tlačítko "Procházet".

Heuristika

Nastavení na této stránce je stejné jako u poskytovatele Internet Mail

Heuristika (Rozšířené)

Nastavení je také stejné jako u poskytovale Internet Mail mimo dvou rozšířených možností:

- Relativní počet

  Zde je možné změnit relativní počet příjemců zprávy, po jehož překročení avast! zareaguje. Tento údaj se uvádí v procentech uživatelů, jejichž e-mailové adresy jsou uloženy v seznamu adres Windows (windows address book). Výchozí hodnota je 20%.

- Minimálně však

  Zde lze nastavit minimální počet příjemců v souvislosti s relativním počtem. Např. pokud by v adresáři Windows byl takový počet příjemců, že 20% z nich by tvořilo méně než 10 adres, avast! bude tento relativní počet ignorovat, dokud nepřekročí hranici 10 příjemců.

Archivy

Tato stránka se zobrazí pouze z nastavení residentní ochrany v okně úloh rozšířeného uživatelského rozhraní. Více informací naleznete na page 55.

Virus

Zde můžete blíže specifikovat, jakou akci program provede po nalezení viru. Také sem se můžete přepnout pouze při konfiguraci úlohy z Rozšířeného rozhraní. Viz. page 54.

5. P2P Štít

Programy

Na této stránce vyberte programy, které mají být poskytovatelem P2P štít chráněny. Ochrana některých programů je k dispozici pouze na operačních systémech Windows NT, 2000, XP, Vista nebo 2003.

Archivy

Tato stránka se zobrazí pouze z nastavení residentní ochrany v okně úloh rozšířeného uživatelského rozhraní. Více informací naleznete na **straně 55**.

Virus

Zde můžete blíže určit, jakou akci program provede po nalezení viru. Také sem se můžete přepnout pouze při konfiguraci úlohy z Rozšířeného rozhraní.

Viz. **strana 54**.

6. Script Blocking

Chráněné programy

Na této stránce zaškrtnutím zvolte, pro které prohlížeče Internetu si přejete blokování skriptů zapnout.

Upřesnit

- Zobrazovat úvodní okno při spouštění.

  Pokud zvolíte tuto možnost, bude se při každém spouštění poskytovatele Script blocking zobrazovat na několik málo sekund úvodní okno (splash screen), informující o tom, že poskytovatel je aktivní.

- Zobrazovat detailní informace o činnosti.

  Pokud zvolíte tuto možnost, bude Vás rezidentní ochrana informovat o souborech, které v daný okamžik testuje. Tyto informace uvidíte v řádcích v pravém dolním rohu obrazovky nad systémovou lištou.

- Tichý režim

  Pokud zaškrtnete tuto možnost, tak program při detekci podezřelého scriptu zablokuje přístup k dané webové stránce.

Virus

Na této stránce lze určit, jaké operace budou provedeny v případě, že úloha nalezne virus. Také sem se můžete přepnout pouze při konfiguraci úlohy z Rozšířeného rozhraní. Viz. **strana 54**.

7. Standartní štít

Testování (Základní)

Na této stránce zadáváte oblasti testování. Doporučujeme zaškrtnout všechny položky na stránce, aby byly testovány soubory na všechny možné typy virů.

Testování (Upřesnit)

Na této stránce můžete blíže upřesnit, zda se další soubory mají testovat na základě koncovky. A to buď při otevření souboru, při jeho vytvoření nebo jeho změně.

- **Prohledávat soubory při otevírání**.

  Jednotlivé přípony oddělte čárkou. Můžete použít i zástupný znak "?" (např. pokud chcete, aby byly testovány otevírané soubory .htm a .html, uveďte do řádku buď "htm,html" nebo použijte zástupný znak - "ht?"; v druhém případě však budou testovány všechny soubory, jejichž přípona začíná znaky "ht", tedy i např. "htt").

  > **Vždy prohledávat WSH - skriptovací soubory**.

    Touto volbou zajistíte, že budou testovány všechny skriptovací soubory (Windows Scripting Host).

  > **Neprohledávat systémové knihovny**.

    Oficiální systémové knihovny se při otevírání nebudou testovat, provede se pouze rychlá kontrola jejich autenticity. Tato volba může mírně zrychlit start operačního systému.

- **Prohledávat vytvářené/měněné soubory**.

  Testovány budou nejen soubory, které jsou otevírány, ale i ty jež jsou vytvářeny nebo měněny. Dále můžete zvolit:

  > **Všechny soubory** nebo

  > **Pouze soubory s vybranými příponami**

Pokud je zaškrtnuto “Standartní sada přípon”, vytvářené či měněné soubory budou testovány pouze v případě, že mají některou z "nebezpečných" přípon. Standartní sadu přípon si můžete prohlédnout kliknutím na tlačítko “Zobrazit”. Přidat můžete i další přípony.

Blokování

Na této straně můžete určit, jaké operace s jakými příponami souborů budou blokovány. Pokud zvolíte možnost “Standartní sada přípon”, budou operace blokovány u všech souborů s “nebezpečnými” příponami (znovu si je můžete prohlédnout po kliknutí na tlačitko “Zobrazit”).

Dále můžete blíže určit, jaké operace by měly být pro určité typy souborů blokovány, např. otevření pro zápis, přejmenování, smazání nebo formátování souboru.

Nakonec určete, co program provede, pokud jedna z blokovaných operací čeká na potvrzení z Vaší strany. Tzn. jestli bude operace povolena nebo zakázána.

Pokročilé

- **Zobrazovat detailní informace o činnosti**.

  Pokud zvolíte tuto možnost, bude Vás rezidentní ochrana informovat o souborech, které v daný okamžik testuje. Tyto informace uvidíte v řádcích v pravém dolním rohu obrazovky nad systémovou lištou.

- **Tichý režim**

  Přednastavená akce po detekování podezřelého souboru je akce interaktivní. Pokud je zvolen také tichý režim, program se se všemi infikovanými soubory vypořádá podle následujícího pravidla:

  > Jestiže je zapnuto “s odpovědí Ano” všechny infikované soubory přiložené k emailové zprávě budou automaticky smazány.

  > Pokud je zvoleno “s odpovědí Ne”, infikovaný soubor bude automaticky přesunut do virové truhly.

