Nejlepší ochrana vašeho počítače

Bezpečnostní balíky nabízejí **PROFESIONÁLNÍ OCHRANU** počítače i pro méně zkušené uživatele, obvykle ale počítač také zpomalují. Chip otestoval, zda jsou produkty pro rok 2009 opravdu rychlejší a jak kvalitní je jimi nabízená ochrana.

FABIAN VON KEUDELL

Surfujete po internetu jen po večerech a o víkendech? Tak to vás některé bezpečnostní balíky mohou opravdu překvapit. Podle hodnocení vyhlášeného antivirového testovacího centra AV-Test poskytují někteří výrobci, jako například F-Secure, během víkendu menší „virovou podporu", a jejich konkurent Panda Security dokonce mezi časným ránem a časem snídaně nenabízí absolutně žádné aktualizace. V tom případě se tedy musíte spoléhat na to, že aktuální antivirové knihovny zajistí, aby se z vašeho PC nestalo „zombie" – počítač ovládaný hackery. Někteří výrobci očividně věří, že období mezi aktualizacemi dokáží dobře překlenout i pomocí tzv. „behaviour detection", technologie, která odhalí neznámé viry podle chování.

Moderní bezpečnostní balíky poskytují ochranu nejen před malwarem a spywarem, ale také před hackery a phishingem. Komplexní balíčky se tudíž skládají z více navzájem propojených komponent: virového scanneru, firewallu a ochrany proti spamu.

ZÁVĚR

Náš vítěz testu Norton Internet Security nabídl nejlepší detekční schopnosti a nejpřátelštější rozhraní a ovládání. Také jeho systémové nároky jsou ve srovnání s předchozí verzí nižší, i když je zde stále ještě prostor pro zlepšení. Stříbrný Kaspersky a bronzový F-Secure jsou v některých oblastech o něco rychlejší, F-Secure však vyřazuje ze hry jeho rozhraní a ovládání.

To je pro programátory vždy výzva, protože jednotlivé komponenty musí být dobře integrovány do systému, a to bez zbytečného zatěžování počítače. Ovládání musí být snadné i pro nováčky, což znamená, že by uživatel neměl narazit na žádná nesrozumitelná chybová hlášení.

Nové verze těchto komplexních ochránců jsme tedy otestovali z hlediska jejich detekčních schopností, výkonu a ergonomie. Také vám ukážeme, který bezpečnostní balík je rychlý a přehledný, a tudíž poskytuje dokonalou ochranu před hackery. Ochrana 24 × 7 (24 hodin 7 dní v týdnu) je dnes už úplnou samozřejmostí, a to i proto, že každých 30 sekund je v nějakém koutu světa vyvinut nový malware...

Detekce: Neexistuje 100% ochrana

Nejdůležitějším kritériem při hodnocení bezpečnostních balíků jsou schopnosti při odhalování malwaru a rychlost reakce výrobců v případě nových hrozeb. Jakmile je nebezpečný software výrobcem nástroje identifikován, přestává být pro uživatele hrozbou. Téměř většina balíků dokázala identifikovat přes 98 % známých hrozeb, pouze Panda zaostala s 91,8 %. V případě spywaru je situace trochu jiná: zdaleka ne všechny nástroje odhalí více než 98 %. Symantec a Panda zvládnou slušných 95 %, BitDefender dokonce pouhých 88 %. Doba do odpovědi na novou hrozbu je u většiny výrobců dvě hodiny, v případě Pandy a BitDefenderu jsou to až čtyři hodiny, přičemž během této doby spoléhají na zmiňovanou „behaviour" detekci.

Tato proaktivní detekce skutečně dobře funguje u balíku od firmy F-Secure a u nástroje od firmy G Data. Čím častěji jsou však virové signatury aktualizovány, tím pochopitelně lépe. Vítěz testu Symantec poskytl během jednoho měsíce přibližně 6 200 aktualizací signatur. V případě Pandy to bylo 58 a například poslední Avira nabídla 126 aktualizací. Bez ohledu na to, zda jde o detekci proaktivní, nebo na základě získaných signatur, nejsou žádoucí falešné poplachy. Během skenu 2,5 milionu souborů náš vítěz testu ani jednou neselhal – to nezvládl žádný z jeho konkurentů.

