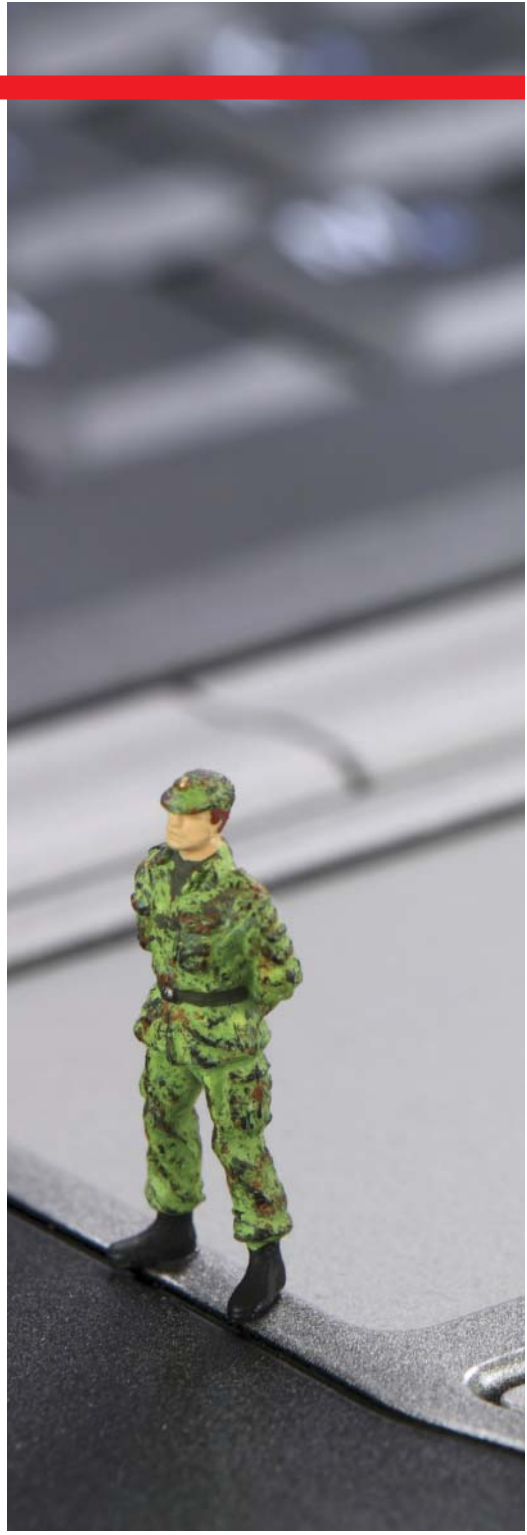
Bezpečná Windows



Hackeři a tvůrci virů mají svůj oblíbený cíl: Windows. Je tedy nejvyšší čas najít ta správná obranná opatření. Chip vám ukáže, jak můžete svůj počítač před útoky ochránit. *Valentin Pletzer*

V tomto článku najdete

Samotná Windows nejsou zrovna „superbezpečný" systém. Tím více je tedy nutné, aby se každý uživatel sám postaral o dodatečné zabezpečení. Jinak totiž převzetí kontroly nad vaším PC přes internet nezabere hackerovi ani pět minut. Chip vám ukáže, jak můžete Windows zabezpečit tak, že budou stejně nedobytná jako pevnost Fort Knox.

INTERNET

Vnější ochrana

Dostat se do Windows je pro zkušeného hackera snadné. Naplánovat rozsáhlou invazi do PC je dětskou hračkou, protože naprostá většina počítačů používá stejnou kombinaci programů pro surfování a zabezpečení. Doporučujeme vám tedy změnit „styl". První a nejjednodušší radou je nahrazení Internet Exploreru bezpečnější variantou: Firefoxem nebo Operou. Důvod je jasný: open-source prohlížeče jsou nejen méně zranitelné, ale v současnosti také hackery a tvůrci zranitelností (především Opera) víceméně ignorovány. Navíc jsou k dispozici některé užitečné plug-iny (Firefox), které razantně zdokonalují ochranu. Představíme vám je v následujících tipech.