  Při přednastavené akci po detekování podezřelého souboru a vypnutém tichém režimu se zobrazí normální okno nalezení podezřelého souboru a program se Vás zeptá, jakou akci chete s infikovaným souborem provést.

  Jestliže je zapnutá jakákoliv jiná akce než akce interaktivní, zaškrtnutí položky “Tichý režim” nebude mít na zvolenou akci žádný efekt.

  Nakonec můžete zadat oblasti, které v tichém režimu testovány nebudou. Oblasti zadané pro ostatní poskytovatele se v tomto seznamu neobjeví.

Archivy

Tato stránka se zobrazí pouze z nastavení residentní ochrany v okně úloh rozšířeného uživatelského rozhraní. Více informací naleznete na **straně 55**.

Virus

Zde můžete blíže určit, jakou akci program provede po nalezení viru. Také sem se můžete přepnout pouze při konfiguraci úlohy z Rozšířeného rozhraní. Viz. **strana 54**.

8. Webový štít

Tento poskytovatel funguje jako lokální proxy server. Na Windows s technologií NT (NT, 2000, XP, Vista a 2003) pracuje zcela transparentně a není většinou potřeba nic zvláštního nastavovat. Na Windows řady 9x je pro správnou funkci nutné změnit jediné nastavení v Možnostech Internetu a sice adresu a port lokálního serveru. Chcete-li tedy tohoto poskytovatele na starších Windows používat, postupujte následovně:

Při použití místní sítě (LAN):	Při použití připojení dial-up (modem):
Spusťte Internet Explorer.	Spusťte Internet Explorer.
V nástrojové liště zvolte **Nástroje → Možnosti Internetu**.	V nástrojové liště zvolte **Nástroje → Možnosti Internetu.**
Přepněte na záložku **Připojení**.	Přepněte na záložku **Připojení**.
Klikněte na tlačítko **Nastavení místní sítě.**	Kliknutím v seznamu označte Vámi používané telefonické připojení a klikněte na tlačítko **Nastavení.**
Zaškrtněte možnost **Používat pro síť LAN server proxy**	Zaškrtněte možnost **Používat pro toto připojení server proxy**.
Do pole **Adresa** vepište **localhost** (nebo IP adresu **127.0.0.1**, obojí má stejný účinek). Do pole **Port** vepište číslo portu **12080**.	Do pole **Adresa** vepište **localhost** (nebo IP adresu **127.0.0.1**, obojí má stejný účinek). Do pole **Port** vepište číslo portu **12080**.
Potvrďte tlačítkem **OK**.	Potvrďte tlačítkem **OK**.

Poznámka: Pokud používáte více připojení, je nutné nastavit adresu a port proxy serveru pro každé připojení zvlášť.

Základní

- Zapnout testování WWW

  Tato volba prakticky zapíná či vypíná testování obsahu WWW (funkce blokování URL adres není touto volbou ovlivněna).

- Používat inteligentní proudové testování.

  Je-li tato volba zapnutá, testují se stahované soubory téměř v reálném čase. To znamená, že stažené části souborů jsou testovány průběžně a další části se stahují až v okamžiku, kdy je test ukončen a virus není nalezen. Vypnete-li tuto volbu, dojde nejprve ke stažení celého souboru do pracovního adresáře, kde jej avast! posléze otestuje a předá webovému prohlížeči.

  Následující volby nejsou dostupné na Windows 95, 98 a Millennium:

- Přesměrované HTTP porty.

  Toto nastavení má význam zejména v případech, kdy pro přístup na Internet používáte nějaký proxy server a chcete testovat komunikaci mezi ním a Vaším počítačem. Používáte-li tedy proxy server a komunikujete s ním např. na portu 3128, zadejte číslo tohoto portu. V opačném případě bude avast! předpokládat komunikaci pouze na portu 80 (výchozí) a ostatní bude ignorovat. **Poznámka:** Nezadávejte jiné porty než HTTP (čili žádné porty pro ICQ, DC++ apod.).
  Jednotlivá čísla portů oddělte čárkou.

- Ignorované adresy.

  Do tohoto řádku můžete vepsat jména serverů nebo IP adresy, které nebudou přesměrovány na avast! proxy. Jednotlivé adresy oddělte čárkou.

- Ignorovat lokální komunikaci.

  avast! bude ignorovat veškerou lokální komunikaci - tj. komunikaci mezi jednotlivými programy v rámci Vašeho počítače.

Testování WWW

Na této konfigurační stránce volíte, které stahované soubory má avast! testovat. Můžete vybrat všechny soubory nebo pouze soubory s určitou koncovkou. Pokud zvolíte druhou možnost, musíte do kolonky vložit koncovky souborů (oddělené čárkou), které chcete testovat. Zadat můžete i MIME typy objektů, které budou programem avast! testovány.

Vyjímky

Na této stránce můžete nadefinovat objekty, které nebudou Webovým štítem testovány. To je vhodné např. při stahování velkého množství souborů z jedné (důvěryhodné!) adresy - serveru.

- Netestovat URL

  Tlačítkem **Přidat** zadejte URL adresu, která bude ignorována. Chcete-li zadat konkrétní stránku, nezapomeňte uvést celou cestu. Zadáte-li např. *http://www.seznam.cz/index.html*, nebude testována pouze stránka *index.html.* Pokud ovšem zadáte *http://www.seznam.cz/**, nebudou testovány žádné stránky začínající *http://www.seznam.cz*. Podobně pokud nechcete testovat konkrétní typ souboru, např. soubory s příponou *txt*, zadejte pouze **.txt*.

- Netestovat MIME typy

  Zde můžete zadat jednotlivé MIME typy/podtypy, které nebudou testovány.

Blokování URL

Webový štít je schopen i blokovat přístup na určené WWW stránky. Použití této funkce je ponecháno na Vašich potřebách a fantazii. Nabízí se např. možnost zakázat některým členům rodiny přístup na určité stránky (porno, "warez" atd.). Při pokusu o zobrazení takovéto blokované stránky se uživateli objeví stránka jiná, informující o tom, že přístup na zadanou stránku byl programem avast! zablokován.

