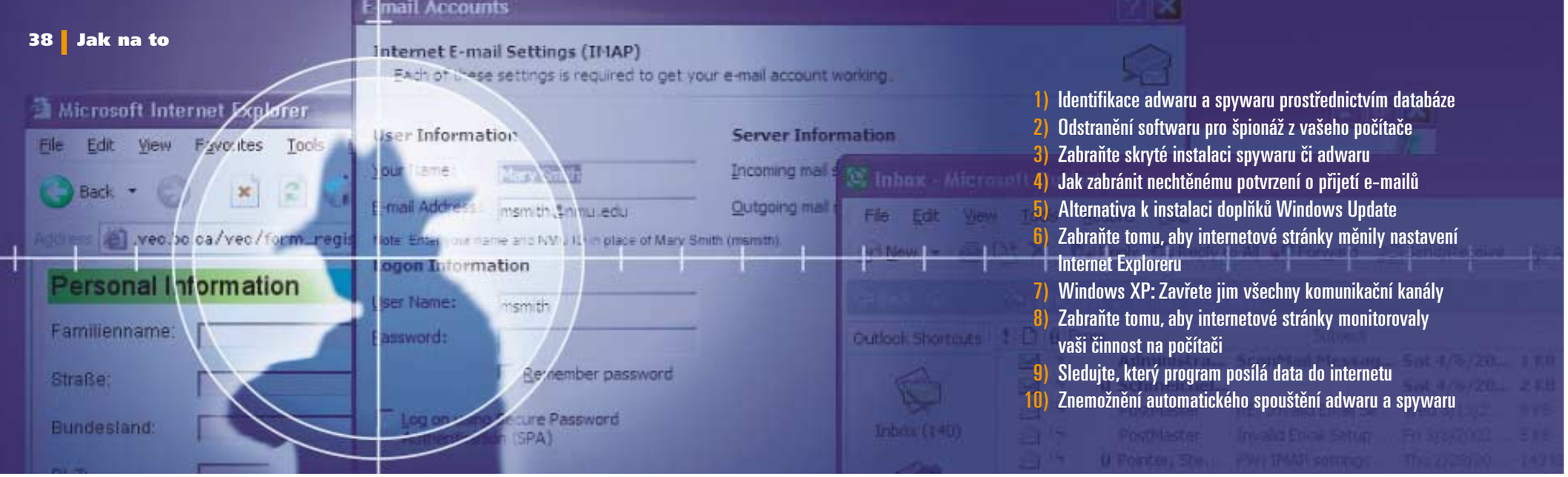


1) Identifikace adwaru a spywaru prostřednictvím databáze
2) Odstranění softwaru pro špionáž z vašeho počítače
3) Zabraňte skryté instalaci spywaru či adwaru
4) Jak zabránit nechtěnému potvrzení o přijetí e-mailů
5) Alternativa k instalaci doplňků Windows Update
6) Zabraňte tomu, aby internetové stránky měnily nastavení Internet Exploreru
7) Windows XP: Zavřete jim všechny komunikační kanály
8) Zabraňte tomu, aby internetové stránky monitorovaly vaši činnost na počítači
9) Sledujte, který program posílá data do internetu
10) Znemožnění automatického spouštění adwaru a spywaru

10 tipů proti spywaru

Jak se účinně bránit proti špionáži z internetu… (CD)

DAVID ČEPIČKA, DANIEL BEHRENS

Můžete být sledováni, a to takovým způsobem, že si toho vůbec nevšimnete. V mnoha programech jsou zabudovány funkce, které mají za úkol posílat přes internet data týkající se vašich osobních údajů či aktivit. Naše tipy a zdarma dostupné utility se vám v tomto článku pokusí pomoci.

Žádný z nás se nemůže před programy pro špionáž cítit dostatečně jistě. Řada výrobců softwaru si nechává do svých produktů zabudovat funkce monitorující, kolikrát jste danou aplikaci spustili a které její funkce nejčastěji používáte. Tyto informace se pak automaticky posílají přes internet. Stejně tak i při surfování po internetu se mohou na pevný disk vašeho počítače dostat programy, které se zabudují do operačního systému a pak vás v internetovém prohlížeči obtěžují spolu s dalšími reklamními pop-up okny.

Programy pro sledování (špionáž): O co vlastně jde

Používání tzv. adwaru či spywaru je jedním ze způsobů, kterým se může financovat jinak zdarma poskytovaný freeware, nebo jde o možnost, jak z programu šířeného jako shareware získat nějakou tu korunu navíc.

V případě adwaru se jedná o takové komponenty programu, jež slouží k tomu, aby se v uživatelském rozhraní aplikace zobrazila reklama (anglické slovíčko *Ad* znamená česky reklama). Za předpokladu, že tyto komponenty nenavazují připojení k internetu, je tato metoda z hlediska špionáže prakticky bezproblémová. Ovšem pokud se jedná o adware, který se připojuje k nějakému internetovému serveru kupříkladu proto, aby z něj stahoval nějaké reklamní banery (proužky), je třeba mít se na pozoru. Je totiž docela dobře možné, že se při tomto přenosu zároveň do internetového serveru přenášejí informace o vaší osobě a vašich zvyklostech, dále o hardwarovém či softwarovém vybavení vašeho počítače. Pak se totiž adware stává tzv. spywarem (z anglického „*to spy*" – tajně pozorovat, sledovat). Takové funkce však má pouze jistá část reklamních modulů.

Vedle kombinovaného ad/spywaru však existuje i čistokrevný spyware. V tomto případě se jedná o drobné komponenty, jež se instalují společně s daným programem, ovšem jejich instalace se provádí bez vědomí uživatele. Spyware potom trpělivě vyčkává na pozadí a zaznamenává všechny akce, které uživatel na svém počítači či provádí, v horším případě pak s operačním systémem manipuluje podle svého gusta.

Třetí skupinou programů patřících do kategorie spywaru jsou utility, které jsou přímo pro sledování daného uživatele určeny. Příkladů takových programů je velké množství. Ať už se jedná o programy, kterými nadřízený tajně kontroluje pracovitost svých zaměstnanců, nebo ať jde o aplikace typu Keyloggeru, jejž může do počítače propašovat útočník, aby kupříkladu zjistil vaše přístupová hesla k nejrůznějším službám.

Ochrana před špionážními programy

V tomto článku bychom vám chtěli poradit, jak se podívat špionážním programům na zoubek a jak je případně zlikvidovat. Dozvíte se tedy nejenom to, jak se už před instalací nějakého programu ujistit, zda neobsahuje nějaký adware či spyware, nýbrž také, jak si váš operační systém prostřednictvím dvou zdarma dostupných programů opravdu od základů prověřit, zda nějaký škodlivý software neobsahuje. Určitě bude pro vás rovněž důležité, aby se adware či spyware nedostal na váš počítač ani při práci s internetovým prohlížečem. Výrobci programů totiž rádi využívají tzv. technologii Active-X zabudovanou v Internet Exploreru. Tato technologie je naopak primárně určena pro to, aby mohl být internetový prohlížeč rozšířen o další užitečné funkce. Zneužití této technologie pak představuje závažný problém, jehož řešení se vám pokusíme nabídnout.

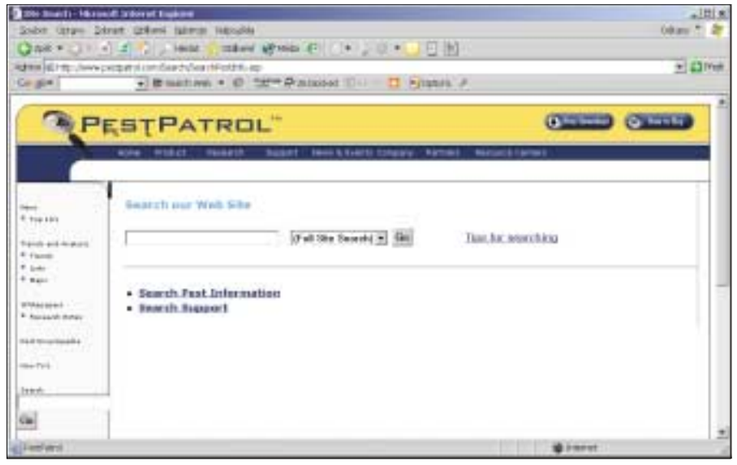
Prvky Active-X jako parazity – kupříkladu Gator

Asi nejlepším příkladem pro zneužívání technologie Active-X jsou tři komponenty vyprodukované firmou Gator, která se před časem přejmenovala na firmu Claria, pravděpodobně proto, že dřívější název již byl u mnoha uživatelů dostatečně nechvalně známý. Zmiňované komponenty se jmenují Date Manager, Precision Time a Gator eWallet a mají společné dvě stránky. První a bezesporu užitečnou stránkou je například u komponenty Gator eWallet možnost automaticky vyplňovat webové formuláře, komponenta Precision Time zase například seřizuje čas na počítači podle času na časovém serveru na internetu.

