Vitamin C

Více odolnosti pro váš počítač

Proti stále rostoucím internetovým hrozbám vám pomůže jen **DOKONALÁ KOMPLEXNÍ OCHRANA.** Chip vám představí balíček, který zabezpečí váš počítač a zároveň se nestane brzdou provozu…

FABIAN VON KEUDELL

Jen odolné tělo má šanci „přežít" podzimní období viróz, chřipek a dalších infekcí. Budovat dobrý obranný systém je ale dobré už nyní – v horkých letních dnech.

Podobné je to i v oblasti počítačové bezpečnosti. Ačkoliv už nyní na nás denně útočí desítky malwaru nebo internetových červů, odborníci očekávají, že ten skutečně silný nápor škůdců teprve přijde. Abyste na něj byli s počítačem připraveni, je potřeba začít budovat obranu již nyní. Výhodou nástrojů, které vám nabízíme, je také možnost individuálně zvýšit výkon počítače. Podívejte se na tipy nabízené na stránce 48.

Penicilin pro Windows: ochrana proti virům

Když prší, vezmete si bundu a sáhnete po deštníku. Ale uživatelé Windows XP v podobné situaci, obrazně řečeno, chodí v tričku s krátkým rukávem. Z hlediska ochrany proti virům jsou uživatelé opravdu téměř bez ochrany, což je činí lákavým cílem pro většinu škůdců. Jako třešnička na dortu působí to, že většina uživatelů navíc pracuje s právy administrátora. Jestliže tedy uživatel například otevře v Outlook Expressu zavirovaný e-mail, může si vir dělat vše, co se mu zlíbí – s právy administrátora je to totiž až příliš snadné. Prvním krokem ochrany uživatelů XP je tedy používání účtů s omezenými právy. Uživatelé Windows Vista jsou již chráněni deštníkem UAC (kontroly uživatelských účtů), která tento problém řeší „po svém". Uživatel (i pokud se přihlásí jako administrátor) má pouze omezená práva a každou změnu systémových nastavení musí individuálně potvrdit. Tím je zaručena relativní bezpečnost i při napadení virem či při objevení systémové zranitelnosti. My vám nabízíme další tipy, jak zvýšit bezpečnost svého počítače.

UPDATE APLIKACÍ Ano, mít nejnovější verzi Windows se všemi záplatami je dnes už považováno za samozřejmost, nicméně obvykle to nestačí. Ptáte se, kde je zádrhel? Útočníci stále častěji využívají programátorské chyby v nejpoužívanějších programech „třetích stran". V minulém roce bylo v nejoblíbenějších programech objeveno přes 150 kritických „děr", ve většině případů snadno zneužitelných. Jestliže nepoužíváte nejnovější verze programů typu Adobe Reader nebo Skype, je váš počítač potenciálně velmi zranitelný.

Pokud si teď říkáte, že není v lidských silách neustále kontrolovat aktuálnost všech důležitých programů na počítači, máme pro vás jednoduchý tip. Doporučujeme instalaci programu SUMo **(www.kcsoftwares.com)**, který dokáže kontrolovat, zda programy nainstalované na vašem PC již nejsou k dispo-

NAJDETE NA CHIP DVD

Ochrana Windows

AntiVir Personal ► obrana proti virům

SpyBot – Search & Destroy ► čistí systém od spywaru

Spamihilator ► filtruje nevyžádanou poštu

Process Monitor ► kontroluje procesy ve Windows

Mozilla Firefox 3 ► alternativa Internet Exploreru

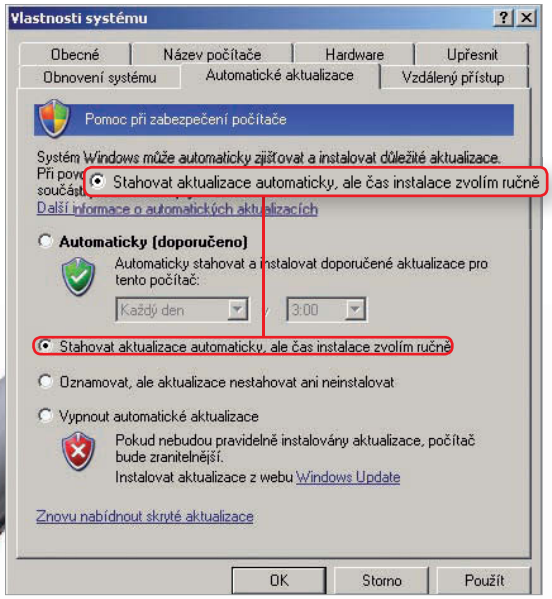
Mozilla Thunderbird ► špičkový poštovní klient poskytovaný zdarma