Vyhněte se stránkám hackerů

Nejnovější verze Firefoxu obsahují phishingový filtr, který vás varuje, pokud vstoupíte na nebezpečné stránky. Filtr najdete v tomto prohlížeči v nabídce *Tools* | *Options* v záložce *Security*. Nicméně i tak doporučujeme použít alternativu. Přestože integrovaná phishingová ochrana není špatná, můžete ji doplnit nabídkou od McAfee, která je zdarma. Plug-in SiteAdvisor nejen rozeznává nebezpečné stránky, ale také velice detailně informuje o důvodech, proč je daná stránka zablokovaná. Plug-in lze získat na adrese **www.siteadvisor.com/download/ff.html**. Zde klikněte na *Download SiteAdvisor for Firefox now*. Na další stránce odsouhlaste „Terms and conditions" a klikněte na tlačítko *Install SiteAdvisor for Firefox now*. Firefox obvykle zablokuje instalaci plug-inů, takže musíte nejprve ve žluté liště Firefoxu kliknout na *Allow* a pak teprve na *Install now*, abyste nástroj mohli nainstalovat. Nakonec restartujte Firefox, aby mohl být plug-in aktivován. SiteAdvisor od McAfee se sám integruje do spodního pravého rohu Firefoxu. Pokud je webová stránka bezpečná, ikonka se zbarví zeleně. Naopak v případě nebezpečné stránky se tato stránka ihned zablokuje a znázorní se červená ikona. Pokud vás zajímá, proč byla stránka zablokována, musíte kliknout na ikonu a otevřou se detaily o stránce. Zde také najdete komentáře ostatních uživatelů.

Vypněte nebezpečné scripty

Plug-in NoScript patří mezi nejdůležitější ochranná rozšíření v pro-

Bezpečnostní nástroje na DVD

Firefox
bezpečnější alternativa Internet Exploreru

McAfee SiteAdvisor
plug-in pro Firefox

NoScript
rozšíření pro Firefox blokující nejen JavaScripty

HijackThis
nástroj pro analýzu systému

Sophos Anti-Rootkit
Detektor rootkitů ve vašem systému

Sandboxie
Download: **www.sandboxie.com**

hlížeči. Přestože máte nejlepší phishingové filtry, může se stát, že během surfování přistanete na nebezpečné stránce. „NoScript“ ochrání prohlížeč tak, že zablokuje scripty na stránkách hackera a zabrání tak dalšímu ohrožení z této strany. Toto bezpečnostní rozšíření lze snadno také získat v archivu plug-inů na Mozilla Foundation, který je dostupný přímo přes Firefox. Otevřete *Tools* | *Add-Ons* a v následujícím okně klikněte na *Get Extensions*. Poté se v okně prohlížeče otevře archiv plug-inů. Plug-in najdete tak, že do vyhledávacího boxu vložíte pojem „NoScript“. Nalezený nástroj si stáhnete a nainstalujete kliknutím na zelené tlačítko *Install now*. Stejně jako v případě „SiteAdvisor“ pak musíte restartovat Firefox, aby se ikona plug-inu znázornila vpravo dole. Jakmile je rozšíření nainstalováno, zablokuje téměř všechny scripty, které běží automaticky. Jeho používání má ale i drobné nevýhody. Pokud webová stránka není správně zobrazena, může to být i kvůli tomuto plug-inu. V tomto případě klikněte na ikonu „S“ a povolte požadovaný script. Například při návštěvě Googlu můžete bez problémů použít volbu „Allow google.cz“, aniž byste museli spustit „zlomyslný skript“. Po tomto „povolení“ bude již stránka považována za důvěryhodnou.

Základní ochrana se standardními nástroji Windows

Chcete si svůj počítač zabezpečit i bez dodatečných externích nástrojů? Bez problémů! Pomocí správného nastavení mohou být snadno odraženi alespoň méně zkušení hackeři.

- Update Windows by měl být základem každého systému. Bez něho se Windows stává cedníkem. V každém případě byste tedy měli aktivovat doporučenou volbu „Automaticky“ v nabídce „Automatické aktualizace“ v kontrolním panelu.