Druhou stránkou, již ne tak pozitivní, je skutečnost, že všechny prvky jsou vybaveny komponentou pro zobrazování reklamy, která slouží k tomu, aby se při brouzdání na internetu zobrazovala reklamní okna. Dále vedou též statistiku o využívání vašeho počítače. Jak firma Claria udává ve svém prohlášení o ochraně dat na **www.gator.com/help/app_ps_v51.htm**, je sledováno a zaznamenáváno softwarové vybavení vašeho počítače, adresy „některých" (!?) internetových stránek, které navštěvujete a také čas, který na nich strávíte. Kromě všech těchto aktivit rovněž sleduje, jak často spouštíte určité aplikace. Co se myslí „určitými aplikacemi", to však již z prohlášení nevyplývá. Dále je tam psáno, že vaše kompletní identita odhalena nebude, neboť software sbírá pouze vaše křestní jméno, město, v němž bydlíte, poštovní směrovací číslo a stát, jehož jste obyvatelem. Odkud komponenty zmiňované informace získávají, není příliš jasné. I když, koho by nenapadla souvislost mezi osobními údaji a komponentou Gator eWallet – program pro automatické vyplňování formulářů přece musí být plný vašich osobních dat, protože jinak jeho použití ztrácí smysl.

Vystopováni mohou být všichni, co hodně surfují

I při surfování na internetu musíte počítat s tím, že vaše chování může být sledováno a zaznamenáváno. To sice probíhá anonymně a ve většině případů určitě ne v tak rozsáhlé formě jako u komponent firmy Claria, přesto to není pro uživatele nic, z čeho by mohl mít radost nebo uži-



▲ **Zjistěte si před stažením programu, zda vás nesleduje: Položte dotaz do databáze www.pestpatrol.com/Search/SearchPestInfo.asp**

tek, o bezpečnosti ani nemluvě. I v tomto případě vám poradíme, kde na vás může číhat nějaká past.

Pro řešení problémů vám v tomto článku nabízíme celou řadu freewarových a sharewarových utilit. Prakticky všechny tyto užitečné aplikace naleznete i NA NAŠEM CD.

1) Identifikace adwaru a spywaru prostřednictvím databáze

Problém: ***Chtěli byste před instalací nějakého programu vědět, zda neobsahuje nějaký špionážní software.***

Řešení: Použijte on-line databázi dostupnou na internetové adrese **www.pestpatrol.com/Search/SearchPestInfo.asp**. Tato služba je stále aktualizována a tak postihuje prakticky všechny utility, o nichž je známo, že mají za úkol sledovat činnost uživatele pracujícího na počítači.

Tipy: Zadejte do vyhledávacího políčka název programu, jenž se vám zdá podezřelý. Pokud se zmiňovaná aplikace v databázi nenalézá, získáte jako výsledek prohledávání větu „*No documents matched the query*“. Pak je takový program pro vás s nejvyšší pravděpodobností bez nebezpečí. Jinak získáte seznam nalezených odkazů, v nichž se vyskytuje název programu. Pokud některý z nich prozkoumáte a zjistíte, že se v textu s popisem programu v poli *Category* objeví odkazy *Adware* či *Spyware*, měli byste okamžitě od stahování takového programu upustit.

Spyware či adware se vyskytuje především u freewarových či sharewarových programů, jež byly vyrobeny v USA. Aplikace naprogramované u nás či třeba v Německu obsahují komponenty pro sledování uživatelů jen velmi zřídka.

Existuje ovšem i adware bez funkcí pro sledování. Kupříkladu internetový prohlížeč **Opera** ve své zdarma dostupné variantě zobrazuje reklamní baner. Výrobce programu však na své internetové stránce **www.opera.com/support/search/supsearch.dml?index=453** slibuje, že činnost uživatele na počítači není sledována.

Protipólem výše popsaného programu je aplikace **Kazaa** pro výměnu hudby, neboť na své internetové stránce **www.kazaa.com/us/help/faq/howis_kazaa_free.htm** otevřeně přiznává, že její zdarma dostupná varianta jisté aktivity uživatele počítače zaznamenává. Ovšem za 29,95 USD autor programu nabízí verzi prostou jakéhokoliv adwaru či spywaru.

2) Odstranění softwaru pro špionáž z vašeho počítače

Problém: ***Máte pocit, že jste si do počítače v poslední době pravděpodobně nainstalovali nějaký spyware či adware, a nyní stojíte před otázkou, jak se jej zbavit.***

Řešení: Pro vyčištění vašeho počítače vám doporučujeme použít dvě zdarma dostupné utility – **Ad-Aware 6.181 SE** a **Spybot Search&Destroy 1.2**. Obě naleznete NA NAŠEM CD. Nejlépe uděláte, pokud použijete postupně obě utility, neboť ne každá aplikace vždy všechno najde. Program Ad-Aware je pro soukromé použití zdarma. NA NAŠEM CD rovněž naleznete instalační program **Language Pack**, který mimo jiné obsahuje i český jazykový modul. Po instalaci Ad-Aware spusťte instalaci Language Packu. Potom otevřete Ad-Aware, klepněte na ikonku *Settings* a v poli *Language file* nastavte volbu *Czech*. Nastavení potvrďte stiskem tlačítka *Provést*.

Tipy: Určitě byste měli vědět, že mnohé programy vybavené moduly pro zobrazování reklamy či pro sledování aktivit prováděných na vašem počítači přestávají v řadě případů fungovat, pokud zmíněné moduly odstraníte.

Ad-Aware: Tato utilita vyhledává adware či spyware přítomný v operační paměti a na pevném disku vašeho počítače. Chová se podobně jako antivirový program, neboť má také jakýsi definiční soubor, v němž jsou obsaženy již známé škodlivé programy výše uvedeného typu. V Ad-Awaru je rovněž zabudována funkce aktualizace, díky níž bude definiční soubor vždy v aktuálním stavu.

Zmíněnou aktualizaci byste měli provádět vždy předtím, než se rozhodnete prověřit svůj počítač, neboť je jasné, že pouze program s nejaktuálnějším seznamem potenciálně škodlivých programů vám tyto pomůže odhalit. Update provedete tak, že se připojíte k internetu, spustíte Ad-Aware, v něm klepnete na tlačítko *Stav* a zde na položku *Aktualizovat nyní*. Vlastní update pak spustíte klepnutím na tlačítko *Připojit*.

Poté, co Ad-Aware prověří váš systém, zobrazí vám seznam všech nalezených objektů. Z nich si můžete vybrat, které budete chtít odstranit do karantény. Samotné odstranění provedete postupným klepáním na tlačítko *Další*. Pod tlačítkem *Ukázat protokol* se vám zobrazí podrobné informace o všech provedených operacích. Jestliže byste se někdy později rozhodli smazané soubory znovu obnovit, stiskněte tlačítko *Karanténa*. Tam si vyberte odpovídající zazálohované objekty a stiskněte tlačítko *Obnovit*.

Utilita Ad-Aware standardně prohledává registr a disk s operačním systémem, což se v praxi může jevit jako nedostatečné. Stiskněte proto tlačítko *Skenovat* a v poli *Režim skenování* klepněte na odkaz *Přizpůsobit*. Nyní klepněte na tlačítko *Skenování* a v poli *Soubory & Adresáře* si nastavte všechny disky a adresáře, které chcete skenovat. V poli *Paměť & Registry* pak doporučujeme aktivovat volby *Skenovat záložky IE na blokované stránky* a *Scan my Hosts file*.

Pokud si za program připlatíte, můžete získat tzv. **Ad-Aware Plus**, který vám nabídne automatickou kontrolu prováděnou na pozadí, funkčností podobnou té, co nabízejí antivirové programy.