NoScript-Plug-in ► rozšíření chránící Firefox před nebezpečnými skripty

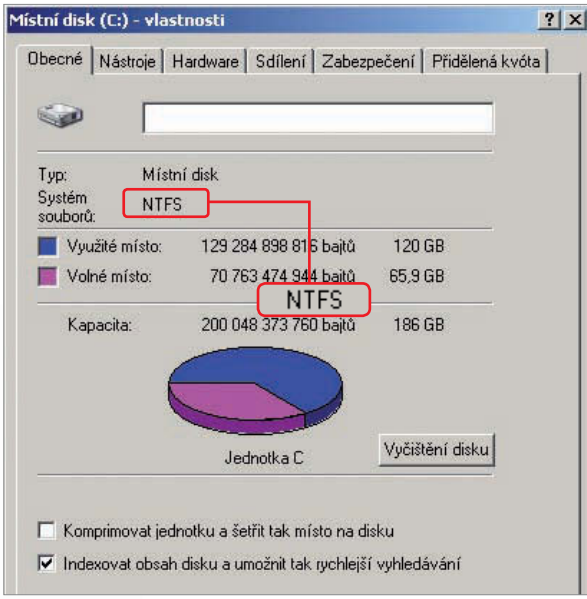
Spyware Terminator ► nástroj k boji proti spywaru

IE7 Pro ► rozšiřuje Internet Explorer o mnoho praktických funkcí

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **OCHRANA**.



Bezpečnější systém: Nechte systém automaticky stáhnout záplaty, ale o době instalace raději rozhodujte sami.



Lepší: Disk naformátovaný v souborovém systému NTFS může být lépe chráněn před útoky.

zici v novější verzi. Tento program vám doporučujeme jako vítěze srovnávacího testu „Update tools“, který najdete v tomto Chipu na straně 74. Pokud nástroj některý program nedokáže detekovat, lze ho přidat kliknutím na »Add«. Podobným způsobem lze řešit bezpečnost „beta verzí“. V nabídce »Options | Settings« aktivujte zatržítko u volby »Allow beta versions« a nakonec vše potvrďte kliknutím na »OK«.

Pokud potřebujete podrobnější informace o používání programu, podívejte se na náš web www.chip.cz, kde najdete praktický návod na použití programu SUMo.

INSTALACE ZÁPLAT VE WINDOWS O nutnosti instalace záplat ve Windows je zbytečné se příliš rozepisovat. Zkušenějším uživatelům lze v okně automatických aktualizací (nejrychleji se tam dostanete pomocí klávesové zkratky [Windows]+[Pause] a kliknutím na »Automatické aktualizace«) doporučit volbu „Stahovat aktualizace automaticky, ale čas instalace zvolím ručně“. Tím lze totiž vyřešit občasnou nutnost restartu po nainstalování kritické záplaty, která se objeví obvykle tehdy, když potřebujete na počítači pracovat. Klikání na tlačítko »Restartovat později...« je totiž poměrně otravná činnost. Ve Vistě je to vyřešeno lépe, a tak volba „Automaticky (doporučeno)“ není problém.

INSTALACE VIROVÉHO SKENERU Dobrý antivirový program je ekvivalentem bílých krvinek v lidském těle. My vám zdarma nabízíme komplexní řešení v podobě AVG Security Chip Edition 8.0. Pokud z jakéhokoliv důvodu nechcete či nemůžete toto řešení použít, nainstalujte

si alespoň samotný antivirový program. Jedním z nejlepších kandidátů v kategorii bezplatných antivirových programů je AntiVir Classic Personal Edition. A protože tato bezplatná verze nedokáže detekovat spyware, doporučujeme ji doplnit o nástroj SpyBot – Search & Destroy.

OPTIMALIZACE SOUBOROVÉHO SYSTÉMU

Základní krok pro vylepšení imunity však hledejte jinde. Je jím použití souborového systému NTFS, který zlepšuje bezpečnost především v oblasti uživatelských kont. Nevíte, ve kterém systému souborů je formátován váš disk? Klikněte v okně „Tento počítač“ pravým tlačítkem na vybraný disk a v nabídce zvolte položku »Vlastnosti«. Hledanou informaci najdete u položky Systém souborů. Pokud jste ale udělali chybu a nainstalovali si XP na disk nainstalovaný ve formátu FAT32, nevěšte hlavu. Poměrně snadno lze tento systém změnit.

