Nastavení bezpečnostních programů

Rychle a bezpečně

NAJDETE NA CHIP DVD

AntiVir 7.0 PE	freeware	www.free-av.com
Ad-Aware SE PE 1.06	freeware	www.lavasoft.de
AVG plus Firewall 7.1 Chip	plná verze	www.grisoft.cz
Sygate PE FW 5.0	shareware	http://soho.sygate.com
Spamihilator 0.9.9.9	freeware	www.spamihilator.com
BitDefender 9 Internet Security	zkušební verze	www.bitdefender.cz

Bezpečnost na internetu, nebo rychlý systém? Obojí! Ukážeme vám, jak spolu mohou virový skener, firewall a spamový filtr optimálně spolupracovat, a to s redukcí výkonnostních brzd a zbytečných varování a při plně komplexní ochraně.

Text: Valentin Pletzer, *autor@chip.cz*

V TOMTO ČLÁNKU NAJDETE

Zní to jako noční můra. Nahrajete si do počítače balík bezpečnostních programů, a zbrusu nový počítač je najednou pomalý jako nějaký veterán z roku 1995. Bootování trvá celou věčnost, odeslání mailu je zkouškou trpělivosti, radost z her kazí cukající se obraz.

Pomalu, ale jistě – tak zní deviza současných kompletních řešení sestávajících z firewallu, antivirového programu a spamového filtru. Počítač sice ochrání před všemi nebezpečími ze sítě, avšak jejich nesmírný hlad po paměťovém prostoru dokáže zbrzdit každý systém. Drastickým příkladem může být souprava Panda InternetSecurity 2006, která pro sebe zabere tučných 91 MB operační paměti. Ale i ty nejskromnější bezpečnostní nástroje si ještě nárokují přes 40 MB (viz graf).

Kromě paměti vás však tyto balíky připraví i o nervy. Plynulost práce narušují neustálé – a často zbytečné – varovné zprávy. A přitom by strážci bezpečnosti měli uživateli práci spíše ubírat!

Máme však pro vás dobrou zprávu: Svou „security suite“ si můžete vychovat. Správným nastavením zredukujete nepříznivé vlivy na výkon počítače a zbavíte se znervózňujících varování. Zároveň své bezpečnostní nástroje optimalizujete tak, aby přesně odpovídaly vašim hardwarovým požadavkům. Jak se dobrat k bezpečnostnímu i výkonnostnímu optimu, to vám ukážeme na konkrétním příkladu stříbrného medailisty našeho dřívějšího testu „bezpečnostních balíků“, kterým je BitDefender 9 InternetSecurity 2006 (viz Chip 2/06). Postup však bude podobný i pro ostatní současné bezpečnostní balíky.

ANTIVIROVÝ PROGRAM

Strážce virů lze bez obav vypnout

Nejprve se věnujme virovému skeneru. Ten totiž často brzdí systém i v případech, kdy vůbec není potřebný. Tak je tomu například vždy, když pracujete off-line nebo hrajete hry. Dokud pak totiž nepřipojíte USB paměť s cizími soubory nebo nezaložíte céčéčko s potenciálními viry, nemůže se nic stát. Platí proto základní pravidlo: Pokud do počítače nenahráváte žádná nová data, vypínejte přechodně antivirovou ochranu. U bezpečnostního balíku BitDefender se to dělá takto: Klikněte na ikonu *Antivirus* v levém sloupci a v okně Štít zrušte zatržítko u položky „Virový štít je zapnutý“. Typickým příkladem zde může být instalace softwaru, jako je MS Office. Při ní by aktivní virový skener každý (!) instalační soubor jednotlivě prověřoval – je to zdlouhavé a v daném případě zbytečné.

Podobné funkce pro dočasnou deaktivaci ochrany nabízejí i ostatní bezpečnostní balíky.