Volba "**Zapnout blokování URL"** musí být zaškrtnuta, pokud chcete přidat adresy k zablokování**.** Pomocí tlačítka **Přidat** vložte masku adresy, která bude blokována. Můžete používat zástupné znaky **?** a *****. Například při zadání *http://www.freefoto.cz/** nebudou zobrazeny žádné stránky začínající adresou *http://www.freefoto.cz*.

avast! sám doplňuje URL adresy dle následujících pravidel:

Pokud zadaná adresa nezačíná řetězcem *http://* nebo zástupnými znaky * či *?*, avast! doplní na začátek adresy *http://* a na konec přidá hvězdičku. Zadáte-li tedy adresu *www.seznam.cz*, avast! ji změní na *http://www.seznam.cz**

Pokročilé

- Zobrazovat detailní informace o činnosti.

  Povolíte-li tuto možnost, budete o činnosti Webového štítu informováni krátkými textovými zprávami objevujícími se nad systémovou oblastí (nad hodinami).

- Tichý režim

  Při zaškrtnutí této možnosti bude po detekci podezřelého souboru spojení ihned přerušeno.

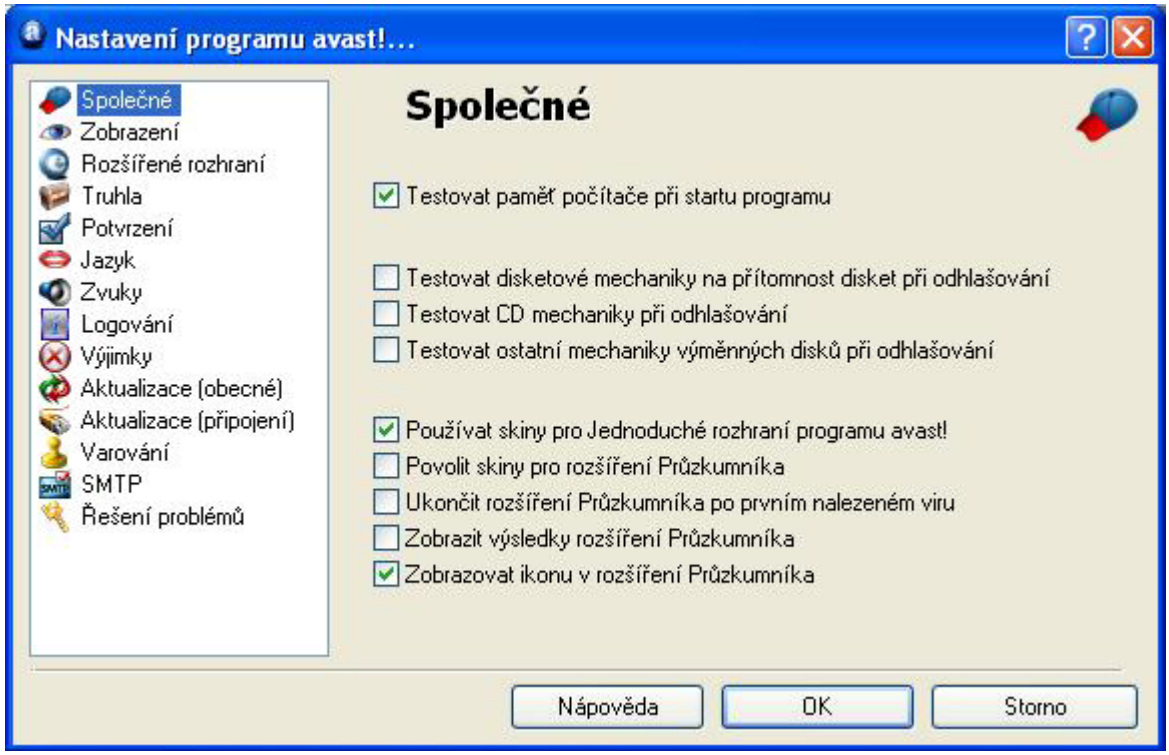
Archivy

Tato stránka se zobrazí pouze pokud nastavujete residentní ochranu pomocí vlastnosti úlohy z Rozšířeného rozhraní, jak je blíže popsáno na straně 55.

Další nastavení programu avast!

Pomocí široké palety možností nastavení chování avastu si jej můžete přizpůsobit Vašim potřebám. Některé z nastavení byly již popsány na předchozích stranách uživatelské příručky.

Pokud používáte jednoduché uživatelské rozhraní a otevřete **Menu jednoduchého rozhraní**, klikněte na "Nastavení". Zobrazí se následující okno. Z rozšířeného uživatelského rozhraní stejné okno zobrazíte také kliknutím na "Nastavení".



Společné

V tomto okně můžete určit, jaké kontroly se provedou po vypnutí či zapnutí počítače. Změnit můžete i vzhled programu vypnutím či zapnutím skinů.

Pozšíření Průzkumníka

Poslední čtyři položky slouží ke konfiguraci Průzkumníka. Pomocí něho můžete testovat jakýkoliv soubor či složku kliknutím pravým tlačítkem myši přímo na ně a zvolením "Testovat <jméno souboru>".

Zobrazení

Po kliknutí na "Zobrazení" můžete určit, zda se bude residentní modrá ikona objevovat v systémové liště a zda bude se bude při prováděném testu otáčet.

Přidat můžete i speciální vizuální efekty, které se projeví po přístím restartu počítače.

Rozšířené rozhraní (zobrazí se pouze pokud zrovna používáte Rozšířené rozhraní)

Můžete určit, zda budou v seznamu úloh zobrazeny i speciální úlohy, jako je rozšíření Průzkumníka nebo Spořič obrazovky (viz. strana 65). Budou-li tyto úlohy zobrazeny, lze také modifikovat jejich parametry.

Zaškrtnutím možnosti "**Posouvat výsledky seance"** budou výsledky seance automaticky posouvány směrem vzhůru, nevejdou-li se již do okna výsledků (tedy tak, aby byl vždy vidět poslední výsledek).

V poslední zaškrtávací položce můžete nastavit, po kolika dnech se mají smazat ukládané seance.

Potvrzení

Na této stránce lze volit, které dotazy a hlášení se mají během práce s programem zobrazovat.

U nezatržených položek se potvrzovací okno nebude zobrazovat; to může mít za následek např. nechtěné smazání úlohy. Vypnutí zobrazování potvrzovacích oken doporučujeme pouze zkušeným uživatelům - některé operace jsou nevratné!