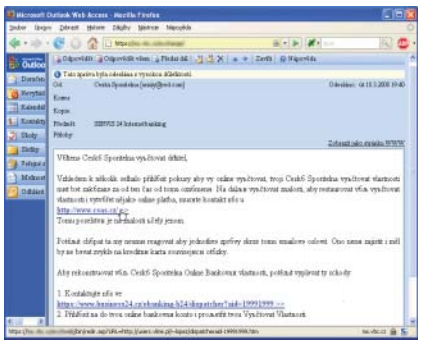
- Stejně důležité jsou updaty aplikací, protože čím dál tím více hackerů využívá děr v softwaru. V každém případě tedy doporučujeme aktivovat automatické aktualizace programů. Pokud to není možné, musíte si aktualizace vyhledat sami. Na nejnebezpečnější díry (a jejich záplaty) vás upozorňujeme v naší pravidelné rubrice Bezpečnost.

- Windows firewall v XP a Vistě nabízí pouze omezenou ochranu před útoky. Pokud nemáte k dispozici lepší alternativu, doporučujeme nainstalovat aspoň tyto bezpečnostní „zámky“, protože pomohou odfiltrovat alespoň část „automatických“ útoků.

- Také byste měli dodržovat některá pravidla.

Nikdy neotvírejte přílohy od neznámého zasilatele, protože PDF přílohy nebo obrázky mohou být využity k útokům. Nenavštěvujte žádné rizikové stránky (případně s maximální rozvahou a alternativním browserem). Porno a pirátské stránky jsou preferovanými distributory pro viry a trojské koně.

A v neposlední řadě: důvěřujte svým bezpečnostním nástrojům, a ne pop-up oknům tvrdícím, že na vašem počítači nalezla virus...



PROTI PHISHINGU: Nejlepší zbraní proti phishingu je opatrnost. Zde odkaz v mailu míří do domény pl...

Zablokujte inboxové útoky

Abyste Windows ulehčili práci s celkovou obranou systému, měli byste co nejdříve osvobodit svůj inbox od všech škůdců. Doporučujeme vám nainstalovat si spamový filtr současně na dvou místech. První a nejlepší možností, jak se zbavit nechtěného spamu a phishingových zpráv, je instalace filtru na mailovém serveru. Mnoho freemailů nabízí automatickou ochranu před spamem, u některých však musí být aktivována. Ochrana proti spamu na mailovém serveru má opravdu smysl, protože její filtr má přístup nejen k datům z vašeho inboxu, ale také ke všem ostatním kontům. A to určitě zvýší úspěšnost zásahů antispamového filtru. To ale neznamená, že byste se měli vzdát druhé možnosti, jak odfiltrovat spam na svém počítači. I přes zmiňovanou úspěšnost totiž mailový server stále nevyfiltruje všechny nevyžádané e-maily, a musíte je tedy odstranit až na svém počítači. My doporučujeme „filtr" jménem Spamihilator. Pozitivem tohoto filtru je především jeho transparentní mod.

Ačkoliv tento program nefunguje jako plug-in, ale jako „proxy" v mailových klientech, lze jeho nasazení doporučit i proto, že škála spolupracujících klientů je opravdu široká. Jediným nedostatkem je, že spojení s mailboxy přes IMAP nefunguje na 100 procent. Autor Spamihilatoru už ale na odstranění této chyby pracuje. A co činí Spamihilator tak dobrým?

Nespoléhá se pouze na jeden filtr; maily prožene řetězcem testovacích „stanic", které mohou být rozšiřovány a upravovány. Ale nebojte se – s konfigurací si nemusíte hrát dlouhé hodiny. Nejefektivnější filtr je na vašem počítači nainstalován ihned a je okamžitě akceschopný. Tímto filtrem je DCC, což je zkratka pro Distributed Checksum Clearinghouse. Tento filtr funguje dobře především proto, že je založen na principu „komunitní spolupráce". Každé PC, které si tento plug-in aktivovalo, zasílá kontrolní součet (checksum) každého e-mailu na jeden z DCC serverů. Server jednoduše vypočítá hodnotu součtu. Pokud údaj překročí kritický bod, DCC klasifikuje mail jako spam. Pokud DCC nesplní svůj účel, do akce jdou ostatní – například bayesovský filtr, který prozkoumá mail na obsah určitých termínů (sex, viagra atd.) a zároveň se dokáže učit na základě toho, co vy označíte jako spam. A pokud selže i tento nástroj, stačí se podívat na **www.spamihilator.com/plugins**, kde najdete další užitečné plug-iny a addony, například Empty Mail, který automaticky vymaže e-maily bez obsahu. Plug-in, který určitě nesmí scházet ve vaší sbírce, se jmenuje „Attachment Extensions Filter". Tento užitečný nástroj pomáhá již „při příchodu" filtrovat maily s určitými nebezpečnými přílohami.