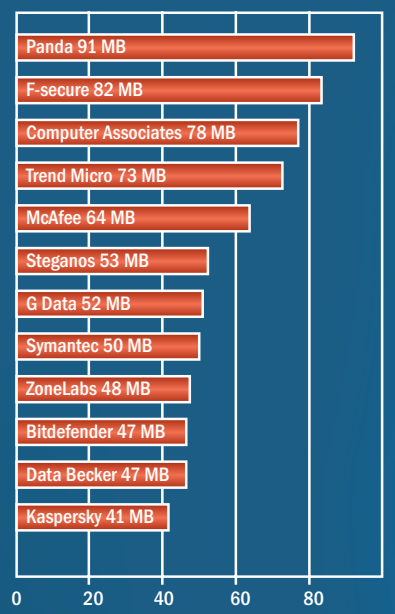
ANTIVIROVÝ PROGRAM

Skenování jen určitých souborů

Dokud pracujete on-line nebo v počítači spouštíte cizí soubory, bylo by příliš nebezpečné virový skener odstavit. V případě nutného skenování ho však alespoň může- →

SPOTŘEBA SYSTÉMOVÝCH PROSTŘEDKŮ

Požírači paměti: Současné softwarové soupravy zajišťující bezpečnost na internetu potřebují mnoho RAM – některé dokonce přes 60 MB.



Brzda **Spojení na domácí síti můžete otevřít a minimalizovat tak chybová hlášení...**

te donutit k efektivnější činnosti a ušetřit tak vzácný výpočetní výkon.

Otevřete proto BitDefender, pak klikněte na *Antivirus* a tam zvolte *Pokročilý*. Zde (v sekci testování přípon, které definuje uživatel) stanovíte, které soubory má antivir kontrolovat. Tímto způsobem je možné ho donutit testovat pouze to, co potřebujete, a ignorovat „okolní balast".

ANTIVIROVÝ PROGRAM

Vypnutí skenování síťových jednotek

Kdo své počítače propojil do malé domácí sítě, může uvolnit další z brzd snižujících rychlost. Předpokladem ovšem je, že ve všech PC je instalován bezpečnostní software. Většina těchto souprav totiž kontroluje nejen lokální počítače, ale i síťové adresáře. A to opět na úkor užitečného výkonu – zejména v případech, kdy je síťové spojení právě zaneprázdněno jinou činností. Pokud si jste tedy jisti, že všechny počítače v síti jsou chráněny, deaktivujte skenování sítě.

Příslušnou volbu najdete v Bitdefenderu pod *Antivirus* | *Pokročilý*. Tam v dolní části okna najdete položku „Zadejte cesty, které nechcete testovat".

FIREWALL

Deaktivace firewallu v privátní síti

Zrovna ta nejdůležitější zbraň proti hackerským útokům, firewall, dokáže nejvíc obtěžovat. Pokud totiž není nakonfigurován naprosto exaktně, neustále svého uživatele bombarduje varovnými zprávami nebo mu bez okolků přeruší spojení s internetem.

Důvod je prostý: Mnohé aplikace používají porty, které firewall nepovažuje za bezpečné – týká se to například sdílení ve Windows a služby RPC (vzdálené volání procedur). Tyto služby jsou typickými vstupními branami hackerských útoků. Firewall proto odpovídající porty pro jistotu uzavře, a navíc ještě uživatele znervózňuje nesrozumitelnými zprávami.

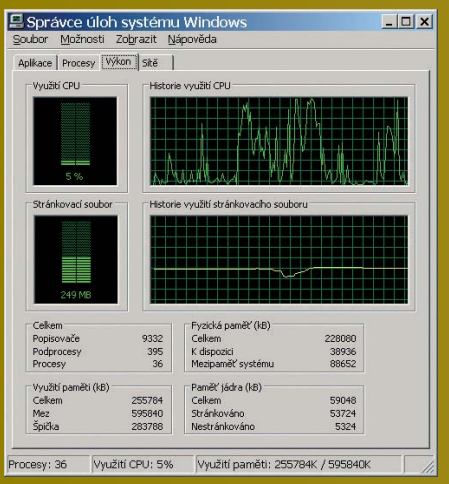
Takové zablokování portů má samozřejmě smysl ve směru k internetu – mezi jednotlivými PC v domácí síti ovšem nikoliv. Tato spojení proto můžete otevřít a minimalizovat tak chybová hlášení i přerušení spojení.