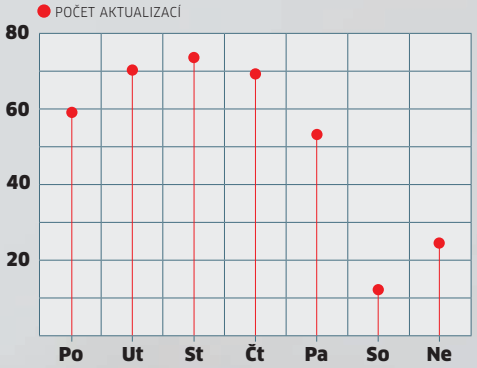
Rychlost: Podstatně lépe než minule

Bezpečnostní balíky by měly zajišťovat bezpečnost, aniž by na počítači překážely. Zde patří k důležitým kritériím především zabraná paměť RAM (zaplněná především virovým monitorem). A kdo je největší nenasyta? BitDefender si rezervuje 82 MB, Avira 80 MB. Všechny ostatní balíky se dokáží spokojit asi s 50 MB, Symantec může zabrat až 60 MB. To je ve srovnání s loňskými výsledky jednoznačný pokrok – je vidět, že výrobci své produkty opravili: minule zabraly některé balíky až 200 MB paměti. Další příznivou novinkou ve srovnání s předešlým testem je fakt, že při běžné práci na PC bezpečnostní balík sotva kdy zahlédnete.

Největší rozdíly jsme naměřili při virové kontrole počítače. Vítěz testu od Symantecu potřeboval pro kompletní sken pouze 33 minut, nejpomalejší byla Panda s 97 minutami. A jak je to s ochranou při kopírování dat nebo při stahování z internetu? Balíku od firmy

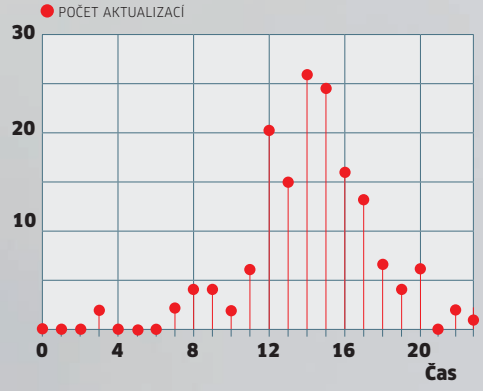
F-SECURE: AKTUALIZACE JEN V PRACOVNÍ DNY

Zdá se, že experti firmy F-Secure mají víkendy volné…



PANDA: AKTUALIZACE BĚHEM DNE

Panda nabízí bezpečnostní aktualizace především během normální pracovní doby.



INFO

Detekce na základě chování

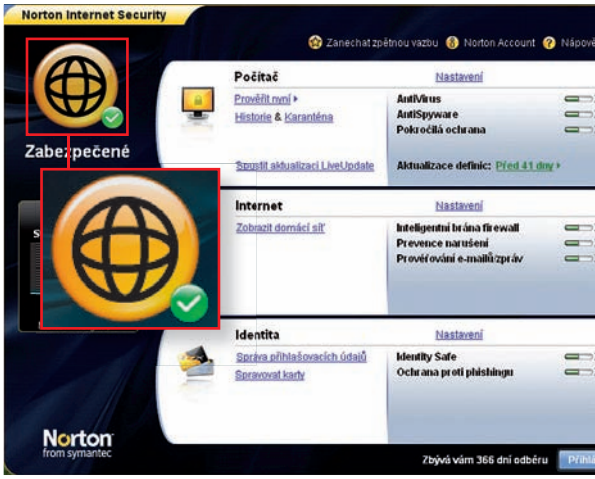
Bitva mezi hackery a výrobci bezpečnostních nástrojů se často odehrává v několika málo minutách. Pokud se v libovolném programu objeví bezpečnostní mezera, dokáží ji útočníci zneužít během krátké doby – obvykle mnohem rychleji, než výrobci dodají pro bezpečnostní nástroje potřebné aktualizace. A právě to je chvíle, kde pomáhají detekce „na základě chování“. Antivirový program kontroluje nová data již v paměti, tzn. dříve, než se dostanou na disk uživatele. Během několika milisekund si bezpečnostní software vytáhne data z paměti a zkontroluje jejich „chování“. Pokud najde podezřelé „přístupy“, dá soubor do karantény a informuje uživatele. Tímto způsobem lze téměř odstranit prodlevu mezi objevením zranitelnosti a dodáním aktualizace. V žádném případě by tento typ kontroly neměl tvořit jedinou ochranu počítače.