To se často hodí, protože celá řada příloh je jednoznačným nosičem škůdce. Do této kategorie lze zařadit například přílohy se souborem ve formátu PIF. Ačkoliv se tento souborový formát dnes již skoro nepoužívá, může obsahovat příkazy, které otevírají dveře virům a trojanům. A to je přesně to, na co zasilatelé phishingových mailů a spamu čekají.

Do této kategorie radíme zařadit i soubory typu EXE, COM a BAT.

Doporučujeme vám dodržovat přísnou bezpečnostní politiku a obecně vůbec neakceptovat mnoho typů příloh. Chcete vědět, jak nastavit Spamihilator ještě lépe a jak najít konfiguraci filtru, která bude pro vás optimální? Přečtěte si o tom v podrobném článku Konec spamu v čísle 12/2007. Najdete ho ve formátu PDF na našem DVD nebo si ho také můžete přečíst na našem webu. →

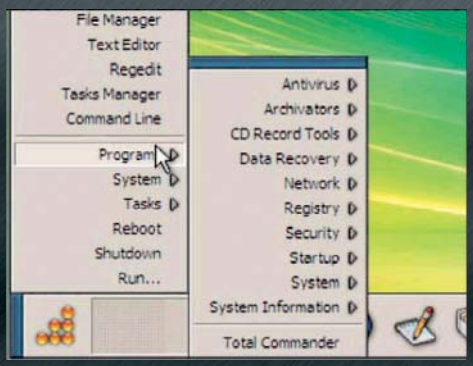
NEUKONČUJTE: Podezřelé procesy nejprve zablokujte pomocí volby „Block Incoming Connections".

Záložní bezpečnostní plán

Neexistuje nic, o čem by se dalo říct, že představuje úplnou bezpečnost. Proto dobří stratégové mají vždy připraven záložní plán pro případ, že by jejich vlastní řady byly již rozmetány. Ve třech krocích vám ukážeme, jak můžete získat kontrolu nad svým počítačem.

1. Nepanikařte

Pokud vám do systému vstoupil vetřelec, zachovejte chladnou hlavu. Neinstalujte žádný nový software ani nerestartujte.



BEZPEČÍ: Na Chip recovery CD najdete všechny důležité nástroje...

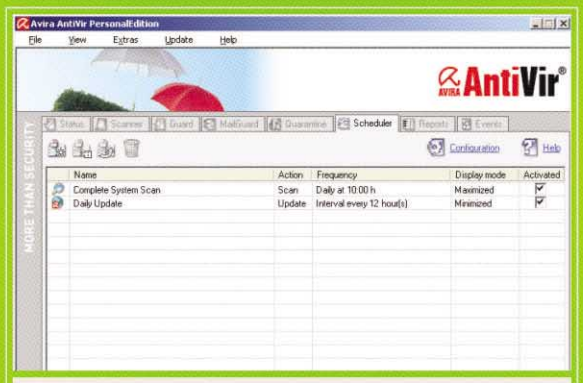
Místo toho proveďte aktualizaci svého virového skeneru. Pokud už nefunguje, nabootujte z „recovery CD". Obvykle můžete použít instalační CD svého virového skeneru. Pokud ne, pak instrukce k užitečnému recovery CD najdete v Chipu 10/07.