▶ **Velmi spolehlivý program pro odstranění spywaru: Ad-Aware prověří celý váš počítač na přítomnost spywaru či adwaru. Pokud si to budete přát, dokáže nalezené komponenty i odstranit**

Spybot Search&Destroy: Při našich testech Spybot našel na našem počítači více špionážních programů než Ad-Aware. Na druhou stranu Ad-Aware našel jeden spyware, který Spybot přehlédl.

Pro spuštění prohledávání stačí pouze stisknout tlačítko *Scan*. Spybot má tu vlastnost, že před smazáním nalezených objektů automaticky vytváří jejich zálohy. Pokud se později rozhodnete některou z komponent nahrát zpět, postačí vám stisk tlačítka *Obnovit*.

Velmi praktickou se jeví funkce *Immunize*. Ta doslova naočkuje Internet Explorer tak, aby při surfování na internetu nestahoval žádné ActiveX prvky, o nichž je známo, že patří k některému z adwarových či spywarových programů. Proto by se vám už na monitoru nemělo nikdy ukázat dialogové okno, které vás vyzve k potvrzení pro nainstalování takového ActiveX prvku. Tím pádem rovněž pomine nebezpečí, že instalaci takového prvku spustíte tím, že omylem ve zmíněném dialogovém okně klepnete na tlačítko *Ano*. Funkci *Immunize* byste měli spouštět po každém updatu definičních souborů Spybotu, tak aby byl Internet Explorer proti těmto prvkům patřičně vyzbrojen.

Spybot se dá přes tlačítko Start otevřít ve dvou zobrazeních. Tzv. *Easy mode* omezuje výběr funkcí jen na ty nejdůležitější, a je tedy velmi vhodný pro začátečníky. Profesionálové by v každém případě měli vyzkoušet režim *Advanced mode*. V něm se dá provést řada pokročilých nastavení, kupříkladu vypnout jednotlivé rutiny pro prověřování programů, či zautomatizování funkce *Immunize*, tak aby tato byla prováděna vždy po provedení aktualizace definičního souboru Spybotu.

3) Zabraňte skryté instalaci spywaru či adwaru

Problém: ***Obáváte se toho, aby se vám při surfování na internetu bez vašeho vědomí nenainstaloval nějaký špionážní software.***

Řešení: Zakažte v Internet Exploreru možnost stahování ActiveX prvků anebo použijte funkci *Immunize*, kterou disponuje program **Spybot Search&Destroy** (viz tip č. 2).

Tipy: Technologie prvků ActiveX integrovaná v Internet Exploreru zajišťuje možnost rozšíření internetového prohlížeče o další funkce. Asi nejznámějším programem využívajícím technologii ActiveX je přehrávač **Flash** firmy Macromedia, který umožňuje přehrávání animací zabudovaných v internetových stránkách. Právě zmiňovaná technologie může být ve vašem počítači zneužita k proniknutí takových nechtěných a nebezpečných programů, jako jsou trojské koně, dialery nebo dokonce aplikace pro sledová-

ON-LINE minitipy

Surfování na internetu

Nastavení standardního programu pro prohlížení internetu

V případě prohlížeče Mozilla si jej můžete jako výchozí program pro surfování na internetu nastavit přes menu *Úpravy/Předvolby* pod položkou *Prohlížeč*, když stisknete tlačítko *Set Default Browser*. Tím se vám nastaví k otevření v tomto programu i všechny odkazy ve složce *Oblíbené položky* v nabídce Start. Pokud budete chtít jako výchozí internetový prohlížeč nastavit znovu Internet Explorer, poklepejte v Ovládacích panelech na ikonu *Možnosti Internetu*. Na záložce *Programy* pak umístěte zatržítko před položku *Aplikace Internet Explorer by měla zkontrolovat, zda je nastavena jako výchozí prohlížeč*, a potom spusťte Internet Explorer.

Internetový prohlížeč

Rychlé vytvoření zástupce

Pro rychlé vytvoření zástupce právě otevřené WWW stránky přetáhněte ikonu z levého horního okraje lišty okna prohlížeče na místo, kde chcete zástupce vytvořit. Tento postup funguje jak u programu MS Internet Explorer, tak i u Mozilly.

Internet Explorer

Chyba při ukládání

Pokud ukládáte stránku v Internet Exploreru přes *Soubor/Uložit jako…* a v poli *Uložit jako typ* máte *Webový archiv, jediný soubor* a při tomto typu ukládání vám nejde žádná stránka uložit a neustále se objevuje chybové hlášení, pak je většinou na vině špatně zaregistrovaná některá z knihoven programu. Pokud pracujete ve Windows 95/98 a NT4, zkontrolujte nejprve, zda máte nainstalovaný Outlook Express – ten je totiž nezbytnou podmínkou pro fungování webových archivů. Potom zadejte na příkazový řádek následující příkaz:

regsvr32 inetcomm.dll

Tím by se měl problém s ukládáním stránek vyřešit.

Telefonické připojení sítě

Automatické odpojení

Automatické odpojení navázaného telefonického připojení sítě při zavření posledního okna internetového prohlížeče funguje pouze tehdy, pokud nemáte otevřený ani Windows Messenger, ani žádný soubor nápovědy ve formátu HTML.

Internet Explorer

Špionáž? Dialer!

Pokud některá internetová stránka vám s velkou slávou zobrazí obsah vašeho pevného disku, aby vás tak upozornila na to, že váš systém obsahuje povážlivou bezpečnostní trhlinu, nenechte se nijak znepokojit. Cílem této taktiky je u vás způsobit strach a využít vašeho úleku k urychlenému nainstalování nějaké pochybné utility. Ostatně zakrátko se vám objeví nabídka na její stažení. Obsah vašeho pevného disku se ale dá jako obrázek ukázat na monitoru pomocí funkce zabudované v Internet Exploreru. Takže vlastně nepochází z internetové stránky a nemůže ani být na ni ani nijak přenesen.

Internet Explorer

Zahlazení stop po surfování na internetu

Nejrychleji po sobě zametete stopy vzniklé při vašem posledním surfování na internetu tak, že si nejprve otevřete Ovládací panely a tam si poklepete na ikonu *Možnosti internetu*. Na záložce *Obecné* pak už stačí stisknout tlačítka *Vymazat soubory cookie*, *Odstranit soubory* a *Vymazat historii*.

Internet Explorer

Oblíbené položky

Oblíbené položky v menu (nikoliv v panelu nástrojů!) *Oblíbené* Internet Exploreru se automaticky otevírají, pokud do nich přetáhnete soubor URL nebo odkaz na nějakou stránku. Tato vlastnost se hodí zvláště tehdy, pokud potřebujete nějaký odkaz umístit do některé z podsložek Oblíbených položek. K tomu účelu přetáhněte například ikonu v levém horním okraji okna prohlížeče se stisknutým levým tlačítkem myši do menu *Oblíbené*, po jeho rozbalení se přesuňte na požadovanou podsložku a pusťte tlačítko myši.

▲ **Pozor u takovýchto dialogových oken: Tady se právě pokouší jeden ze špionážních programů nainstalovat do vašeho počítače**

ní vašich aktivit na počítači. Dostanete-li se při surfování na internetu na stránku, která využívá nějaký prvek ActiveX, obdržíte v případě standardního nastavení Internet Exploreru upozornění zabezpečení systému, které vám dává možnost instalaci takového prvku povolit či odmítnout. Pokud máte jenom trochu pochybností, měli byste instalaci takových prvků zcela určitě zamítnout.

Jakmile se totiž nějaký program využívající technologie ActiveX jednou dostane do počítače, získá tím k vašemu systému úplná přístupová práva, takže může odesílat a přijímat prakticky libovolná data. Souhlasit s instalací takových prvků byste měli opravdu pouze v případě, kdy provozovateli takových internetových stránek bezvýhradně důvěřujete.

Pokud sázíte na jistotu, můžete také jako alternativu použít možnost úplného zákazu používání technologie ActiveX. K tomu účelu klepněte v menu *Nástroje* na položku *Možnosti Internetu* a přesuňte se na záložku *Zabezpečení*. Ujistěte se, že jako zónu obsahu máte nastavenu položku *Internet*, a stiskněte tlačítko *Vlastní úroveň*. V dialogovém okně *Nastavení zabezpečení* si pak vyhledejte položku *Stahovat podepsané ovládací prvky ActiveX*, nastavte ji na volbu *Zakázat* a klepněte na *OK*. Ocitnete se zpět na kartě *Zabezpečení*. Nyní vyberte ikonu *Důvěryhodné servery*. V případě, že chcete pro některé internetové stránky udělat výjimku a dovolit, aby se z nich prvky ActiveX mohly stahovat, stiskněte tlačítko *Servery* a do okna, které se objeví, zadejte internetové adresy pro servery, jež považujete za důvěryhodné. Úroveň zabezpečení zóny *Důvěryhodné servery* pak nastavte na střední. V případě, že bude na internetových stránkách serverů, kterým důvěřujete, nějaký prvek ActiveX, jejž bude nutno do vašeho počítače nainstalovat, budete vždy před jeho instalací požádáni o svolení.