Kaspersky trvá kontrola při kopírování 500 MB dat (s velkými či malými soubory, EXE soubory a DLLs) pouhých 38 sekund, naopak balík od firmy G Data k tomu potřebuje téměř o minutu více. Při stahování 370 MB nebyly rozdíly mezi jednotlivými produkty příliš velké, pouze Avira vyžaduje o něco více času než konkurence. Shrneme-li tedy všechny naměřené hodnoty, zjistíme, že z hlediska výkonu dominují bezpečnostní balíky Kaspersky a F-Secure, jen v těsném závěsu za nimi se pak umísťuje Norton Internet Security.

Podpora: Křiklavé rozdíly

Některé balíky otravují uživatele mnohem více než ostatní. „Attack jumper22. dll from UDP 2355" – je vám to jasné? Podíváte-li se do tabulky na sekci ergonomie, ihned poznáte, kde je i „stav bezpečnosti" pochopitelný na první pohled. Balík, který varuje před útokem v zašifrovaném jazyce, k nalezení řešení problému příliš nepřispívá.

Kromě BitDefenderu žádný z testovaných produktů nenabízí užitečné průvodce. S „problémem nastavování" se nástroje musí vypořádat pomocí promyšleného a snadno ovladatelného rozhraní. V této oblasti získává body především Symantec. Pro současnou verzi balíku výrobce kompletně upravil rozhraní, což se mu skutečně povedlo. Uživatel ihned vidí, zda je vše v pořádku, zda jsou signatury aktualizované a kolik zdrojů nástroj vyžaduje. Z konkurence sto-



Vše je v pořádku: Vítěz testu od Symantecu ukazuje stav bezpečnosti systému přehledně už na „titulní straně".