2. Izolujte Windows

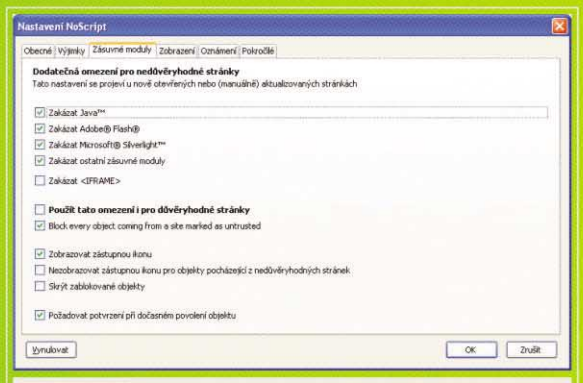
Po updatu signatury ihned přerušte síťové spojení. Přes internet se může „aktualizovat" i vetřelec a uniknout virovým skenerům.

3. Zkontrolujte podezřelé soubory

To, že váš virový skener již nemůže najít další vetřelce, ještě neznamená, že váš systém je zcela bez malwaru. Dejte si trochu času a zkontrolujte neznámé soubory a složky. Mějte po ruce aplikace umožňující bezproblémové ukončení podezřelých procesů (např. již v Chipu zmiňovaný Killbox). Podezřelé soubory až do velikosti 5 MB můžete nechat zkontrolovat 20 virovými skenery na webových stránkách **www.virustotal.com**.



AVIRA: Antivir od firmy Avira lze doporučit jako bezplatnou alternativu komerčních antivirů.



BLOKÁDA: Rozšíření NoScript umí zablokovat i Javu, Flash nebo Silverlight.

LOKÁLNÍ OCHRANA

Vnitřní bezpečnost

Ve Windows je integrován pouze primitivní antispywarový nástroj, který vám sám o sobě nepomůže ochránit systém před nechtěnými návštěvami vykradačů dat. Měli byste si tedy na své PC nainstalovat také antivirový program. Naše doporučení je pochopitelné: použijte nejnovější bezpečnostní balíček AVG Security Chip Edition 8.0, který najdete na našem DVD. Ten mimo jiné obsahuje i antivirus, firewall a kvalitní antispywarový nástroj, což by mělo vytvořit dobrý základ pro komplexní ochranu počítače.

Jakmile jednou tuto bezpečnostní sadu nainstalujete, můžete se zříci Windows Firewallu a případně také Windows Defenderu. Pokud preferujete individuální ochranu pro každou oblast zabezpečení, doporučujeme jako freewarovou alternativu virový skener Avira Antivir (**www.free-av.com**), případně skener od firmy Kaspersky (trial verze na **www.kaspersky.com**), který vyhrál nejnovější srovnávací test antivirových nástrojů. Ať už ale vyberete jakýkoliv program, virový skener by měl vždy aktivně běžet na pozadí. Pouze tak bude tento bezpečnostní nástroj schopen zablokovat útok malwaru co nejdříve.

KOMPROMIS: Pokud chcete mít automatické aktualizace pod kontrolou (a zároveň je nechcete vypínat), je toto optimální řešení...

Objevte špionážní nástroje

Dříve než se opravdu dají do „práce“, hackeři nejprve své cíle zkoumají. Ve světě Windows tuto práci zastávají spywarové nástroje. Proti tomu vám pomůže podceňovaný Windows Defender. Ačkoliv z hlediska detekce se komerčním virovým skenerům nevyrovná, obsahuje užitečné funkce, které zvyšují jeho „užitečnost“. Pokud ho již ve svém počítači nemáte, můžete si ho táhnout ze stránek Microsoftu (**www.microsoft.com/downloads**). Po nainstalování program automaticky monitoruje bezpečnost vašeho systému. Protože ale žádná ochrana není perfektní, měli byste znát skrytý, ale velice šikovný nástroj. Ten se v Defenderu ukrývá pod nabídkou *Tools* | *Software Explorer* a pomůže vám se sledováním počítače a vystopováním spywaru.