Jednodušší, i když méně bezpečnou variantou je použití funkce *Immunize*, což je funkce utility Spybot Search&Destroy (viz tip č. 2). Zmíněná funkce dokáže zabránit instalaci již známých škodlivých prvků ActiveX. Ovšem nebude vám k ničemu u špionážního softwaru, který ještě není v databázi programu zaznamenán.

4) Jak zabránit nechtěnému potvrzení o přijetí e-mailů

Problém: ***Prostřednictvím do e-mailu vnořených a skrytých obrázků si může odesílatel e-mailu snadno zjistit, zda jste jeho zprávu obdrželi a zda jste si ji i přečetli. To-muto byste však chtěli zabránit.***

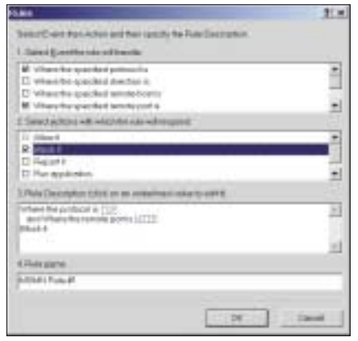
Řešení: Na výběr máte několik možností. První možností je používat program pro práci s elektronickou poštou tak, aby sice vytvářel e-maily ve formátu HTML, ale aby obrázky vložené do e-mailu zobrazoval pouze tehdy, když jsou v něm vloženy jako příloha – ne tedy tak, že se musejí při pokusu o jejich otevření teprve stahovat z internetu. Takto vhodně se dá nakonfigurovat například zdarma dostupný program pro práci s elektronickou poštou **Pegasus Mail**, který naleznete NA NAŠEM CD.

Jestliže pro práci s e-maily využíváte Outlook Express, nakonfigurujte jej tak, aby zobrazoval e-maily pouze v textovém formátu.

Další možností je použití firewallu, který filtruje nejen na úrovni portů, ale také na úrovni aplikací. Takovým je například zdarma dostupný **Outpost Firewall**, který rovněž naleznete NA NAŠEM CD. V něm si vytvořte nové pravidlo, jež vašemu programu pracujícímu s elektronickou poštou dovolí odesílání a přijímání e-mailů na standardních portech 110 a 25, ovšem zakáže nahrávání objektů přes protokol *http* na portu 80.

Tipy: Zvláště ti, co se živí rozesíláním reklamy, a také rozesilatelé spamu mají eminentní zájem se nějakým způsobem dozvědět, zda jejich reklamní e-maily příjemci čtou. Někteří proto do odesílaných e-mailů vkládají odkazy na obrázky ležící na jejich serveru. Často se však jedná o transparentní obrázky, které příjemce stejně neuvidí. Název souboru s obrázkem je prostřednictvím speciální utility pro každého příjemce vždy znovu vygenerován a pak přiřazen do seznamu e-mailových adres. Program pro práci s elektronickou poštou pak tyto vložené obrázky automaticky nahrává v případě, že podporuje HTML formát e-mailů a že je k dispozici připojení k internetu.

▲ **Zvýšení bezpečnosti v Outlook Expressu: Aktivujte si položku Číst všechny zprávy jako prostý text. Pak vám program nebude zobrazovat žádné e-maily ve formátu HTML a potenciální škůdci nemají žádnou šanci**



▲ **Více bezpečnosti: Zkonfigurujte si Outpost Firewall Free tak, aby váš program pro práci s elektronickou poštou nesměl z internetu stahovat žádný potenciálně škodlivý obsah**

Na základě souborů se záznamy o přístupu k WWW serveru pak může rozesilatel reklamních e-mailů rozpoznat, které obrázky byly otevřeny. Speciální software pak tyto soubory porovná s dříve sestaveným seznamem, v němž jsou přiřazeny soubory obrázků k e-mailovým adresám a tím se získá seznam těch, kteří si e-mail s reklamou přečetli. Obrázky používané ke zmiňovaným praktikám sledování uživatelů se nazývají *Moles* (v českém překladu Krtci).

Změna programu pro práci s elektronickou poštou: Tento způsob předpokládá, že si chcete zvykat na novou aplikaci. Bohužel například Pegasus Mail spoustu zpráv v HTML formátu zobrazuje s chybami.

Outlook Express: Uživatelé Outlook Expressu 6.0 SP1 mohou zakázat zobrazování e-mailů ve formátu HTML. Stačí k tomu klepnout do menu *Nástroje/Možnosti* a přesunout se na kartu *Čtení*. Zde zatrhněte položku *Číst všechny zprávy jako prostý text*. V mnoha případech pak ale Outlook Express zobrazí prázdné okno se zprávou, a to zvláště tehdy, když program pro práci s elektronickou poštou odesílatele nevytváří, jak je zvykem, textovou verzi bez HTML formátování a tuto nezasílá společně v e-mailu se zprávou v HTML formátu.

Firewall: Toto řešení vyžaduje poněkud náročnější konfiguraci systému. Celý postup budeme vysvětlovat na příkladu programu **Outpost Firewall Free**, který je zdarma dostupný na internetu a samozřejmě jej najdete i NA NAŠEM CD. Stejně tak vám přinášíme i novější verzi **Outpost Firewall Pro 2.1**, která je však distribuována pouze jako 30denní trial verze. V dalším textu budeme popisovat verzi Outpost Firewall Free. Vycházíme z předpokladu, že pro váš program pro práci s elektronickou poštou nejsou definována doposud žádná pravidla a že máte Outpost spuštěný. Spusťte si nyní program pro práci s elektronickou poštou a spusťte v něm přijímání a odesílání zpráv. V tomto okamžiku se objeví dialogové okno Outpostu, které se vás bude ptát, zda může poštovnímu programu dovolit připojit se k internetu. Nyní označte možnost *Create rules using preset* a potvrďte stiskem *OK*. Jestliže se vám ukázalo dialogové okno *Rules*, aktivujte v něm položku *Allow all activities*.

V dalším kroku zakážete svému programu pro práci s elektronickou poštou stahovat obrázky a další objekty, které budou vloženy přímo v e-mailech ve formátu HTML. Obrázky, jež budou posílány zvlášť jako příloha, budou samozřejmě zobrazovány dále. Otevřete si hlavní okno Outpostu a v něm si vyberte volbu *Options/Application*. Zde by se nyní měla objevit položka pro váš program pro práci s elektronickou poštou, a to v poli *Partially allowed applications*. Poklepejte na ni a ověřte si, zda se v následujícím dialogovém poli objevila položka končící výrazem *http connection*. Pokud tomu tak je, pak ji odstraňte. Nyní stiskněte tlačítko *New* a aktivujte volbu *Where the specified protocol is*. Nyní klepněte na políčku *Rule Description* na položku *Undefined* a z ní vyberte výraz *TCP*. Potom označte body *Where the specified remote port is* a *Deny it*. V poli *Rule Description* opět klepněte na *Undefined* a do následujícího políčka vložte hodnotu 80. To je číslo portu, přes nějž komunikují internetový prohlížeč a programy pro práci s elektronickou poštou, aby mohly stahovat objekty jako jsou například již zmíněné obrázky.

Zklamáni budou zřejmě ti uživatelé Outlook Expressu, kteří mají své poštovní stránky u Hotmailu, jenž ve všech případech používá port 80. Vzhledem k tomu, že jsme v předcházejícím kroku Outlook Expressu zakázali přistupovat na port 80, nebude již nadále možné stahovat poštu z Hotmailu a tak jediná cesta, která bude k dispozici, povede vždy přes webové rozhraní internetového prohlížeče.