VÍTĚZ TESTU 01/2009

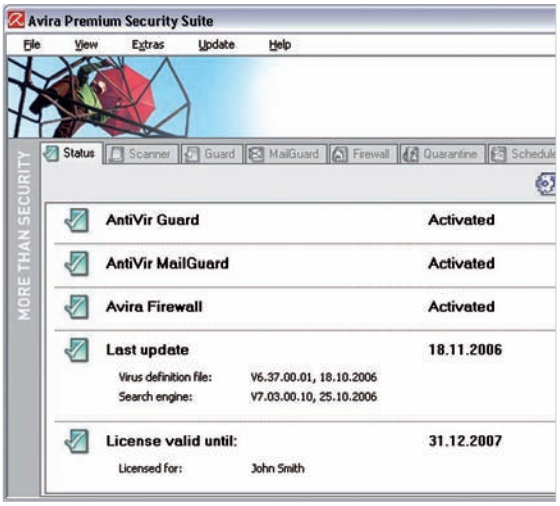
POŘADÍ 1–7	1. MÍSTO	2. MÍSTO	3. MÍSTO	4. MÍSTO	5. MÍSTO
Produkt	Norton Internet Security 2009	Kaspersky Internet Security 2009	F-Secure Internet Security 2009	G DATA Internet Security 2009	BitDefender Internet Security 2009
Orientační cena *	1 270 Kč	1 190 Kč	1 520 Kč	35,95 Eur	1 356 Kč
Internet	www.symantec.com	www.kaspersky.com	www.f-secure.com	www.gdata.de/portal/GB/	www.bitdefender.com
Počet licencí	1	1	3	1	1
Celkové hodnocení	89	88	86	84	75
Detekce (40%)	89	78	81	88	79
Výkon (35%)	87	96	95	76	67
Ergonomie (25%)	92	91	83	88	81
Poměr výkon/cena	dobrý	velmi dobrý	dobrý	dobrý	uspokojivý
Detekční schopnosti					
Rozpoznaný známý malware (1 164 662 variant)	98,7%	98,4%	99,2%	**99,8%**	97,6%
Rozpoznaný spyware (94 291 variant)	95,4%	98,3%	99,6%	**99,8%**	**88,0%**
Falešné poplachy (u 2,5 mil souborů)	žádné	4	2	2	2
Ochrana proti neznámému malwaru	dobrá	dobrá	velmi dobrá	velmi dobrá	velmi dobrá
Reakční doba výrobce na nové hrozby	maximálně 2 hodiny	maximálně 2 hodiny	maximálně 2 hodiny	maximálně 2 hodiny	maximálně 4 hodiny
Počet updatů (1.8. - 28. 8. 2008)	**6 202**	696	145	543	424
Antiphishingová ochrana/rozšíření do prohlížeče	●/Internet Explorer a Firefox	●/Internet Explorer a Firefox	●/–	●/Internet Explorer a Firefox	●/Internet Explorer a Firefox
Výkon					
Doba skenování systému (24 GB)	**33 minut**	37 minut	38 minut	49 minut	34 minut
Zabraná paměť RAM	61 MB	53 MB	**49 MB**	51 MB	**82 MB**
Kontrola při stahování z internetu (370MB)	34 sekund	**31 sekund**	**31 sekund**	35 sekund	32 sekund
Kontrola při kopírování souborů (500MB)	54 sekund	**38 sekund**	52 sekund	**99 sekund**	90 sekund
Ergonomie					
Rozhraní	Velmi přehledné, varovná hlášení jsou rozdělena podle barevného kódu	Velmi přehledné, varovná hlášení jsou rozdělena podle barevného kódu	Srozumitelné, hlášení příliš malá, ale rozdělená podle barevného kódu	Srozumitelné, hlášení příliš malá, ale rozdělená podle barevného kódu	Příliš mnoho textu, varovná hlášení nelze snadno rozpoznat
Nápověda/průvodce	Extrémně podrobná nápověda/žádný průvodce	Extrémně podrobná nápověda/žádný průvodce	Základní nápověda/žádný průvodce	Podrobná nápověda/žádný průvodce	Podrobná nápověda/základní průvodce
Firewall detekuje nežádoucí programy	automaticky, možná manuální úprava	automaticky, možná manuální úprava	ne zcela, možná manuální úprava	automaticky, možná manuální úprava	ne zcela, možná manuální úprava
Bootovací CD k dispozici/možnost jeho aktualizace	●/●	●/●	●/●	●/●	●/●

* Zdroj: www.sw.cz, www.antivirovecentrum.cz

● Špičková třída (100–90) ● Vyšší třída (89–75) ● Střední třída (74–45) ● Nelze doporučit (44–0)
Všechna hodnocení v bodech (max. 100)

● ano – ne

Údaj nejlepší údaj
Údaj nejhorší údaj



Zatržítka: Uživatelské rozhraní bezpečnostního balíku od Aviry bylo z celého pelotonu nejméně přívětivé...

jí ještě za zmínku balík od firmy Kaspersky, který znázorňuje současný stav zabezpečení počítače pomocí barevného značení a přístup k důležitým možnostem nastavení nabízí přes záložky. Na konci závodního pelotonu je opět Avira. Její rozhraní je plné textů a i ovládání zůstává zbytečně složité – k důležitým informacím se zde musíte proklikat...