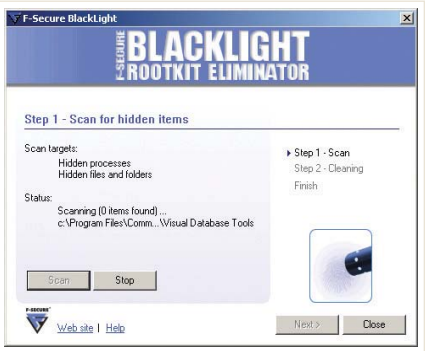
Nejdůležitějším seznamem jsou zde „automaticky spouštěné programy“ (Startup programs). Zde vám nástroj ukáže veškerý software, který se automaticky aktivuje, jakmile se spustí Windows. Stačí jen kliknout na jméno souboru a získáte podrobnou informaci, jako je umístění na harddisku, nebo dokonce i den instalace. Bude-li se vám soubor zdát podezřelý, můžete ho neškodně potlačit pomocí tlačítka „Disable“. Pokud se jedná o jasný spyware, zbavíte se ho pomocí „Remove“.

Vylepšená verze task manageru (Správce úloh) se v Software Exploreru skrývá pod položkou „Currently running programs“, mnohem zajímavější je však volba „Network connected programs“. Zde nástroj uvede nejenom seznam všech otevřených portů, ale také jména programů, které za ně „zodpovídají“.

Doporučujeme tedy neukončovat podezřelé procesy naráz; místo toho použijte tlačítko „Block Incoming Connections“, abyste zablokovali port a aplikaci pomocí firewallu.

Alternativou tohoto nástroje je námi již několikrát zmiňovaný HijackThis. Nástroj, který je poskytován zdarma a který „spravuje“ a vyvíjí firma Trend Micro, se vyvinul do pseudostandardu ve spoustě webových bezpečnostních fór. Tak jako Windows Defender i tento pro-

AKTUÁLNÍ: U antirootkitu doporučujeme vždy používat nejnovější verzi...



PROTI ROOTKITŮM: **Jedním z doporučeníhodných nástrojů může být i BlackLight od F-Secure.**

gram monitoruje všechny lokace pro umístění automaticky spouštěných programů. Navíc dokáže tento seznam jedním kliknutím exportovat do textového souboru. Tato data pak stačí uveřejnit na některém z mnoha fór, např. na **www.viry.cz**, kde vám zkušenější uživatele pomohou s jejich „dešifrováním" a odhalením škůdců.

Získejte zpět ukryté soubory

Čas od času zkontrolujte své PC, zda neobsahuje skryté škůdce, např. rootkity. Navzdory všem preventivním opatřením můžete mít v systému nějaký neidentifikovaný rootkit, a to proto, že je neviditelný pro Windows Explorer, Registry Editor, dokonce i pro virový skener. Nástroje typu FSecure Blacklight či Sophos Anti-Rootkit vám s tímto problémem pomohou. Tyto programy používají následující trik. Disk skenují dvěma různými způsoby.

Windows (API) interfaces se využívají v prvním kole, a to pro nahrání adresářové struktury a obsahu registrů. Ve druhém kole pak nástroje použijí svůj vlastní API, který s určitostí nebyl kompromitován rootkitem. Jestliže se mezi těmito dvěma záznamy objeví odlišnosti, pak je téměř jisté, že se rootkit snaží skrýt soubory.

Tak jako většina běžných antivirů vám i Blacklight umožní soubory buď smazat, nebo je dát do karantény. My navrhujeme karanténu. Pokud se poději soubory ukážou jako neškodné, mohou být experty vyhledány a opět obnoveny.

Tip pro profesionály: Většina základních antirootkitů neukáže žádné technické informace. Jestliže chcete více, sáhněte po Gmeru (**www.gmer.net**). Mimo jiné zobrazuje odkloněné systémové funkce, aktivní procesy a nainstalované drivery…

Valentin Pletzer

Profesionální tip: Zabezpečte Windows pomocí Sandboxie

Pomocí všech až dosud popsaných tipů a nástrojů dosáhnete vysokého stupně zabezpečení. Jde to ale ještě lépe. S nástrojem Sandboxie, který je k dispozici zdarma, lze zabezpečit každou aplikaci ještě více a dosáhnout tak poslední náročné bezpečnostní úrovně – podobné zredukovaným právům Internet Exploreru 7 pod Vistou.