5) Alternativa k instalaci doplňků Windows Update

Problém: ***Pracujete ve Windows 98, 2000, ME, nebo XP a chtěli byste zabránit tomu, aby Microsoft prostřednictvím funkce Windows Update shromažďoval informace o vybavení vašeho počítače.***

Řešení: Nejprve zapomeňte na spuštění funkce Windows Update. V případě, že pracujete ve Windows XP, deaktivujte rovněž i provádění automatických aktualizací. Všechny důležité záplaty a updaty získáte prostřednictvím stránek *Microsoft Download Center*.

Tipy: V časopise Tecchannel byla v článku v originále nazvaném **Windows-Update unter der Lupe** (k dispozici je též na internetové adrese **www.tecchannel.de/betriebsysteme/1125/12.html**) provedena analýza služby Windows Update. Byla zaměřena zejména na zjištění, která data jsou prostřednictvím zmiňované služby Microsoftu zasílána. Výsledkem bylo konstatování, že prostřednictvím Windows Update Microsoft získává nejen tzv. *Product-ID*, aby si ověřil, zda se jedná o legálně získanou verzi operačního systému. Přes internet se zasílá i seznam všech hardwarových komponent na počí-

ON-LINE minitipy

Internet Explorer

Zabezpečené připojení

Pokud chcete vědět, zda je připojení k nějaké internetové stránce zabezpečeno přes protokol SSL, podívejte se na stavový řádek internetového prohlížeče. Mozilla a Nescape vám tuto skutečnost ukazují pomocí žlutého zámku, u Internet Exploreru je rovněž žlutý zámek, který je ovšem viditelný pouze při zabezpečení SSL.

Internet Explorer

Uložení Oblíbených položek

Svoje *Oblíbené položky* si můžete zazálohovat buď kompletně všechny, anebo pouze ty, jež se nacházejí v nějaké podsložce *Oblíbených položek*. Použijete k tomu funkce importu a exportu Internet Exploreru, jež vytvoří HTML soubor, v němž tyto odkazy budou uvedeny. Klepněte do menu *Soubor/Import a export* a ve stručném průvodci si v jednotlivých krocích nastavte složku či podsložku, kterou budete chtít exportovat.

Internet Explorer

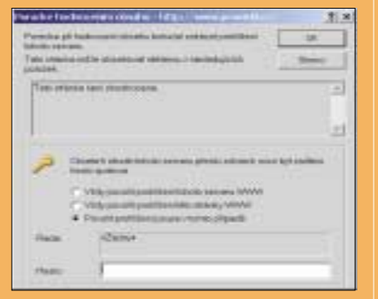
Funkce Automatické dokončování

Každá položka, kterou zadáváte při vyplňování formulářů na internetových stránkách, se umístí do seznamu vytvořeného funkcí automatického dokončování a objeví se znovu při zadání počátečních písmen uloženého výrazu opět do nějakého jiného internetového formuláře. Objevují se zde však i položky, obsahující pravopisné chyby. Takové slovo pak při zadávání jednoduše vyberte a stiskněte klávesu <Delete>, čímž ji ze seznamu automatického dokončování odstraníte.

Internet Explorer

Bezcenný filtr pro kontrolu obsahu stránek

Poradce hodnocením obsahu, jenž se nachází v Internet Exploreru v menu *Nástroje/Možnosti Internetu* na záložce *Obsah*, slibuje filtr pro kontrolu obsahu internetových stránek, s jehož pomocí by měly být například děti chráněny před zobrazením nevhodných stránek. Podle našeho názoru je zbytečnou ztrátou času se tímto nástrojem vůbec zabývat, neboť asi těžko nějaká internetová stránka obsahující sex či obsah vhodný pouze pro dospělé bude takový filtr používat. Pokud tedy takovou funkci zapnete, výsledkem bude to, že si zablokujete přístup k celému webu, neboť Internet Explorer zakáže zobrazení každé stránky bez



tohoto filtru. Jak vidíte na obrázku, je z výše uvedeného důvodu i obsah internetové stránky **www.pcworld.cz** pro děti nevhodný.

Internet Explorer

Nastavení zabezpečení

K nastavení úrovně zabezpečení internetu se dostanete z libovolného okna Internet Exploreru. Na stavovém řádku vpravo dole najdete ikonu internetu. Když na ni poklepete, dostanete se přímo do dialogového okna pro nastavení zabezpečení.

Internet Explorer

Prohlížení obsahu WWW stránky

Internetová stránka se vám už nahrává celou věčnost, a přesto ještě není nic vidět. Nevzdávejte se však, nýbrž proces načítání zkraťte. Mnohdy je většina obsahu stránky již načtena, chybí pouze nějaký větší obrázek nebo snad už vůbec přebytečný nějaký reklamní baner. Přenos dat pro internetovou stránku přerušíte stiskem klávesy <Esc>. V mnoha případech nyní uvidíte alespoň část stránky, když už ne celou. Budou ale chybět obrázky, jež budou nahrazeny pouze odkazy na ně.

Internet Explorer

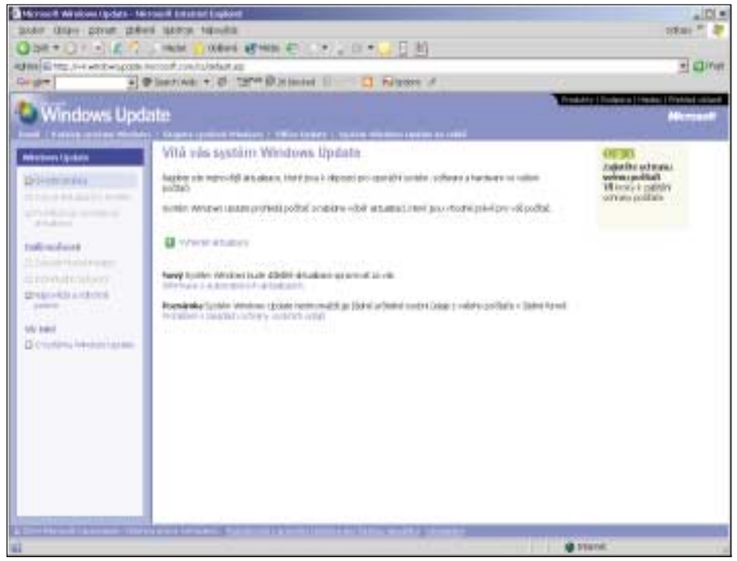
Rychlé vyplňování internetových formulářů

Na internetové stránce potřebujete vyplnit formulář obsahující velký počet políček. Není v tomto případě pro přesun mezi jednotlivými políčky nutné používat myš. Klávesou <Tab> se posunte o políčko vpřed a naopak klávesovou zkratkou <Shift><Tab> o políčko formuláře zpět.

tači nainstalovaných. Pravda, že oficiálně pouze k tomu, aby se mohly vyhledat aktualizace ovladačů pro tyto komponenty a mohla se následně doporučit jejich instalace. A oficiálně Microsoft tato data ani nikde neukládá. Stejně se ale jen trochu nedůvěřivější uživatel bude funkci Windows Update vyhýbat. Někteří už snad i kvůli tomu, že se do ní údajně má zabudovat funkce, která bude načítat i softwarové vybavení počítače. Zatím zmiňovaná funkce ještě není aktivována.

Jak ale vypadá slibovaná alternativa? Důležité bezpečnostní záplaty uveřejňuje Microsoft i jednotlivě. Dají se nalézt na tzv. Download Centru na internetové adrese **www.microsoft.com/downloads/search.aspx?displaylang=cs**. Z rozevíracího políčka *Produkt či technologie* si vyberte vámi používanou verzi Windows, klepněte na tlačítko *Hledat* a na další stránce pak zvolte z rozevíracího menu *Seřadit výsledky podle Datum* a stiskněte tlačítko *Přejít*. Nyní uvidíte ty nejnovější updaty pro váš systém.

Uživatelé operačního systému Windows XP mohou automatický update Windows deaktivovat buď pomocí utility **XP Antispy** (viz dále), nebo ručně. Klepněte si na Ovládací panely a poklepejte na ikonu *Systém*. Na záložce *Automatické aktualizace* zrušte možnost *Udržovat počítač aktualizovaný* (Windows XP SP1). Pokud si přejete být o nových updatech pravidelně informováni, nechte si zasílat tzv. *Microsoft Newsletter*. Registrovat se můžete na adrese **http://register.microsoft.com/subscription/subscribeme. asp?ID=135**.



