

Bezplatné antiviry

Virová ochrana zadarmo: antiviry z našeho testu by měly ochránit počítač před virovou nákazou. Zjišťovali jsme, jaká je skutečnost. *Valentin Pletzer, Vratislav Klega, vratislav.klega@chip.cz*

Zkáza přijde z internetu: podle studie pocházející od Googlu obsahuje přibližně každá desátá stránka spyware, viry a trojské koně. Naštěstí je většina internetových surfařů vybavena antivirovým štítem. V ideálním případě dokáže štít v reálném čase všechny škůdce „odpálkovat“, případně je odstranit později.

Taková ochrana navíc nemusí být ani drahá – koneckonců může být zcela zadarmo. Otestovali jsme tři programy, za které nemusíte zaplatit ani korunu: Avast Home Edition, AntiVir PE a AVG Chip Edition – ten samozřejmě není zadarmo, jakožto čtenáři Chipu jej však můžete používat bezplatně (více informací na Chip DVD). Všechny antiviry fungují pod XP i pod Vistou a měly by být dostatečnou základní ochranou před útoky z internetu. Všechny tři aplikace naleznete na Chip DVD.

» V testu přesnosti

Náš expresní test vyzkoušel programy celkem ve čtyřech disciplínách:

Rozpoznání známého malwaru: Měsíc co měsíc zveřejňují experti na webové stránce www.wildlist.org seznam aktuálních škůdců. Z tohoto seznamu jsme nachechali 1000 škodlivých programů a kódů. AVG nenašlo jednoho škůdce, AntiVir i Avast měly 100% úspěšnost.

Rozpoznání neznámého malwaru: Heuristický engine musí rozpoznávat kódy,

Pro bezpečnost maximum



Jen málokdo si uvědomuje možné důsledky bezpečnostního selhání, dokud nepřijde o data nebo dokud se konkurence díky softwarovým špiónům nedostane k interním dokumentům. V Chipu však děláme pro bezpečnost maximum, a to v každém čísle.

Každý měsíc máte k dispozici plnou výzbroj od AVG – antivír, antispysware a firewall. V tomto čísle například přinášíme následující plné verze bezpečnostních nástrojů:

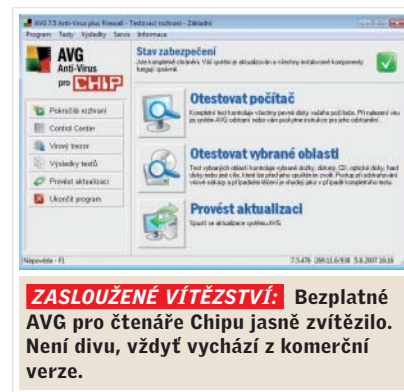
- ▶ Outpost Security Suite Pro 2007 – bezpečnostní balík na šest měsíců;
- ▶ trojice bezpečnostních programů od McAfee (Firewall, SpamKiller, Antispysware) na 12 měsíců;
- ▶ Spy Sweeper ve verzi s antivírem na tři měsíce;
- ▶ šifrovací nástroj Magical Security 2007 bez omezení.

Pro neprůstřelný operační systém navíc přinášíme bezpečnostní updaty a service packy pro Windows 98/2k/XP/Vista (Service DVD).

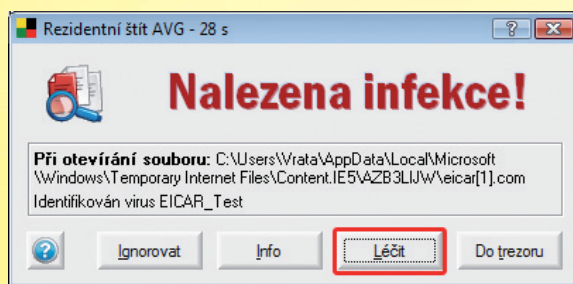
kteří by mohly být potenciálním zdrojem nebezpečí pro počítač. Jedná se jednoznačně o nejtěžší disciplínu. Zde bylo nejlepší AVG, výsledek by však mohl být u všech mnohem lepší.