Přínos Sandboxie

Čtení a zápis dat patří k rutinním činnostem každého počítačového programu. Avšak pokud má webový prohlížeč právo zapisovat cokoliv v kritických oblastech (jako například složka Windows), pak je něco určitě špatně. XP se dokonce ani nepokusí těmto akcím zabránit – a přesně to je místo, kde se do hry dostává Sandboxie.

Jakmile je jednou tento bezpečnostní nástroj aktivován, můžete určit programy, které by neměly mít přímý přístup k disku, ale pouze k virtuálnímu disku vytvořenému pomocí nástroje Sandboxie. V tomto chráněném prostředí jsou tedy všechny změny do systémových kritických oblastí po uzavření aplikace „zamítnuty"; takto zůstává váš počítač nepoškozený a čistý.

Spuštění Sandboxie

Po instalaci (z **www.sandboxie.com**) se nástroj Sandboxie automaticky spustí po každém startu Windows a může být okamžitě aktivován dvojitým kliknutím na ikonku v panelu snadného spuštění. Nejprve ale spusťte přes nabídku Start „Sandboxie Control".

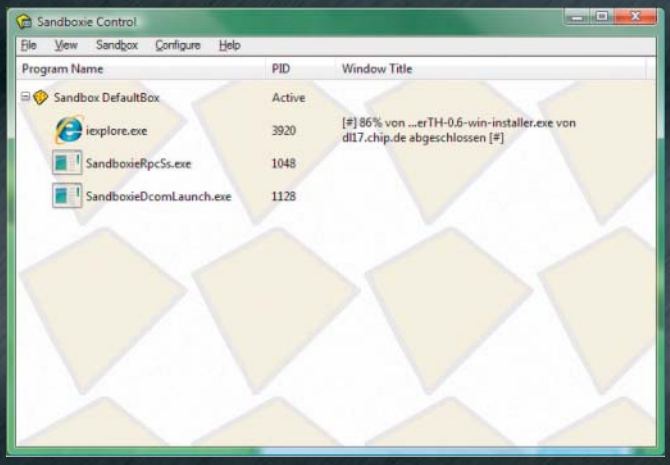
Dohled nad aplikacemi

Jakmile je Sandboxie nainstalováno, máte celou řadu možností, jak spustit programy v ochranném prostředí. Doporučujeme použít pravé tlačítko myši. Například bezpečný Firefox spustíte takto: klikněte pravým tlačítkem na ikonu Firefoxu a zvolte „Run Sandboxed". Firefox se spouští jako obvykle, ale funguje v kontrolovaném prostředí. Abyste poznali, že se tak opravdu děje, musíte vidět znak string „[#]", který Sandboxie používá k označení názvu programu v okně Windows.

Virtuální prostředí vám bude pochopitelnější, jakmile začnete ukládat na disk. Zpočátku vše běží normálně, ale pokud po „úspěšném uložení" nenajdete žádný soubor na disku, pak Sandboxie odvedlo svou práci…

Uvolnění stahování

Je zřejmé, že nebezpečné webové stránky by neměly mít přístup k počítači. Avšak Sandboxie by nemělo blokovat „downloady", které byly spuštěny záměrně. Proto tento bezpečnostní nástroj také nabízí možnost,



PRAKTICKÉ: **S nástrojem Sandboxie lze zabezpečit každou aplikaci – i Internet Explorer…**

která (pouze vám) umožní přístup k disku. V okně „Sandboxie Control" klikněte pravým tlačítkem na *Sandbox DefaultBox* a pak na *Sandbox Settings*. Nyní zvolte na levé straně stromové struktury příkaz *Recovery | Quick Recovery*. Poté přidejte složku pro své „downloady" pomocí příkazu *Add Folder* a vše potvrďte kliknutím na *OK*. Soubory uložené v tomto adresáři se neztratí.

Abyste se však k datům dostali, musíte kliknout pravým tlačítkem na ikonu Sandboxie v liště a zvolit *DefaultBox | Quick Recovery*. Poté se objeví okno se staženými daty. Označte si soubory, o které máte zájem, a klikněte na tlačítko *Recover to Same Folder*. Teď Sandboxie přenese soubory z virtuálního prostředí do „skutečné" složky pro stahování souborů, kde vám jsou data už normálně k dispozici.