Následující potvrzení jsou přednastaveny jako zapnuté, ale mohou být samozřejmě vypnuty:

- ***Dotaz před uzavřením jednoduchého rozhraní, pokud probíhá testování.*** Pokud je program ukončen v průběhu testování, test se automaticky přeruší.

- ***Dotaz před úpravou běžící residentní úlohy.***

  Tato zpráva se zobrazí, pokud se rozhodnete ukončit jednotlivou residentní úlohu – viz. strana 22. Jesliže zvolíte "Ano", jednotlivé moduly zůstanou vypnuty dokud je znovu neaktivujete. Pokud zvolíte "Ne", zaktivují se při dalším restartu počítače.

- ***Dotaz před zastavením rezidentní ochrany***

  Tato zpráva se zobrazí, pokud se rozhodnete ukončit residentní úlohu jako celek (viz. strana 19 Pokud zvolíte "Ano", residentní ochrana zůstane vypnutá, ale automaticky se zapne při příštím restartu počítače.

- ***Dotaz před mazáním souborů z truhly***

  Při zaškrtnutí této položky se program vždy dotáže na potvrzení smazání souboru.

- ***Hlášení o úspěšném zpracování výsledků***

  Potvrzení, že všechny akce, které mají být programem reportovány, byly provedeny úspěšně.

- ***Hlášení o chybách při zpracování výsledků***

  Zpráva o tom, že akce, která měla být reportována programem, nemohla být provedena.

- ***Zpráva při používání starého VPS souboru***

  Upozornění na to, že Vaše virová databáze je zastaralá. Pravidelně aktualizovaná virová databáze je nutná k zajištění plné ochrany systému. Více informací naleznete na straně 34.

- ***Hlášení o BETA verzi programu***

  Zpráva, která Vás upozorní, že používáte testovací verzi programu.

- ***Zobrazit zprávu po úspěšném zaslání zprávy o chybě***

- ***Ukázat dialog v Truhle, pokud byla akce provedena úspěšně***

Pokud je položka zaškrtnuta, dostanete zprávu k potvrzení úspěšně provedené akce.

- ***Zpráva při vybraných OK výsledcích v konfiguraci úlohy***

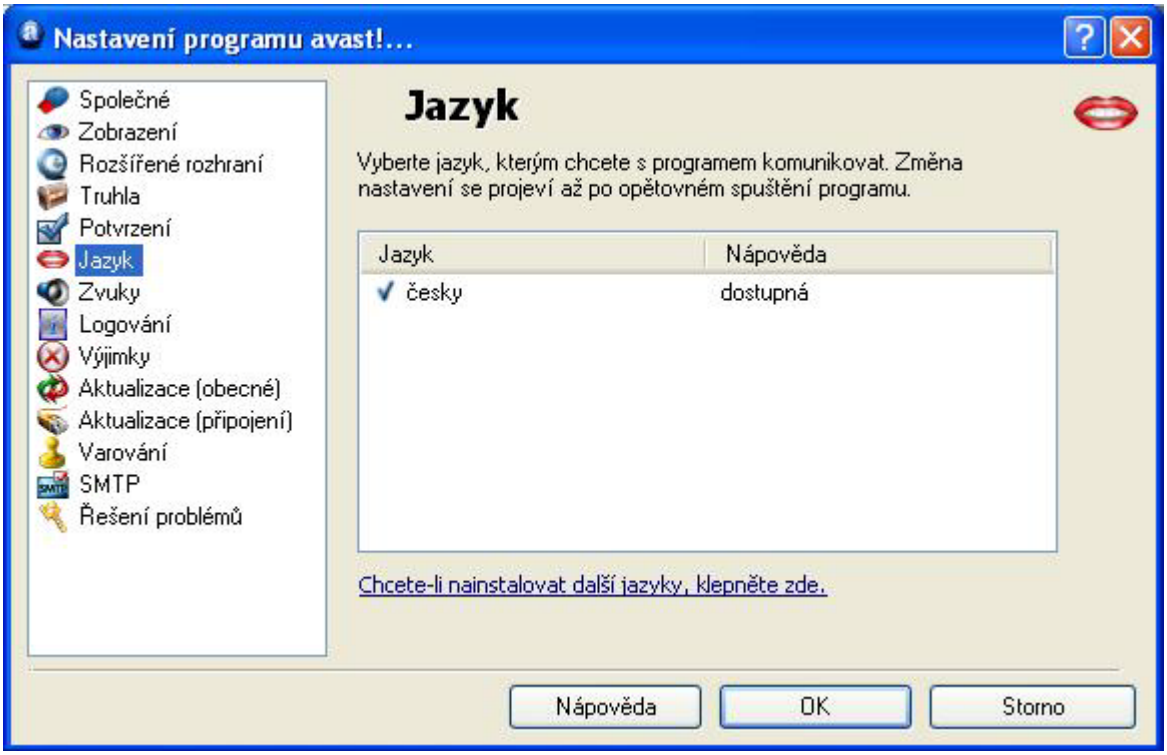
  Při zaškrtnutí se Vám zobrazí varování vždy, když určíte, že "OK soubory" mají být součásti výsledků testu. Toto platí pouze pro vytváření úloh v rozšířeném uživatelském rozhraní.

- ***Mazání souborů s nebezpečnou příponou***

  Varování, že soubor, který chcete smazat, je souborem obsahujícím důležitá data.