Reakční doba na nový malware: Čím déle trvá, než antivír získá informace o novém druhu nebezpečí, tím větší je šance škodlivých kódů způsobit ve vašem počítači újmu. Brzká aktualizace je tedy nutnou podmínkou úspěšného antivíru. V této disciplíně vedl AntiVir, AVG mu dýchalo na záda. Avast měl poměrně značnou ztrátu.

Rozpoznání zoo malwaru: Škůdci, kteří nejsou příliš rozšíření a šíří se jen v malém množství, se na seznam Wildlist nedostanou. Jsou pak označováni jako zoo malware. Dobrý antivirový štít by měl tyto škůdce také rozpoznat. Jedná se hlavně o různé back- →



ZASLOUŽENÉ VÍTĚZSTVÍ: Bezplatné AVG pro čtenáře Chipu jasně zvítězilo. Není divu, vždyť vychází z komerční verze.



LÉČIT: To je to správné tlačítko.

Rezidentní štít

Pokud máte štěstí, odhalí antivír nákazu ještě předtím, než se vůbec dostane do počítače. K tomu slouží rezidentní štít. Pro dokonalou funkčnost je však třeba štít vhodným způsobem používat. Jak takový štít funguje?

Při pokusu o stažení nakaženého souboru z internetu se zobrazí podobné okno, jako vidíte vlevo. K dispozici jsou čtyři tlačítka:

▶ **Ignorovat:** Toto tlačítko je nesmyslně hned na první pozici a měli byste se mu zdaleka vyhnout. Pokud jej zvolíte, antivír

nechá škodlivý soubor projít do počítače.

▶ **Info:** Zobrazí veškeré známé informace o tomto viru.

▶ **Léčit:** To je to správné tlačítko. Po kliknutí na něj bude vir deaktivován a vašemu počítači již nijak neublíží. Pokud je vir součástí jiného souboru, nemělo by dojít k jeho poškození – smaže se jen vir, ne celý soubor.

▶ **Do trezoru:** Toto tlačítko již dnes také nemá příliš význam. Infikovaný soubor se uloží do speciální hlídané složky, ve které nezpůsobí žádnou škodu.



Bezpečnost na webu

Otázka bezpečnosti je velmi důležitá a hodně diskutovaná. I na českém webu existují desítky zájmových serverů, které se problematikou zabývají. Představíme vám tři spřízněné stránky.

www.viry.cz – Stránka věnovaná boji s počítačovými škůdci. Přináší i informace ze serveru Virus Bulletin, který se zabývá testováním antivirů.

www.spyware.cz – Informace o všech možných dalších havětech, které jsou zhoubou pro váš počítač.

www.rootkit.cz – Rootkity jsou vůbec největší hrozbou operačních systémů. Na této stránce se dozvíte aktuality i doporučení.

→ doory, boty a trojské koně. Výsledky AVG a AntiViru jsou prakticky vyrovnané, rozhodly desítky. Avast opět mírně ztrácí.

» Silní a slabí

Dobrá zpráva: všechny tři programy se směle mohou rovnat komerčně prodávaným produktům, a to především co se týká rozpoznávání známého malwaru. Zde nezaváhal žádný z testovaných programů.

Rozpoznání neznámého malwaru bylo mnohem horší, heuristické analýzy nejlepších programů nenalezly ani polovinu škůdců. Na vině jsou samozřejmě také stále rafinovanější struktury virů, které odolávají heuristikám. Potom nezbyvá než se spolehat na pravidelné aktualizace ze strany výrobce.

» Shrnutí

Na bezpečnosti se nevyplácí šetřit. Bezplatné antiviry poskytnou jen základní ochranu. Výjimkou je AVG pro čtenáře Chipu, které je