▲ **Windows Update: Funkce pro aktualizaci operačního systému Windows přenáší Microsoftu spoustu dat o hardwarovém vybavení vašeho počítače. Oficiálně ale firma tato data neukládá**

6) Zabraňte tomu, aby internetové stránky měnily nastavení Internet Exploreru

Problém: ***Po jednom surfování na internetu zjišťujete, že se vám najednou v Internet Exploreru změnila domovská stránka a stránka pro vyhledávání, navíc zjišťujete, že se vám do oblíbených položek uložily odkazy na stránky, které jste tam původně vůbec neměli.***

Řešení: Konfiguraci Internet Exploreru si můžete provádět pouze manuálně. Takto provedená nastavení si však můžete chránit, a to instalací zdarma dostupné utility **Browser Hijack Blaster**, kterou naleznete NA NAŠEM CD.

Tipy: Méně seriózní provozovatelé internetových stránek využívají bezpečnostních trhlin v Internet Exploreru k tomu, aby vám podstrčili svoje odkazy nebo aby vám změnili nastavení domovské stránky, stránky pro vyhledávání či jinak pozměnili konfiguraci Internet Exploreru. V některých případech se tyto akce dají provádět prostřednictvím prvků ActiveX, jejichž instalaci jste zřejmě nějakým nedopatřením povolili. Motivem pro toto jednání provozovatelů webu může být fakt, že si takto chtějí zvýšit návštěvnost svých internetových stránek, což vede ke zvýšení podílu reklamy a potažmo i zisku.

Návrat nastavení prohlížeče do původního stavu: Pro návrat takto nechtěně provedených nastavení zkuste ze všeho nejdřív změnit domovskou stránku a stránku pro vyhledávání na standardní (výchozí) hodnoty. Klepněte proto v menu *Nástroje* na příkaz *Možnosti Internetu* a na záložce *Programy* stiskněte tlačítko *Obnovit webové nastavení*. Nechtěné odkazy v oblíbených položkách odstraníte přes menu *Oblíbené* a příkaz *Uspořádat oblíbené položky*.

▲ **Browser Hijack Blaster: Tato utilita vás varuje v momentě, kdy se nějaká internetová stránka pokouší změnit domovskou stránku či stránku pro vyhledávání**

Nyní zavřete Internet Explorer a spusťte jej znovu. Pokud bude vše v pořádku, pak jste měli skutečně štěstí v neštěstí.

Jestliže se manuální přenastavení konfigurace neosvědčilo a po spuštění Internet Exploreru je vše nastaveno jako předtím, pak je ve vašem systému přítomen nějaký prvek ActiveX, jenž provádí konfiguraci Internet Exploreru vždy podle svého gusta. Je proto třeba tohoto záškodníka najít a odstranit. Doporučujeme použít některý z programů Ad-Aware či Spybot Search&Destroy (anebo klidně oba, jak to bylo popsáno v tipu č. 2).

Browser Hijack Blaster: Prostřednictvím této utility můžete svůj systém sledovat, a tak jej uchránit před nechtěnými změnami v konfiguraci Internet Exploreru. Zmiňovaný program sice provedení změn zabránit nedokáže, ale upozorňuje vás na ně a nabízí vám jejich nastavení do původního stavu.

Aby tato utilita běžela neustále na pozadí, musíte klepnout na nabídku *Settings/Startup minimized to system tray*. Pak zkopírujte zástupce *Browser Hijack Blaster (no splash)* z programové skupiny *Browser Hijack Blaster*, nacházející se v nabídce Start, do programové skupiny *Po spuštění*.

7) Windows XP: Zavřete jim všechny komunikační kanály

Problém: ***Obáváte se, že Windows XP sledují vaši činnost a posílají takové záznamy do internetu.***

Řešení: Pro uzavření všech komunikačních kanálů, jimiž může operační systém Windows XP zasílat do internetu data, můžete použít zdarma dostupnou utilitu **XP Antispy**, kterou naleznete NA NAŠEM CD.

Tipy: S utilitou XP Antispy ucpete Windows XP všechny otvory, kudy by mohla utíkat nějaká data. Obsluha programu je vskutku velmi jednoduchá. Po spuštění program zobrazí všechna aktuální nastavení Windows a červeným vykřičníkem ukáže ta, která se mu zdají podezřelá, a která by tudíž měla být deaktivována.

▲ **XP Antispy: Tento freewarový program se stará o to, aby Windows XP nekontrolovaně nezasílala data na server Microsoftu. Funkce, které se jeví pro takové odesílání dat jako vhodné a jsou tudíž nebezpečné, jsou označeny červeným vykřičníkem a měly by se vypnout**

Klepnutím na tlačítko *Použít nastavení* vypnete programem navržené a červeným vykřičníkem označené podezřelé funkce. Pokud chcete některou z nich přesto nechat aktivní, klepněte na ni myší tak, aby se vykřičník změnil na prázdný černý čtvereček.

Jaká podezření ze špionáže vlastně na Windows XP padají? Podezřelá data se údajně mohou posílat při odesílání zpráv o chybách při zatuhnutí programu, při odesílání informací o používání Windows Media Playeru, synchronizaci času přes internet a při automatickém vyhledávání updatů Windows (více viz tip č. 5).

Konkrétně má jít o zasílání informací o hardwarovém vybavení vašeho počítače.

8) Zabraňte tomu, aby internetové stránky monitorovaly vaši činnost na počítači

Problém: ***Chtěli byste zabránit tomu, aby nějaký provozovatel internetových stránek shromažďoval informace o vás či vašich aktivitách.***

Řešení: **Webwasher Classic 3.3** je aplikací, která se stane spojovacím článkem mezi internetovým prohlížečem a připojením k internetu a na základě vašich požadavků bude odfiltrovávat všechny prvky, jež mají nějaký sklon k monitorování vašich aktivit. Zmiňovaná utilita je k dispozici zdarma a naleznete ji i NA NAŠEM CD.

Tipy: Provozovatelé internetových stránek zaměřených na velkou nabídku služeb a zboží používají ty nejrozličnější způsoby, jak se co možná nejvíce dozvědět o návštěvnících svých WWW stránek. Tak kupříkladu každému návštěvníku přiřadí identifikační číslo, které si pak internetový prohlížeč uloží do souboru cookie. Při příští návštěvě vás pak webový server provozovatele na

ON-LINE minitipy

Internet Explorer

Panel Adresa

Skutečnost, jak mnoho mají společného Windows a Internet Explorer, ukazuje tento tip. Pokud máte ve Windows otevřeno okno s obsahem nějaké složky a v něm pak do panelu *Adresa* zadáte internetovou adresu, ukáže se vám zakrátko internetová stránka. Jestliže naopak v Internet Exploreru zadáte do panelu *Adresa* cestu k nějaké složce, zobrazí se vám za okamžik její obsah.

Elektronická pošta

Rychlejší práce s e-maily

Pro rychlé zaslání e-mailu stiskněte klávesovou zkratku <Win klávesa><R>. Do dialogového okna *Spustit* pak zadejte příkaz **mailto:** a za dvojtečku napište e-mailovou adresu příjemce. Stiskněte tlačítko *OK*. Spustí se vámi nastavený program, který používáte pro práci s elektronickou poštou, a vytvoří vám prázdné okno s již předvyplněnou adresou příjemce. Do něj stačí pouze dopsat předmět a vlastní text e-mailu.

Mozilla

E-mail místo prohlížeče

Jako internetový prohlížeč používáte Mozillu a jako program pro práci s elektronickou poštou program, který je součástí Mozilly. Chtěli byste pohodlným způsobem přímo spouštět pouze program pro práci s elektronickou poštou? Vytvořte si zástupce k souboru MOZILLA.EXE a umístěte jej kupříkladu na pracovní plochu nebo do nabídky Start. V kontextovém menu zástupce si klepněte na příkaz *Vlastnosti*. Na záložce *Zástupce* pak umístěte do políčka *Cíl:* za tam uvedený příkaz mezeru a následně parametr *-mail*. Takto upravený zástupce pak bude přímo spouštět pouze program pro práci s elektronickou poštou.

Internetový prohlížeč

Sem s obrázky!

Někdy zkouší autor internetových stránek znemožnit uložení obrázků přes pravé tlačítko myši. V tomto případě klepněte do menu *Zobrazit/Zdrojový kód* a podívejte se, zda se zde nacházejí nějaké adresy odkazující na obrázky. Adresy, jež začínají řetězcem *http*, pak můžete pomocí příkazů *Kopírovat* a *Vložit* umístit do panelu *Adresa* Internet Exploreru za poslední lomítko adresy, která je v tom okamžiku v panelu *Adresa* uvedena.