Nakonfigurujte si tedy firewall tak, aby veškerý provoz na těchto adresách portů v žádném směru neblokoval. Při tom vám pomůže toto pravidlo: Pro privátní sítě jsou rezervovány tři adresní prostory, totiž 10.255.255.255, 172.16.255.255 a 192.168.0.255. Ty proto zadejte bezpečnostnímu softwaru. V našem konkrétním příkladu toto nastavení můžete upravit v okně *Firewall* | *Přenos*. Zde po kliknutí na ikonu složky se znaménkem „+" můžete vytvořit nové pravidlo pro provoz na lokální síti.

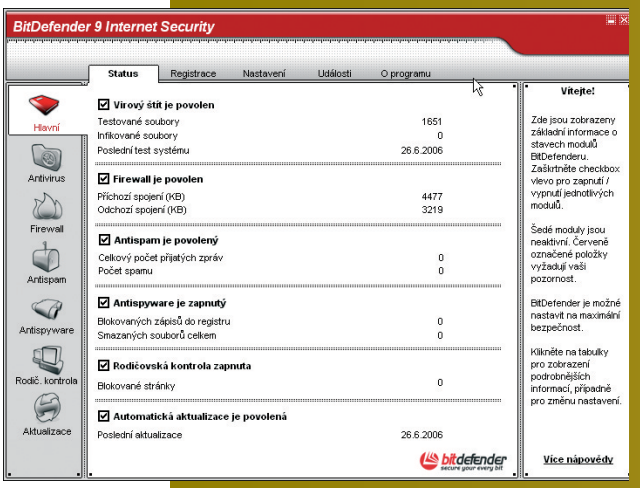
FIREWALL

Odsunutí lokálního firewallu

Bez příslušné ochrany se váš počítač nejpozději do 15 minut stane obětí hackerského útoku nebo napadení červem. Avšak rychle a bez stresů běží Windows jenom bez lokálního firewallu – že by šlo o neřešitelnou antitezi? Nikoli, firewall se totiž dá přemístit na jiné místo! Pokud jsou všechny počítače v síti nezavirované, nemusí mít každý z nich vlastní ochranu.



Náročný **Při aktualizaci zatížil BitDefender testovací počítač s CPU Celeron 2,3 GHz na přibližně 60 – 70 %.**



Cena za bezpečí **Kompletní bezpečnostní balík zajistí ochranu počítače ze všech úhlů, ovšem za nemalou cenu.**

Spamový filtr **Odesilatele a domény, jejichž zprávy určitě chcete dostávat, zapište na „whitelist".**

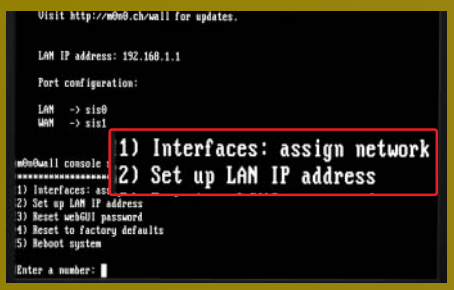
PROFESIONÁLNÍ FIREWALL SKORO ZDARMA

Odlehčete své počítače a zároveň zvyšte jejich ochranu – pomocí opensourcového firewallu M0n0wall a odloženého počítače, který předřadíte. Tak zdokonalíte svou domácí síť a uspoříte drahocenné systémové prostředky pod Windows.