EXPRESNÍ TEST		1. MÍSTO	2. MÍSTO	3. MÍSTO
Název		AVG pro Chip	AntiVir PE Classic	Avast Home Edition
Cena		zdarma pro čtenáře Chipu	freeware	freeware
Internet		www.avg.cz	www.free-av.com	www.avast.cz
Celkové hodnocení		90	78	69
		■■■■■	■■■■□	■■■□□
Shrnutí		Velmi dobrý antivir s vydatnou heuristikou, snadným ovládním a doplňkovými funkcemi.	Vydatný antivir s výkonným enginem a horším ovládním.	Celkem dobrý antivir s příjemným ovládním.
Rozpoznání				
Rozpoznání známého malwaru		99,9 %	100 %	100 %
Rozpoznání neznámého malwaru		36,54 %	26,44 %	10,34 %
Reakční doba na nový spyware		4 - 5 hodin	3 - 4 hodiny	7 - 8 hodin
Rozpoznání backdoorů		99,68 %	99,21 %	94,58 %
Rozpoznání botů		99,04 %	99,76 %	95,57 %
Rozpoznání trojských koní		99,23 %	99,40 %	93,52 %
Funkce				
Operační systémy		Windows 2k/XP/Vista	Windows 2k/XP/Vista	Windows 2k/XP/Vista
Rezidentní štít		●	●	●
Zvláštní e-mailová ochrana		●	-	-
Firewall		●	-	-
Jazyk		česky	anglicky	česky
Podpora		plný support od výrobce	diskusní fórum	diskusní fórum

vlastně komerční verzí a obsahuje kompletní ochranu – antivir, antispyware i firewall. Pokud tedy patříte mezi pravidelné čtenáře, doporučujeme používat AVG. Jedině tento program ochrání váš počítač beze zbytku. Body navíc získal za integrovaný firewall a zvláštní ochranu e-mailových účtů.

Na druhém místě skončil AntiVir, který má výborné výsledky a poměrně dobře ochrání váš počítač před útoky virů. Nevýhodou je složitější ovládní – chybí podpora českého jazyka.

Na konci našeho testovacího pole skončil Avast, který si sice částečně poradí i se spywarem, instalaci čistě antispywarového programu však přesto doporučujeme. Komu nevyhovuje anglické prostředí programu, tomu můžeme Avast doporučit. I když je jeho aktualizace pomalejší a databáze škůdců mírně zaostává, dokáže průměrný počítač, obzvláště v kombinaci s firewallem a antispywarem, docela dobře ubránit. Navíc existuje i ve verzi pro Linux, která je také zadarmo.

Valentin Pletzer, Vratislav Klega, vratislav.klega@chip.cz ■

Boj se spywarem

Výrobci své antiviry necílí na boj se spywarem, proto ani v našem testu nebereme v potaz, jak si se spywarem poradí. K odstranění špiónů totiž existují specializované nástroje, které odvedou lepší práci a jsou více zaměřené právě na signatury špiónů.

K nejlepším antispywarům patří Spybot S&D nebo komerční Anti-SpyWare, jehož plnou verzi naleznete na Chip DVD.

Kdo chce mít počítač skutečně bezpečný, ten potřebuje silnou trojku: antivir, antispyware a firewall. Na to určité nezapomínejte.



Přehled současných hrozeb

Pod pojmem malware rozumíme programy, které škodí počítači a které by měl antivir odstranit. Co všechno lze pod označením malwaru hledat?

► **Adware** hnízdí v počítači a bombarduje vás reklamou.

► **Boty** umožňují internetové mafii, aby ovládala váš počítač. Umožní vzdálené ovládní počítače, takže se z vašeho stroje může stát šířitel spamových mailů, aniž byste to vůbec tušili.

► **Backdoor** otevírá zadní vrátka do vašeho systému. Hacker pak získá přístup k počítači obzvláště snadno.

► **Trojské koně** se vydávají za užitečné programy, ve skutečnosti způsobují netušícímu uživateli škodu.

► **Wormy** jsou malé škodlivé programy, které využívají mezer v operačním systému.

► **Sniffery** zasahují především do vašeho soukromí. Odchytávají dění na počítači a to zasílají svému tvůrci. Nejčastěji sniffery odposlouchávají ICQ, ale také jakoukoliv další komunikaci.

► **Viry** v klasickém významu se dnes již prakticky nevyvíjejí. Jejich cílem je další šíření a provádění určené činnosti – například mazání souborů. K tomuto účelu modifikují své nositele – běžné soubory.