Změna Jazyka programu

Pokud chcete změnit jazyk, kterým s Vámi program bude komunikovat, klikněte na “Jazyk”. Objeví se následující okno:



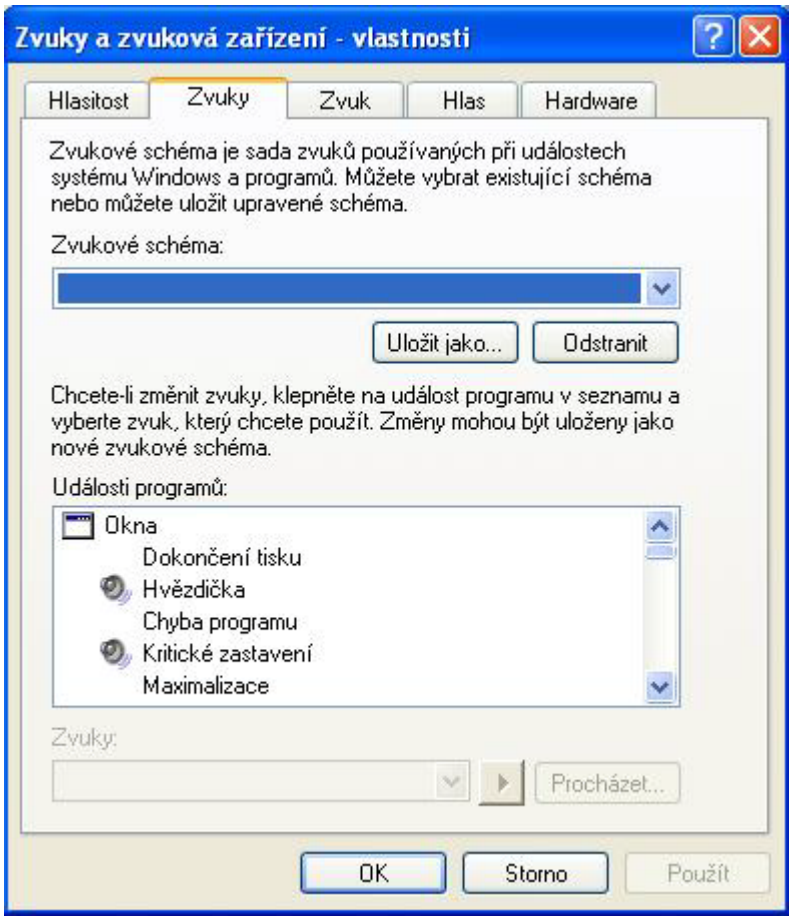
Pokud je Vámi požadovaný jazyk uveden v pravém okně, zvolte ho, a klikněte na tlačítko “OK”. Změna nastavení se projeví po opětovném spuštění programu.

Jestliže tam požadovaný jazyk zobrazen není, klikněte na “Chcete-li nainstalovat další jazyky, klepněte zde.” Potom zaškrtněte políčko s příslušným jazykem a klikněte na tlačítko “Další”. Instalaci další jazykové verze ukončíte kliknutím na “Dokončit”.

Zvuky

Na této stránce můžete nastavit nebo úplně vypnout zvuky v programu avast!

Po kliknutí na tlačítko "**Nastavení"** se zobrazí standardní okno nastavení zvuků prostředí Windows. Konkrétně stránka "**Události programů"**.



V nabídce "Události programů" se nachází i sekce "avast! antivirus" a seznam zvuků přiřazených jednotlivým událostem programu avast!. Chcete-li nastavit nový zvuk, klikněte na příslušnou položku ze seznamu a potom na tlačítko "Procházet...". Ze seznamu vyberte zvuk, který si přejete nastavit a potvrďte stisknutím tlačítka "OK".

Potom se vrátíte zpět do okna zobrazeného výše. Klikněte na "Použít" a znovu "OK".

To Vás znovu vrátí do hlavní nabídky nastavení zvuků, kde změnu znovu potvrďte kliknutím na tlačítko "OK".

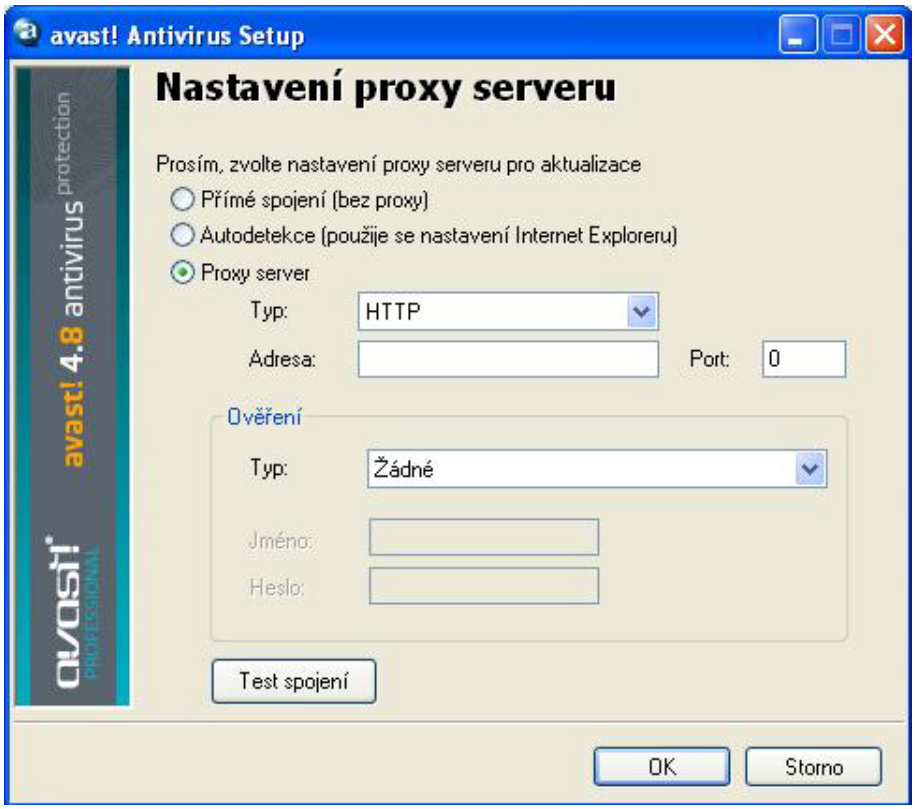
Aktualizace (připojení)

V tomto okně můžete zaškrtnutím příslušné položky určit typ Internetového připojení. A to buď

- Pro přístup k Internetu používám výhradně vytáčené připojení (modem), nebo
- Můj počítač je neustále připojen do sítě Internet

Tímto nastavením můžete optimalizovat detekci a stahování aktualizací virové databáze a programu.

Poté co určíte typ připojení, klikněte na tlačítko "Proxy". Zobrazíte okno, ve kterém lze změnit nastavení proxy serveru. Nastavení proxy serveru je důležité ve chvílích, kdy avast! potřebuje přistupovat k Internetu, např. při aktualizacích.



Pokud se k Internetu připojujete přímo (nepoužíváte proxy), zvolte možnost "Přímé spojení". To platí většinou pro uživatele, kteří se na Internet připojují vytáčenou linkou (modemem).