Internetový prohlížeč

Ušetřete poplatky za připojení

Jestliže si budete chtít nějakou internetovou stránku v klidu přečíst, určitě se vyplatí, pokud si v menu *Soubor* aktivujete položku *Pracovat offline*. Tím dojde k přerušení internetového připojení, čímž nějakou korunu ušetříte. Jakmile si klepnete na nějaký další odkaz, automaticky se objeví dialogové okno pro připojení k internetu.

Netscape/Mozilla

Klávesové zkratky pro ukončení aplikací

Jestliže končíte surfování na internetu přes Mozillu či Netscape a potřebujete rychle zavřít prohlížeč, nemusíte zavírat jednotlivá okna. Klávesová zkratka <Ctrl><Q> ukončí všechny instance včetně *Historie* a případných otevřených náhledů zdrojových kódů internetových stránek.

Elektronická pošta

Zpožděné doručení e-mailu

Technické problémy mohou e-mailový server ochromit na několik hodin, či dokonce dní – například pokud je server přetížen množstvím na něj došlých zpráv. Pokud jste poslali e-mail nějakému uživateli tohoto serveru, většinou obdržíte varovné hlášení (v angličtině), že jeho doručení bude zpožděno („delayed"). V tomto případě vy nemůžete dělat nic. Pokud později nedostanete informaci o tom, že se e-mail nepodařilo doručit, můžete vycházet z toho, že zpráva přece jen k adresátovi dorazila.

Internetový prohlížeč

Rušivé barvy

Ne všichni tvůrci internetových stránek mají při výběru barev pro svá díla šťastnou ruku. Někdy jsou barvy písma a pozadí tak nešťastně nastaveny, že rozluštění textu je téměř nemožné. Můžete si sice v Internet Exploreru přes nabídku *Nástroje/Možnosti Internetu* na záložce *Obecné* stiskem tlačítka *Usnadnění* nastavit, aby prohlížeč barvy ignoroval a používal standardní nastavení Windows. Vzhledem k tomu, že většinou vám vadí nastavení barev jen na několika stránkách a výše popisované řešení se uplatní pro všechny stránky, není to zrovna to pravé. Existuje však jedna velmi jednoduchá pomoc: Stačí si celou stránku označit pomocí klávesové zkratky <Ctrl><A>, a text se vám zobrazí v kontrastních barvách.

Důležité nástroje v boji proti spywaru

Program	Operační systém	Internetová adresa	Název a velikost souboru		Cena	Jazyk
Ad-Aware 6.181 SE	98/ME, NT4, 2000, XP	*www.lavasoft.de* a NA NAŠEM CD	AAW6.EXE (1,67 MB)		soukromé použití zdarma	český
Ad-Aware Language Pack	98/ME, NT4, 2000, XP	*www.lavasoft.de* a NA NAŠEM CD	AAW-LANG-PACK.EXE (342 KB)		soukromé použití zdarma	jazykový modul pro Ad-Aware
Browser Hijack Blaster 1.0	95/98/ME, NT4, 2000, XP	*http://ftp.pcworld.com/pub/new/privacy___security/firewalls/bhblaster setup.exe* a NA NAŠEM CD	BHBLASTERSETUP.EXE (393 KB)		zdarma	anglický
Outpost Firewall FREE 1.0	95/98/ME, NT4, 2000, XP	*www.agnitum.com* a NA NAŠEM CD	OUTPOSTINSTALL.EXE (2,49 MB)		zdarma	anglický
Outpost Firewall Pro 2.1	95/98/ME, NT4, 2000, XP	*www.agnitum.com* a NA NAŠEM CD	OUTPOSTPROINSTALL.EXE (7,82 MB)		zdarma	anglický
Pegasus Mail 4.12a	95/98/ME, NT4, 2000, XP	*www.pmail.com* a NA NAŠEM CD	W32-412A.EXE (4,23 MB)		zdarma	anglický
Spybot Search & Destroy 1.2	95/98/ME, NT4, 2000, XP	*www.safer-networking.org* a NA NAŠEM CD	SPYBOTSD12.EXE (3,51 MB)		zdarma	český
Startup Control Panel 2.8	95/98/ME, NT4, 2000, XP	*www.mlin.net* a NA NAŠEM CD	STARTUPCPL.ZIP (57,2 KB)		zdarma	anglický
Webwasher Classic 3.3	95/98/ME, NT4, 2000, XP	*www.webwasher.com/client/home* a NA NAŠEM CD	WASH33.EXE (1, 04 MB)		soukromé použití zdarma	anglický
XP Antispy 3.72	XP	*www.xpantispy.org** a NA NAŠEM CD	XPANTISPY_CZ.ZIP (32 KB)		zdarma	český
Zone Alarm 4.5.538.001	98 SE/ME, 2000, XP	*www.zonelabs.com* a NA NAŠEM CD	ZLSSETUP_45_538_001.EXE (4,77 MB)		soukromé použití zdarma	anglický

* **Pozor:** Internetové stránky **www.xpantispy.de** a **www.xp-antispy.de** obsahují dialer (program pro vytáčení čísel s drahým tarifem)!

▲ **Aplikace zabraňující vytvoření profilů obsahujících seznam vašich aktivit: Webwasher mimo jiné omezuje životnost souborů cookies na 24 hodin**

základě již existujícího cookie souboru znovu identifikuje. Během nějaké doby tak provozovatel internetových stránek získá jakýsi váš profil, v němž bude uvedeno, jak dlouho a kterou část on-line služeb jste využívali či na které reklamní banery jste klepli. Pokud jste na zmíněnou internetovou stránku nezadávali žádné osobní údaje, jste pořád pro provozovatele jenom číslo. Pokud jste se však zúčastnili nějaké hry či jste si něco objednali nebo jste se přihlásili k pravidelnému zasílání nějakých novinek či příspěvků, může provozovatel internetových stránek vaši osobu jednoznačně danému profilu přiřadit.

Webwasher v základní konfiguraci omezuje životnost všech souborů cookie na 24 hodin. Po uplynutí této doby je webový server už nebude moci načíst, čímž bude učiněna přítrž pokusům o vyhodnocování vašich aktivit po delší časové období.

Pokud spustíte Webwasher poprvé, objeví se vám dialogové okno týkající se konfigurace prohlížeče. Zde zvolte režim bez konfigurace. Ten totiž funguje velmi spolehlivě se všemi internetovými prohlížeči. Poklepáním na ikonu Webwasheru v pravé části Hlavního panelu se dostanete do možností konfigurace utility. Umístěte zde zatržítko před položku *Cookie Filter*. V pravé části okna pak můžete provádět podrobnější nastavení. Tady můžete kupříkladu zakázat přístup cookie z vámi zadaných internetových stránek.

Jakmile klepnete na odkaz, jenž vás přenese na internetovou stránku nabízející různé služby, předá internetový prohlížeč webovému serveru informaci o tom, ze které stránky jste se na tu jeho dostali. Pokud budete chtít zakázat posílání takových informací, umístěte zatržítko před volbu *Referrer Filter*. Webwasher dokáže ale fungovat i jako filtr reklamních banerů. Pokud byste si tuto funkci naopak nepřáli mít aktivovanou, deaktivujte položky *Dimension Filter* a *URL Filter*.

9) Sledujte, který program posílá data do internetu

Problém: ***Chtěli byste získat informaci o tom, který program zkouší do internetu posílat nějaká data. Zároveň byste chtěli znát i možnost, jak takovým aktivitám zabránit.***

Řešení: Nainstalujte si nějaký osobní firewall, který dokáže pracovat na úrovni aplikací, kupř. **Outpost Firewall Free**, jenž je k dispozici zdarma, či **Zone Alarm**, který je zdarma pouze pro soukromé použití. Oba najdete NA NAŠEM CD.

Tipy: Oba firewally chrání váš počítač nejen před útoky zvenku, nýbrž zabraňují také tomu, aby aplikace nainstalované na vašem počítači posílaly bez vašeho vědomí data do internetu. Pokaždé, když se nějaká aplikace pokusí o vámi neautorizovaný přístup do internetu, budete o této aktivitě informováni varovným hlášením. Na vás pak je rozhodnout, zda takovou komunikaci povolíte či zakážete, a to buď pouze pro tento případ, nebo nastálo.