Prostor pro zlepšení však najdete i u konkurenčních produktů. Například balík od Pandy by měl zpřehlednit nabízené informace, hlášení o problémech jsou pro méně zkušené uživatele opravdovým oříškem. Další problematickou oblastí je poskytování podpory – pokud umíte anglicky a máte po ruce instant messenger nebo e-mail, příliš zklamaní nebudete. Telefonní podporu však v České republice nabízí jen Symantec, Kaspersky a BitDefender (přes web Antivirovecentrum.cz).

Bootovací CD pro případ havárie počítače nabízí většina z testovaných bezpečnostních balíků a za pozitivum lze označit i fakt, že je obvykle i schopno „updatů". Výjimkou je pouze bootovací CD od Pandy, které je klasickou ukázkou absurdního přístupu – jak vám má pomoci neaktualizovaný nástroj, když se malwaru podařilo „porazit" jeho dospělejšího a „zkušenějšího" sourozence? Smutnou tečku opět dělá Avira, která záchranné bootovací CD nenabízí vůbec. I to může být důvod, proč se tomuto nástroji vyhnout... AUTOR@CHIP.CZ

	6. MÍSTO	7. MÍSTO
	Panda Internet Security 2009	Avira AntiVir Premium Security Suite 2008
	2 450 Kč	1 080 Kč
	www.pandasecurity.com	www.avira.de
	3	1
	71	65
	71	77
	73	63
	69	48
	uspokojivý	dostatečný
	91,8%	99,8%
	95,6%	99,0%
	2	2
	velmi dobrá	dobrá
	maximálně 4 hodiny	maximálně 2 hodiny
	58	126
	●/–	●/–
	97 minut	38 minut
	54 MB	80 MB
	34 sekund	43 sekund
	41 sekund	55 sekund
	Příliš mnoho textu, varovná hlášení nelze snadno rozpoznat	Příliš mnoho textu, varovná hlášení nelze snadno rozpoznat
	Podrobná nápověda/ žádný průvodce	Pouze základní nápověda/ žádný průvodce
	automaticky, možná manuální úprava	automaticky, možná manuální úprava
	●/–	–/–

SOUHRN _ BEZPEČNOSTNÍ BALÍKY

RADY PRO NÁKUP

BEZPEČNOST

Proti novému malwaru vám signatury příliš nepomohou. I z toho důvodu jsme otestovali i detekční schopnosti založené na základě „sledování chování". Dalším důležitým kritériem byl počet falešných poplachů.

SYSTÉMOVÁ ZÁTĚŽ

Nemáte-li na svém počítači rychlý dvoujádrový procesor a 8 GB RAM, bude pro vás důležité i to, kolik ze systémových zdrojů si ukousne bezpečnostní balík. Navíc pokud bude balík příliš náročný při kontrole, znepříjemní vám každodenní práci.

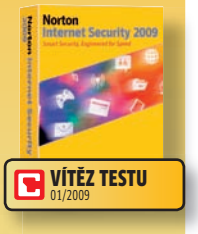
SROZUMITELNOST

Pokud nejste bezpečnostní odborník, měl by mít vámi zvolený produkt srozumitelné ovládání a neměl by vaši pozornost zahlcovat komplikovanými zprávami.

VÍTĚZ TESTU

NORTON INTERNET SECURITY

Bezpečnostní řešení od Symantecu nabízí nejlepší detekční schopnosti, příjemné a srozumitelné ovládání a přijatelné systémové nároky.
CENA: 1 270 Kč



NEJRYCHLEJŠÍ

KASPERSKY INTERNET SECURITY

Z hlediska detekčních schopností sice za vítězem poněkud zaostal, výměnou ale nabízí rychlost a přehledné ovládání.
CENA: 1 190 Kč

JAK JSME TESTOVALI

Spolu s naší redakcí se na testu podílela i renomovaná virová laboratoř AV-Test. Kromě detekce virů a počtu falešných poplachů jsme sledovali i rychlost updatů. Dalšími sledovanými parametry bylo množství zabrané paměti RAM a rychlost antivirové kontroly. Pro méně zkušené uživatele je také důležité přehledné ovládání a srozumitelné zprostředkování informací. Vzhledem k podobným cenám nenabízíme cenový tip.