Nejprve zálohujte důležitá data – převod sice bývá bezproblémový, ale „jistota je jistota“. Po vytvoření zálohy otevřete nabídku »Start | Programy | Příslušenství« a zvolte položku »Příkazový řádek«. Poté do příkazového řádku zadejte:

```
convert c: /fs:ntfs
```

Pozor: Převod může trvat i několik desítek minut, v závislosti na velikosti disku. Dalším krokem pro uživatele Windows XP (pro ty se souborovým systémem NTFS) je skok do nabídky »Start | Ovládací panely | Uživatelské účty«. Zde nastavte nového administrátora a ihned po jeho vytvoření vytvořte svůj nový účet s „omezeným oprávněním“. Poté můžete pracovat nebo surfovat mnohem bezpečněji.

Tip pro zkušené: vypněte softwarový firewall

Některé softwarové firewally jsou spíše brzdou provozu než ochranou počítače. Pokud máte firewall i ve svém routeru, lze jen doporučit poslat jeho softwarového bratra na smetiště...

Naše rada zní – pokud máte doma moderní router s integrovaným firewallem SPI (Stateful Packet Inspection), lze vypnutím softwarového firewallu ušetřit systémové zdroje a čas (o který vás okrádají jeho zvídavé dotazy). Firewally SPI pracují na jiném principu než jejich příbuzní (které jsme vám představili v minulém Chipu). Firewally SPI totiž nespojují data s aplikacemi, ale kontrolují každý datový paket. Například pokud se z domácího počítače připojíte k webové stránce (přes HTTP), stránka s vámi může (díky SPI firewallu) komunikovat opět pouze pomocí HTTP paketů.

Ukážeme vám, jak aktivovat a nastavit firewall v routeru Netgear WNR854T. Princip je ale stejný i v případě routerů jiných výrobců.

Jak postupovat: Adresu routeru otevřete v prohlížeči – obvykle je „192.168.1.1“ – a zadejte své přihlašovací údaje. V záložce »WAN konfigurace» nejprve zrušte zatržítko »Deactivate SPI firewall» a nastavení potvrďte kliknutím na »Accept«.

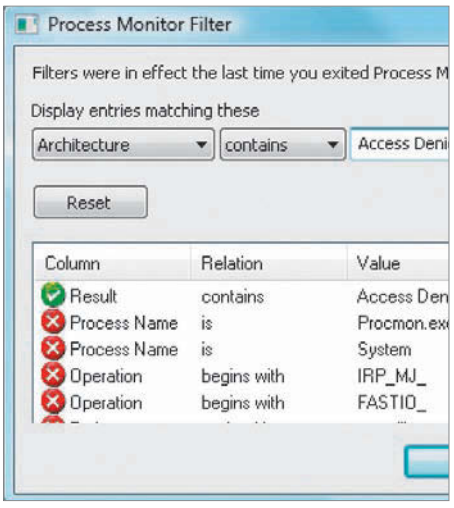
Riziko: Pokud používáte programy pro sítě P2P (jako je například síť BitTorrent nebo eMule), může firewall SPI dělat problémy. Pokud ale chcete programy tohoto typu používat pouze na jediném počítači, nemusíte se ochrany firewallu SPI vzdávat v celé domácí síti. Jediné, co potřebujete, je IP adresa počítače

Problém: Mnoho programů přistupuje ke zdrojům, které jsou dostupné pouze pro systém či pro administrátora (ačkoliv je tento postup v přímém rozporu s programátorským doporučením Microsoftu). S velkými problémy se budete často potýkat při konfiguraci některých programů a při instalaci.