Pokud nevíte, zda využíváte proxy server a jaký, zvolte možnost **"Autodetekce"**, případně se obraťte na Vašeho poskytovatele připojení k Internetu (providera) či správce sítě.

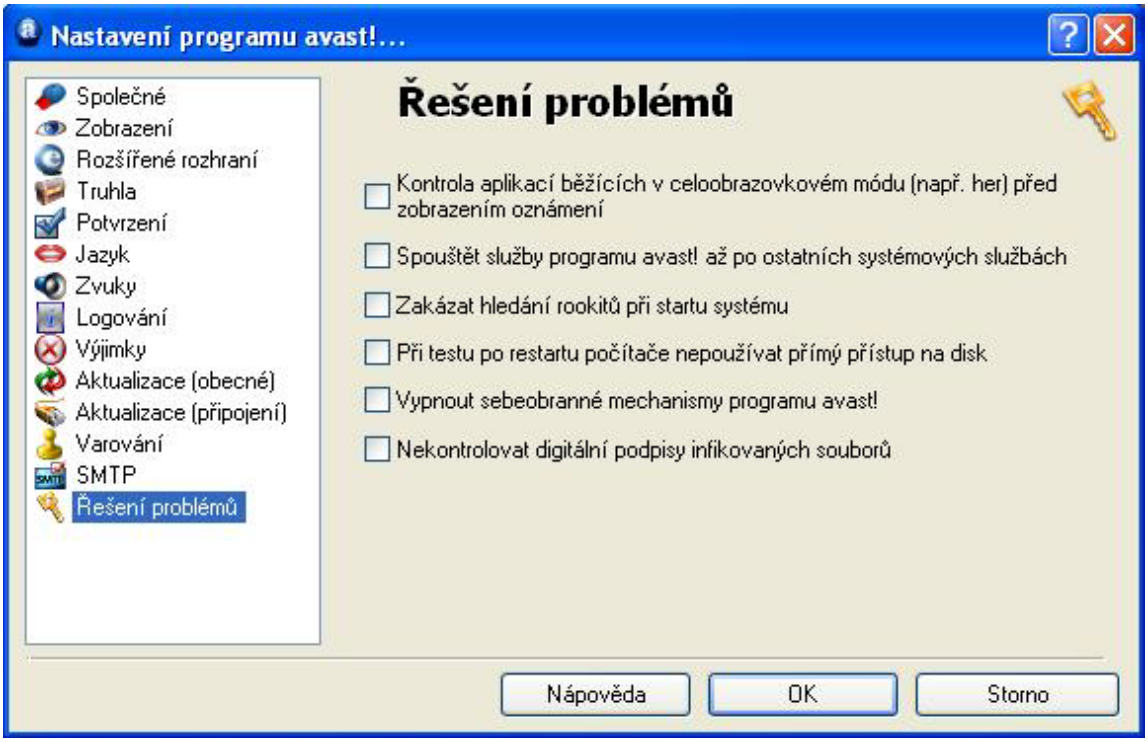
Pokud znáte adresu a port Vašeho proxy serveru, zvolte možnost "Proxy server" a zadejte následující údaje:

- **Typ**. HTTP nebo SOCKS4
- **Adresa**. Vepište adresu proxy serveru.

- **Port**. Uveďte port proxy serveru.
- **Ověření**. Pokud je přístup k síti Internet přes proxy server zabezpečen nutným ověřením, nastavte zde příslušné ověření.
- **Jméno a heslo**. Zvolte, pokud je tento typ ověření požadován.

Nakonec klikněte na tlačítko "Test spojení", čímž ověříte, zda je zde nastavené spojení se sítí Internet v pořádku.

Řešení problémů



Změna nastavení na této stránce Vám může pomoci při různých problémech. Nicméně neměla by být prováděna, pokud k tomu nemáte žádný důvod. Pokud si nejste jisti některým z těchto nastavení, kontaktujte podporu společnosti ALWIL software.

Kontrola aplikací běžících v celoobrazovkovém módu (např. her) před zobrazením oznámení.

V závislosti na nastavení programu avast! se mohou při chodu počítače zobrazovat různé zprávy (např. zprávy o aktualizaci virové databáze nebo o testování příchozích zpráv). Zprávy se zobrazí vždy, když probíhá příslušná událost. To může vést k přerušení některých aplikací, které běží v celoobrazovkovém módu (např. her). Pokud zaškrtnete tuto možnost, avast! bude detekovat běžící aplikace. Jestliže zjistí, že běží v celoobrazovkovém módu, nezobrazí žádnou zprávu.

Spouštět služby programu avast! až po ostatních systémových službách

Služba programu avast! antivirus se spouští brzy v procesu bootování. Při spouštění jiných služeb to může někdy způsobovat problémy (jako např. chvilkové zamrznutí po startu počítače). Tato možnost proto umožňuje odložit start služby programu avast! a spustit ji až po startu služeb ostatních.

Zakázat hledání rootkitů při startu systému

avast! testuje počítač na přítomnost rootkitů při každém startu systému. Při zaškrtnutí této položky rootkity testovat nebude.

Při testu po restartu počítače nepoužívat přímý přístup na disk

Při naplánování testu po restartu avast! používá speciální metodu přímého přístupu na disk, což mu umožní detekovat viry, které své soubory skrývají. Zde můžete tuto možnost vypnout, program poté bude používat standartní metodu přístupu na disk.

Vypnout sebeochranné mechanismy programu avast!

Některé viry jsou schopné vypnout běžící antivirový program, smazat jeho soubory nebo je změnit. avast! proto obsahuje sebeochranné mechanismy, které umožňují takto nebezpečné operace zablokovat. Pokud chcete sebeochranné mechanismy vypnout, zaškrtněte toto políčko.

Nekontrolovat digitální podpisy infikovaných souborů

Aby se avast! vyhnul falešným detekcím, kontroluje digitální podpisy testovaných souborů. Pokud je soubor detekován, ale obsahuje digitální podpis, jedná se s největší pravděpodobností o falešný poplach a avast! bude takovou detekci ignorovat. Po zaškrtnutí této položky bude program hlásit všechny detekované soubory.