1 Hardware: Pro připojení přes DSL postačí starý PC 486 s alespoň 64 MB operační paměti. Pokud je vybaven disketovou jednotkou, nemusí mít pro pozdější uložení nastavení firewallu ani pevný disk. Dvě síťové karty jsou ovšem předpokladem, aby mohly být sítě navzájem odděleny i fyzicky.

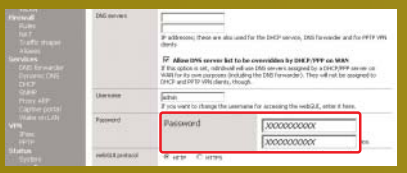
2 Instalace: Freeware M0n0wall je vlastně operační systém pro „krabici“ s firewallem – v podobě komfortního boot-image. Pod Windows si jej například můžete otevřít v Neru a vypálit. Pozor! Je důležité, aby jak mechanika, tak BIOS starého PC dovolovaly i bootování z CD.

3 Zadání adres: Po zavedení programu se objeví prostá ovládací plocha. Nejprve pod bodem menu „1“ zřiďte dva síťové adaptéry. Při tom musí být síťové kabely zastrčeny. Potom pod bodem „2“ nastavte IP adresy obou síťových karet. Pak počítač prozatím odpojte od internetu.



4 Webová konfigurace: Ostatní nastavení proveďte z libovolného počítače v síti. Ve webovém prohlížeči k tomu zadejte jen IP adresu firewallu. Standardně má firewall adresu „192.168.1.1“, ovládací plochu najdete na *http://192.168.1.1,* přihlašovací jméno a heslo je vždy „m0n0“.

5 Základní nastavení: Na webové ovládací ploše jděte nejprve na bod *General Setup,* kde se zhostíte nastavení hlavních parametrů. Zde zadáte například DNS server, ale také do systému vložíte aktuální čas, abyste později při analýze protokolu poznali, kdy došlo k útoku. Nezapomeňte také v *General Setup* změnit přihlašovací jméno a heslo. Přednastavené jméno byste v žádném případě neměli ponechat.



6 Pravidla firewallu: Srdce firewallu, seznam pravidel, definujete v menu *Firewall.* Které možnosti máte k dispozici a které pro vás mají smysl, to se nejlépe dozvíte na adrese *www.m0n0.ch/wall/documentation.php.* Jakmile pravidla nadefinujete, znovu připojte internetový kabel – a váš M0n0wall je připraven k provozu.

Tu tedy můžete umístit do nějakého předřazeného prostoru. Mnozí uživatelé – aniž by o tom měli tušení – tak mají například firewall v DSL routeru. Jinou možností je postavit si ze starého PC firewall hardwarový; jak na to, to se dozvíte v rámečku na této straně.

ANTISPAM

Rychlejší vytřiďování mailů pomocí „whitelistu“

Spamové e-maily okrádají o čas. Hlavně tehdy, je-li filtr v bezpečnostním softwaru nastaven tak ostře, že důležité zprávy špatně vytřídí kvůli podezření na spam. Tohoto problému se zbavíte použitím tzv. „whitelistu“, který poštu od důvěryhodných odesilatelů propustí.

V našem demonstračním balíku najdete příslušné nastavení pod *Antispam | Seznam přátel/spammerů.* Tam klikněte na „trojitou šipku“ vpravo od vybrané položky (seznam přátel) a zadejte všechny e-mailové adresy (nebo domény), které zaručeně neposílají žádný spam. Chcete-li například, aby žádná zpráva odeslaná z domény *chip.cz* nebyla považována za spam, klikněte na přepínač „Jméno domény“ a zadejte do políčka „@chip.cz“. Pokud hodláte dát „zelenou“ jen konkrétnímu odesilateli, použijte volbu „E-mailová adresa“.

Kromě toho můžete seznam adres a domén importovat a ovládat tak najednou celou řadu odesilatelů. Příslušnou volbu najdete v dolní části okna pod tlačítkem „Načíst“. Některé bezpečnostní soupravy, například produkt F-Secure, nabízejí například možnost přenést do whitelistu celý klientský adresář.