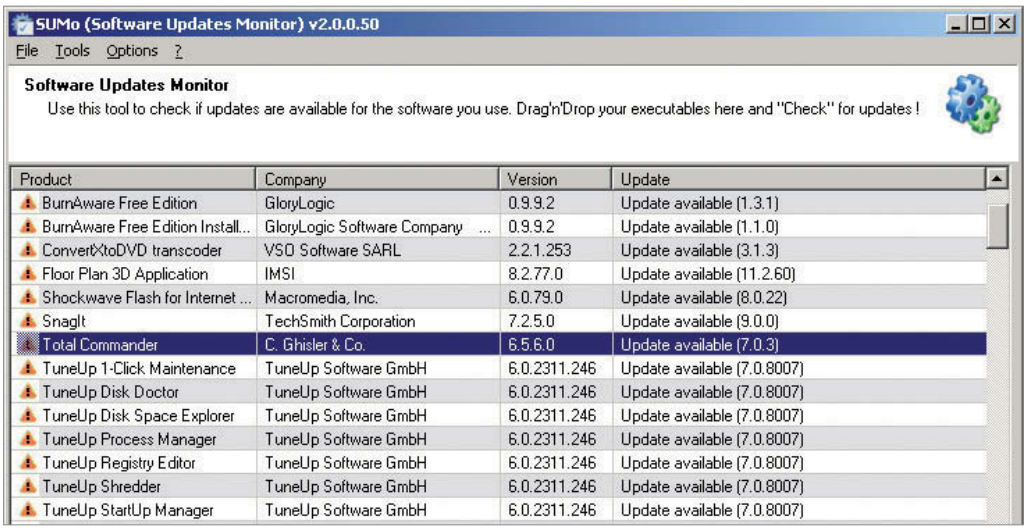
Řešení: Uživatel s omezeným oprávněním by měl spouštět instalaci pomocí nabídky „Spustit jako...“, která se objeví po kliknutí pravým tlačítkem na soubor. Poté už jen stačí zvolit administrátorské konto, zadat heslo, a instalace může začít. Pokud není program po nainstalování dostupný, přepněte na své administrátorské konto a zpřístupněte ho pro všechny uživatele. Pokud nepomůže ani to, máte dvě varianty řešení.

První z nich je poněkud nepraktická – vždy když budete chtít s problematickým programem pracovat, přepněte se přes nabídku »Start | Odhlásit« na své administrátorské konto.

Druhá možnost je určena profesionálům. Pomocí programu Sysinternals Process Monitor, (který najdete na našem DVD, nebo přímo na adrese **http://tech-**



Chybějící práva: Program Process Monitor ukáže, které nástroje mají ve Windows XP (a v systému NTFS) problémy s přístupovými právy.

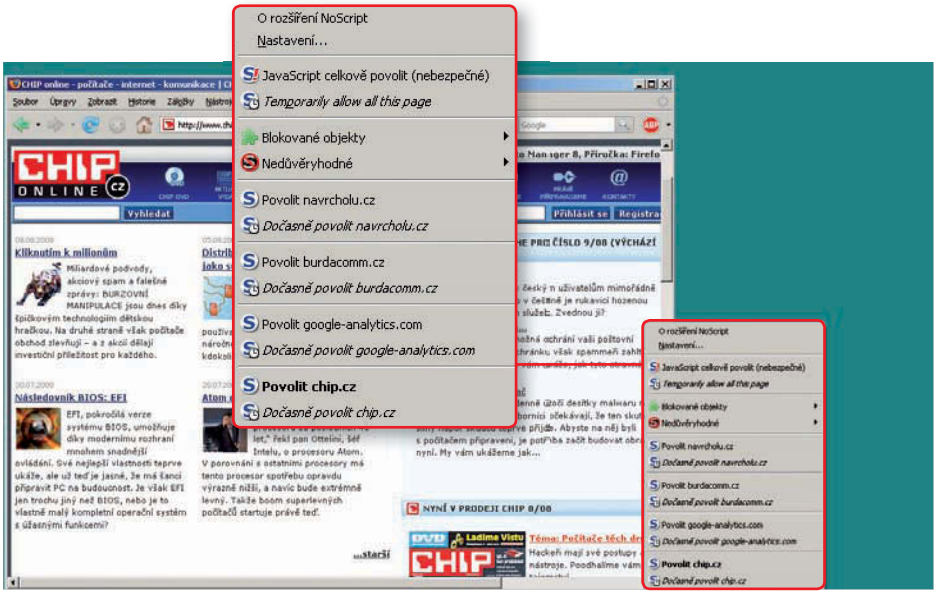


Vždy aktuální: Nástroje na kontrolu „updatů“, jako například SUMo, dokáží detekovat programy nainstalované na PC a automaticky zjistit, zda je k dispozici novější verze.

(který má zůstat nechráněn). Tu zjistíte například tak, že v ovládacích panelech kliknete na sekci »Síťová připojení« – IP adresu najdete vlevo dole v sekci „Podrobnosti“. Opět v konfiguraci routeru klikněte na záložku „WAN configuration“, aktivujte položku „Default DMZ server“ a do okna vpravo zadejte IP adresu počítače, který nemá být firewallem SPI chráněn.

Tip pro zkušenější: Pokud máte na svém počítači například FTP server, nepoužívejte obvyklé implicitní porty (jako například port 21 pro FTP). Místo toho mu přiřaďte méně obvyklý, nepoužívaný port (například 5677).

Důvod: Útočníci se vždy snaží připojit k počítači přes nejpoužívanější porty. Poté, co v routeru v nabídce „Forvard port“ propojíte externí port 5677 s interním portem 21, bude FTP server fungovat bez problémů dále.