Jak používat test z příkazové řádky

Program ashCmd, je běžně nainstalován v adresáří C:\program files\alwil software\avast4.

Program ashCmd se ovládá výhradně z příkazové řádky za pomoci **přepínačů** a **parametrů**. Pokud chcete vidět popis všech příkazů, přepněte se do výše uvedeného adresáře a spusťe soubor ashCmd. Seznam všech parametrů také nleznete v nápovědě programu avast! v části "Program ashCmd".

Chcete-li spustit antivirový test, přepněte se do příkazového řádku Windows a zadejte jméno souboru ashCmd spolu s oblastí, kterou chcete testovat a s příslušným parametrem. Například pokud chcete otestovat všechny lokální disky, příkaz bude vypadat následovně:

*C:\Program Files\Alwil Software\Avast4 ashCmd.exe /**

Můžete přidat i další parametry. Pro test jednotlivého souboru vpište jeho adesářovou cestu a ujistěte se, že jméno obsahuje všechny potřebné znaky uzavřené závorkami, jak můžete vidět níže.

C:\Program Files\Alwil Software\Avast4 ashCmd.exe c:\"program files"

Chcete-li spustit úlohu vytvořenou programem avast!, potom za znaky "/@=" (tj. za parametr zavináč) napište její jméno.

Například pro úlohu "týdennítest" bude příkaz vypadat takto:

C:\Program Files\Alwil Software\Avast4 ashCmd.exe /@=týdennítest

Úloha se provede tak, jak je v programu avast! nastavená. Ostatní parametry budou na řádce ignorovány.

Obsahuje-li jméno úlohy mezeru, musí být uvedeno v uvozovkách.

Po skončení testu mohou být výsledky uloženy použitím parametru"/_>". Tedy např. "ashCmd.exe c:\windows /_> test.txt" otestuje adresář C:\Windows a výsledek testování zapíše do souboru test.txt, který vytvoří v adresáři, kde je nainstalován avast!

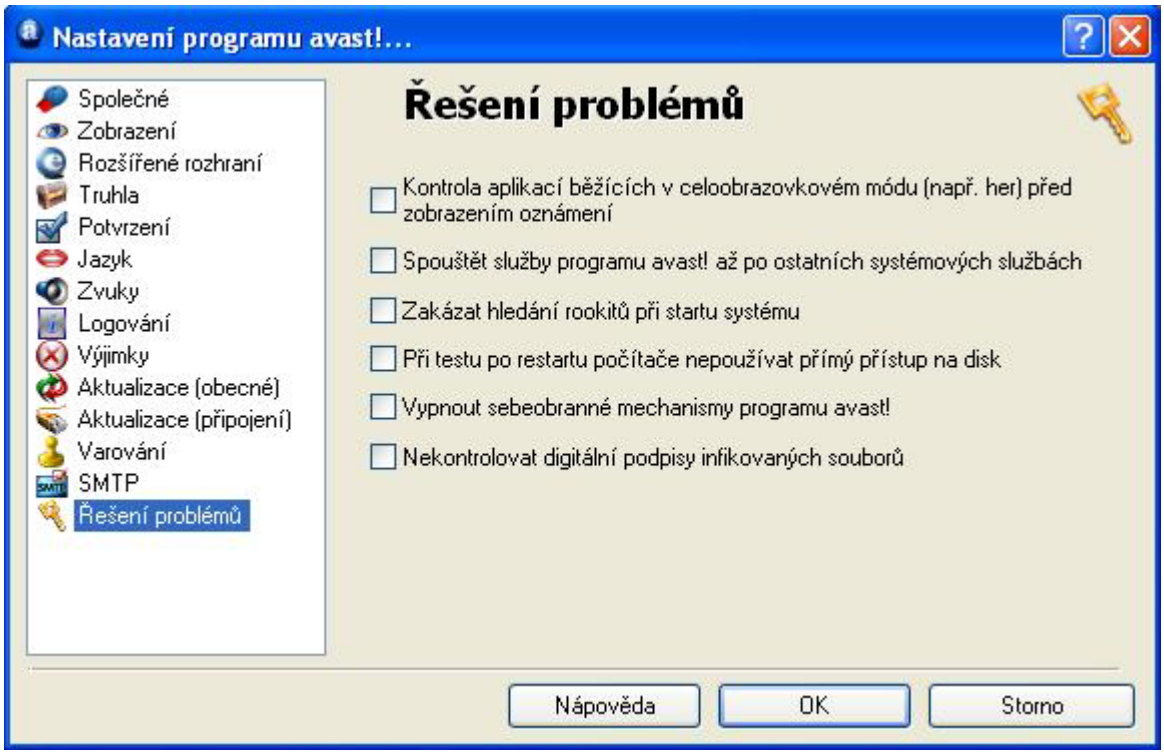
Jak odinstalovat program avast! antivirus

Některé viry jsou schopné vypnout antivirový program na počítači. Proto je avast! vybaven silnými sebeochrannými mechanizmy, které zabraňují smazání nebo změně souborů programu avast!. Kůli tomu může nastat při odstraňování problém. Pokud chete avast! odstranit, musíte dodržet přesný odinstalační proces.

Nejdříve Vám doporučujeme zavřít všechny ostatní běžící aplikace. Pro odinstalaci programu avast! postupujte následujícím způsobem:

1. Vypněte sebeochranné mechanismy programu avast!

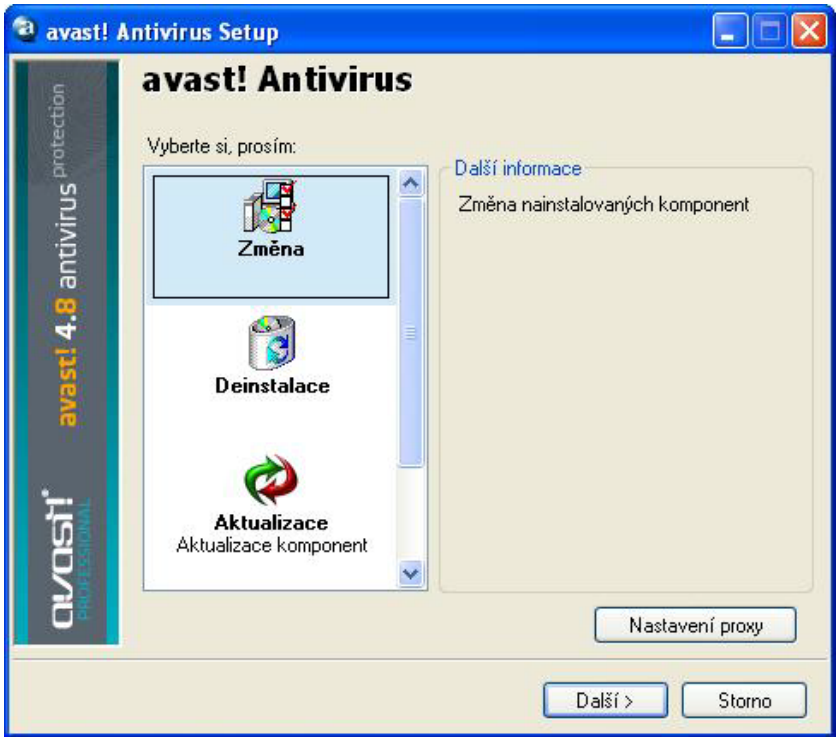
- Klikněte pravým tlačítkem myši na modrou ikonu a v systémové liště a ze zobrazeného menu vyberte “Nastavení programu”.
- Klikněte na “Řešení problémů” na levé straně. Objeví se toto okno:



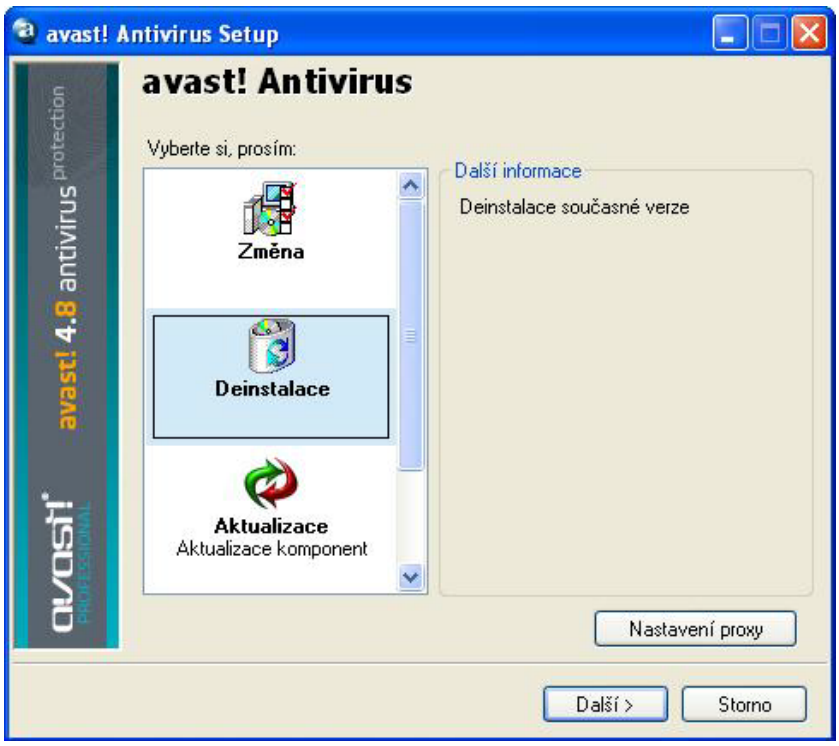
- Zaškrtněte položku “Vypnout sebeochranné mechanismy programu avast!” a klikněte na tlačítko “OK”.
- Sebeochranné mechanismy jsou nyní vypnuty.

2. Odstraňte program

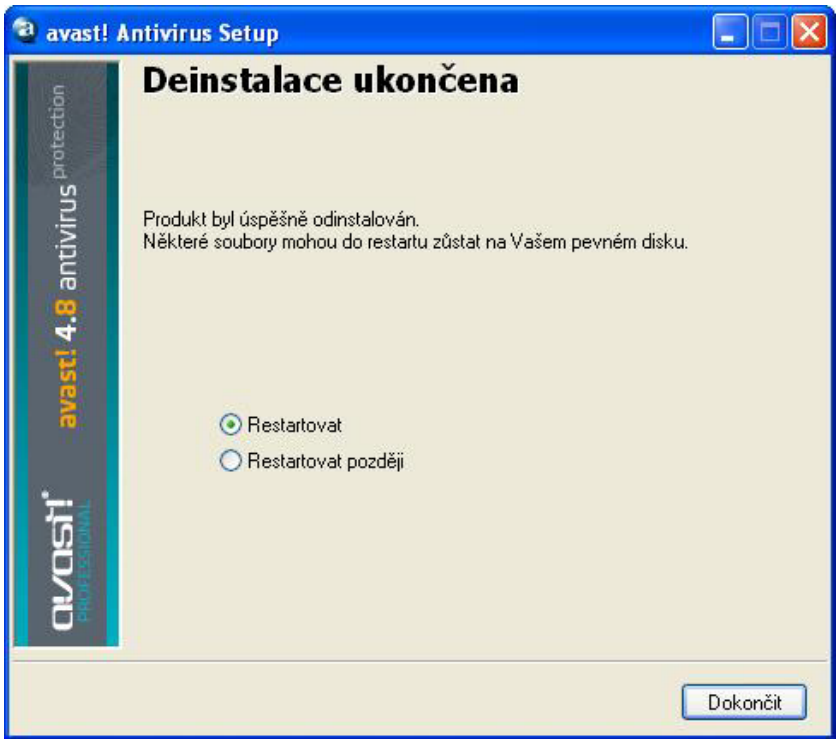
- Klikněte na “start” vlevo dole na obrazovce počítače a otevřete Ovládací panely.
- V ovládacích panelech klikněte na “Přidat nebo odebrat programy”.
- Zobrazí se seznam všech nainstalovaných programů.
- Vyberte “avast! antivirus” a poté klikněte na “Změnit nebo odebrat”.
- Zobrazí se následující okno:



Klikněte na “Deinstalace” a potom na “Další”



Program bude odinstalován a zobrazí se následující okno:



Pro dokončení odinstalačního procesu je nutné restartovat počítač. Nechte zvoleno “Restartovat” a klikněte na “Dokončit”. Váš počítač bude automaticky restartován.