Outpost: Velmi flexibilním programem se jeví být Outpost Firewall, v němž můžete pro každou aplikaci přiřadit několik pravidel. Tak můžete například pro nějakou aplikaci povolit přístup na internet, nikoliv však na internetovou stránku výrobce programu. Jakmile se vám objeví dialogové okno, v němž máte rozhodnout o povolení či zákazu přístupu na internet, nejprve vždy zkontrolujte, co se skrývá za tzv. *Remote Host*. Pokud je v ní uvedeno jméno výrobce programu, vyberte z kontextového menu příkaz *Create Rule using preset…* a tam položku *Other…* V následujícím dialogovém okně vytvořte pravidlo pro přístup k této doméně. Ty nejdůležitější údaje, jako je IP adresa serveru a ostatní kritéria, pak Outpost Firewall doplní automaticky. Vám pak zbývá pouze doplnit do pravidla příkaz, který se má vykonat – v tomto případě *Deny it*, a stisknout tlačítko *OK*.

Jakmile vaše aplikace bude chtít získat přístup k jiné internetové adrese, znovu se objeví dotaz od Outpostu, zda jí tento přístup dovolíte. Pokud budete chtít zmiňované aplikaci povolit přístup ke všem internetovým stránkám, až na výše popisovanou výjimku, postupujte analogicky jako v předchozím případě. V dialogovém okně *Rules* zrušte položky *Where the specified protocol is* a *Where the specified remote host is* a *Where the specified remote port is*. Umístěte zatržítko před volbu *Allow it* a klepněte na *OK*.

▶ **Startup Control Panel: Tato utilita vám ukazuje, které programy se automaticky spouští při startu Windows. Tyto položky můžete deaktivovat, smazat či upravit**

10) Znemožnění automatického spouštění adwaru a spywaru

Problém: ***Chtěli byste vědět, které programy se spouští při startu Windows. Pokud by se mezi nimi objevil nějaký, který patří mezi adware či spyware, chtěli byste jej odstranit.***

Řešení: Prostřednictvím freewarového programu **Startup Control Panel** uvidíte nejen to, které programy se spouští při startu Windows. Můžete také jednotlivé položky upravit či rovnou smazat. Utilitu samozřejmě najdete NA NAŠEM CD.

Tipy: Windows programátorům či uživatelům nabízejí několik míst, do nichž mohou umístit programy, jež se mají spouštět při startu systému. Takovým asi nejobvyklejším místem je složka *Po spuštění* v nabídce Start, kterou může každý rychle prověřit a případně pozměnit. Méně zkušeným uživatelům však zůstávají zcela skryty záznamy pro spuštění programů v registru. Ty lze najít v klíčích **Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Run** a **Hkey_Current_User\Software\Software\Microsoft\Windows\CurrentVersion\Run**. Ve Windows 95/98/ME se k těmto klíčům ještě přidává klíč **Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunServices**.

Startup Control Panel: Ten, kdo nechce manipulovat s Editorem registru, získá prostřednictvím této utility pohodlný přístup k seznamu všech položek, jež se spouští při startu Windows. Klepnutím pravým tlačítkem myši na položku a vybráním příkazu *Delete* takovou položku odstraníte. Všechny odstraněné záznamy pak utilita umisťuje do vlastního Koše, jehož obsah si můžete zobrazit přes záložku *Deleted*. Pokud nějakou položku smažete nedopatřením, můžete vše napravit právě zde. Při úpravě či mazání jednotlivých záznamů byste ale měli být maximálně obezřetní, a to i přesto, že utilita disponuje Košem, jehož použití jsme již popsali. Zejména při deaktivování některých položek, protože některé z nich patří k důležitým systémovým komponentám samotných Windows – kupříkladu programy DSENTRY.EXE či CTFMON.EXE. V případě pochybností můžete nahlédnout na internetovou stránku **www.reger24.de/prozesse.html**, kde se můžete přesvědčit o tom, zda se nejedná zrovna o nějakou důležitou část vašeho operačního systému.

Za zmínku stojí i skutečnost, že můžete u jednotlivých položek upravovat jejich názvy či parametry. Klepněte v tomto případě na záznam pravým tlačítkem myši a z kontextového menu zvolte příkaz *Edit*. 4 0230/OK ❑

ON-LINE minitipy

Elektronická pošta

Delivery Failure

Pokud se v předmětu zprávy objeví výraz *Delivery Failure*, nemusí se vždy jednat o pokus o odeslání e-mailu na neexistující nebo chybně napsanou adresu. Často se jedná o trik spammerů. Reklama se v tomto případě objevuje ve zdánlivě vráceném e-mailu.

Internetový prohlížeč

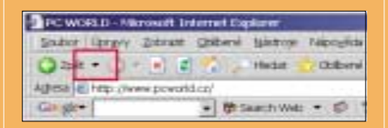
Rychlejší spuštění Mozilly

Podobně jako u Internet Exploreru můžete i Mozillu nahrát do paměti při spuštění Windows. Pak se dá spouštět stejně rychle jako Internet Explorer. Popisovanou funkci si zpřístupníte v menu *Úpravy/Předvolby* klepnutím na položku *Rozšířené nastavení*. Tam zatrhněte volbu *Ponechat Mozillu v paměti pro zrychlení při spuštění*.

Internetový prohlížeč

Klepnutí na tlačítko Zpět

U některých internetových stránek tlačítko *Zpět* internetového prohlížeče jednoduše nefunguje. Buď je šedé, tzn. neaktivní, anebo jeho stisk vyvolá stejnou stránku, kterou máte právě zobrazenou. To je k zlosti zejména v případech, pokud se chcete vrátit na stránku s výsledky vyhledávání nějakého výrazu, kde máte ještě další odkazy, jež si chcete prohlížet. Přesto existuje způsob, jak se na dříve prohlížené stránky přemístit. Klepněte na malou šipku nacházející se vedle tlačítka *Zpět*. Ukáže se vám chronologicky uspořádaný seznam všech naposledy navštívených stránek. Klepnutí na libovolnou položku vás pak přenese na požadovanou stránku.



Ping

Otestování připojení

Systémová utilitka Ping vám pomůže při rozboru problémů s internetovým připojením. Můžete na příklad na příkazový řádek zadat příkaz:

ping www.pcworld.cz

Ping pak zasílá dotazy na zadanou adresu a ukazuje dobu pro vyřízení odpovědi. Pokud se vyskytnou při připojení problémy, vydá patřičné chybové hlášení.

Pegasus Mail

Minimalizace a maximalizace

Pokud zmíněný program pro práci s poštou zminimalizujete, pak kompletně zmizí i z Hlavního panelu, a místo toho se vytvoří malá ikonka v pravé části Hlavního panelu. Klepnutí na ni způsobí opět otevření okna programu. Pokud ale pracovní plochu překrývají okna jiných aplikací, otevře se Pegasus Mail neviditelně na pozadí. V tomto případě je třeba použít klávesovou zkratku <Alt><Tab>, kterou si vyberete ikonku Pegasus Mailu, a aplikaci přenesete do popředí.

Internet Explorer 6

Přesunutí panelu nástrojů

Standardně není změna umístění panelů nástrojů v Internet Exploreru možná. Jde to pouze v případě, kdy si v menu *Zobrazit/Panely nástrojů* deaktivujete položku Uzamknout panely nástrojů. Provedené nastavení se projeví při dalším spuštění Internet Exploreru.

Traceroute

Sledování paketů

Chcete vědět, jakou cestou putují data od vás k nějakému určitému internetovému serveru? Zadejte na příkazový řádek příkaz:

tracert <jméno serveru>

Získáte seznam všech míst, přes která pakety prošly.

Elektronická pošta

Rychlý přístup do poštovní schránky Outlook Expressu

Outlook Express se spustí daleko rychleji a zároveň ušetříte jedno klepnutí myší, pokud zakážete zobrazování uvítací zprávy. V menu *Nástroje/Možnosti* na kartě *Obecné* proto povolte položku *Po spuštění přepnout do složky Doručená pošta*.

Ipconfig

Informace o připojení

Aktuální informace o vašem síťovém připojení získáte ve Windows 2000/XP tak, že na příkazový řádek zadáte příkaz **ipconfig**. Podrobnější informace, jako například IP adresu DHCP serveru nebo serveru DNS, pak získáte zadáním příkazu **ipconfig/all**.