Do doplňujícího „blacklistu“ byste pak měli vkládat pouze adresy, které nevytřídí žádné jiné filtry. Neustále měněné adresy odesilatelů spamu totiž udržování takového seznamu v podstatě znemožňují.

ANTISPAM

Vypnutí antivirové ochrany e-mailů

Přídavná kontrola virů v poštovním programu patří v bezpečnostních soupravách

BEZPLATNÉ NÁSTROJE NA CHIP DVD

TO NEJLEPŠÍ PRO BEZPEČNOST

Pokud jste si dosud nenainstalovali žádnou bezpečnostní soupravu nebo nepotřebujete všechny komponenty, které taková souprava obsahuje, k ochraně vašeho počítače postačí i freeware. Ušetříte tak nejen systémové prostředky, ale i peníze. Jedinou nevýhodou je, že musíte ovládat jednotné ovládací prostředí.

Firewall: Freewarový Sygate Personal Firewall poskytuje lepší ochranu než firewall integrovaný ve Windows XP.

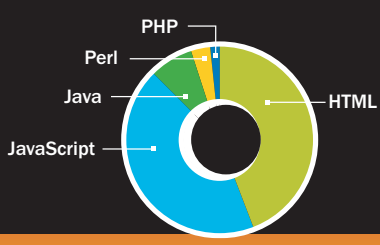
Virový skener: Momentálně nejlepší freewarový antivirový nástroj AntiVir se před komerčními produkty vůbec nemusí stydět.

Antispam: Spamihilator je mezi bezplatnými antispamovými prostředky stále ještě volbou číslo 1

Antispyware: Profesionální řešení Ad-Aware SE je v boji proti spywaru trvale na čelném místě.

ÚTOKY NA WEBOVÉ STRÁNKY

Bezpečnostní balíky jsou dnes důležitější než kdykoli dříve. Objem malwaru na internetu totiž rapidně stoupá. V roce 2005 došlo celkem k 1933 různým útokům na webové prohlížeče. Nejčastěji se škodlivý programový kód skrývá v HTML



Zdroj: G Data Antivirus Lab

Brzda **Rodičovská kontrola může patřit k největším brzdám při surfování...**

k největším systémovým brzdám. Je proto lépe ji vypnout a spolehnout se na virový skener příslušného providera elektronické pošty. Všichni naši velcí poskytovatelé takovou službu nabízejí. V Bitdefenderu tuto možnost najdete pod *AntiVirus | Nastavení štítu.* Tam zrušte zaškrtnutí u *Testovat příchozí poštu.* Tím svému počítači zase o něco ulehčíte. Proaktivní programy jako Outbreak-Shield byste však měli nechat zapnuté. Jimi totiž bezpečnostní software blokuje nová nebezpečí, která virový skener providera dosud nezná.

DĚTSKÁ POJISTKA

Jednoduché odinstalování nepotřebných komponent

Všechny bezpečnostní soupravy už jsou dnes dodávány se spoustou různých vymožeností, které ne každý potřebuje, jako jsou například „dětská pojistka“ a webové filtry. Tady už se vyplatí „vykydat“. Takové nástroje totiž nejen užírají systémové prostředky, ale bývají také příčinou nevysvětlitelných chyb – například se náhle přestanou nahrávat webové stránky. Proto platí zásada instalovat jen to nejnutnější. Programy, které neznáte nebo nepotřebujete, jenom ztěžují práci.

Abyste se takového balastu zbavili, máte dvě možnosti: buď pomocí odinstalační rutiny nepotřebné komponenty odstranit, nebo služby deaktivovat v konfigurační centrále. Druhá cesta ne vždy ušetří systémové prostředky, zato vás však zbaví nesrozumitelných chybových zpráv, které tyto nástroje hojně produkují. ■ ■ ■