Bezpečný browser: Když už nechcete používat Operu, alespoň doplňte Firefox o rozšíření NoScript. To dokáže znesnadnit práci většině útočníků.

net.microsoft.com/cs-cz/sysinternals/bb896645(en-us).aspx) lze zjistit, kde má program problémy. Nezapomeňte, že program musíte spustit jako administrátor. Když se objeví potíže s programem (nefungujícím s omezenými právy), přepněte do Process Monitoru a pomocí klávesové zkratky [CTRL+E] zastavte sběr dat. Poté klávesovou zkratkou [CTRL+L] otevřete „filtrovací dialog“ (Process Monitor Filter). Objeví se dialogové okno a v něm nastavte položky filtru na „Result, contains, Access Denied“. Vše potvrďte kliknutím na »Add« a na »OK«. Poté program ukáže pouze zamítnuté přístupy. Klikněte pravým tlačítkem na kteroukoliv zobrazenou položku a zvolte příkaz »Jump to«. Ten vás přesune přímo do registru a v něm zjistíte, na kterém místě se „problém“ objevil. Jestliže jde o složku, klikněte na ni pravým tlačítkem a zvolte »Vlastnosti | Zabezpečení«. Zde v sekci „Název skupiny nebo jméno uživatele“ vyberte své jméno a v sekci „Oprávnění pro“ nastavte požadovaná zatržítka (Číst, Zapisovat...). Chybějící práva vidíte v Process Monitoru v sekci Operations. Oprava problémů v registrech je analogická opravě problémů v souborech a ve složkách.

Vitamin C zlepší obranu vašeho počítače

Browser: Tyto nástroje udrží počítač zdravý i při surfování

Jedy internetové mafie mohou být fatální – je tedy více než rozumné se od nich držet dále. I když se konkurence snaží ze všech sil, stále je a určitě ještě chvíli bude nejrozšířenějším prohlížečem Internet Explorer. Nikoho tedy určitě nepřekvapí, že většina útoků směřuje právě na něj a na jeho plug-iny.

POZADÍ Nejprve je oběť nalákána na určitou, na první pohled neškodnou stránku (například pomocí odkazu v e-mailu nebo ve zprávě IM). Druhým krokem je detekovat konfiguraci počítače oběti a především odhalit typ prohlížeče. Poté je spuštěn útok, odpovídající zjištěnému prohlížeči nebo jeho doplňkům. Další krok je ve všech případech stejný – na počítač oběti je nainstalován tzv. downloader, který posléze do PC nahrává požadovaný malware. Downloader je průběžně modifikován, a proto je pro většinu antivirových programů tvrdým oříškem. Navíc jakmile se downloader dostane do počítače, bývá jeho dalším krokem okamžité vypnutí všech bezpečnostních produktů. Poté už malwaru nic nebrání ve „studiu“ citlivých dat, osobních údajů nebo v hlídání vaší činnosti...

ŘEŠENÍ Jak už jsme se několikrát zmiňovali, nejjednodušším řešením je přechod na alternativní program. Pokud i nadále z různých důvodů musíte používat Internet Explorer, používejte ho pouze pro návštěvy osvědčených webů. Na riziková místa internetu surfujte pomocí jeho konkurentů. Ideálním řešením je nová Opera (9.5x), kterou většina mafiánských nástrojů prozatím ignoruje. Pokud je ale pro vás konfigurace příliš obtížná nebo pokud máte specifické požadavky, vyzkoušejte Firefox. Je ale důležité si uvědomit, že se stále rostoucím podílem Firefoxu vzrůstá zájem útočníků i o tento původně zcela bezpečný prohlížeč. Je více než rozumné doplnit schopnosti browseru pomocí různých rozšíření a odstranit tak potenciální slabiny. Ideálním řešením tohoto problému je rozšíření NoScript, které na stránce implicitně zablokuje všechna potenciální rizika (JavaScript, Javu nebo Flash). Pokud stránce důvěřujete, lze tyto prvky jednorázově povolit, případně stránku přidat mezi důvěryhodné. Při surfování v rizikových vodách pak stačí dodržovat jediné pravidlo – pokud vás stránka nutí k zapnutí některého z prvků, dejte jí sbohem...

Pokud navíc budete surfovat „s hlavou otevřenou“ (nebudete spouštět neznámé soubory, stahovat podezřelé doplňky a prohlížet rizikové dokumenty), nemusíte se spárů internetových mafií vůbec obávat...

AUTOR@CHIP.CZ