Zahlaďte po sobě stopy!

Každý nemusí hned vědět, co na svém počítači děláte (CD)

DAVID ČEPIČKA, DANIEL BEHRENS

Váš počítač o vás může prozradit mnohé. Ostatní si tak mohou velmi rychle udělat obrázek o vaší práci a dokonce i o vašich zvyklostech. Učiňte přítrž všem zvědavcům slídícím po vašem soukromí!

Ukaž mi svůj počítač a já ti povím, kdo jsi. To není žádná přemoudřelá průpovídka, ale hořká skutečnost. Prakticky každý program, jenž běžně používáte, totiž sbírá informace o vašich aktivitách.

Údaje skryté v dokumentech Wordu

Například Word: stačí otevřít dokument Wordu a z menu *Soubor* vybrat příkaz *Vlastnosti*. A už zde jsou uvedeny (bez vašeho vědomí) informace o vaší osobě a o právě vznikajícím dokumentu. Díky takovým funkcím Wordu, jako jsou *Rychlé ukládání* či *Sledování změn*, se rovněž může stát, že se z nějakého dokumentu mohou načíst takové informace, které by ostatní raději neměli vůbec spatřit.

Zkusili jsme provést malý ukázkový test. Při něm jsme na internetu vyhledávali dokumenty vytvořené ve formátu dokument Word. Velmi pohodlně to jde pomocí vyhledávače Google. Do políčka *Pokročilé vyhledávání* jsme zadali formát souborů Microsoft Word (**.doc*) a do políčka pro zadání vyhledávaného výrazu jsme zadali nějaké běžně používané slovo. A hned se objevily tisíce dokumentů roztroušených po celém webu. A už při prvních pokusech se nám podařilo v některých z nich odhalit utajené informace, o nichž s největší pravděpodobností jejich autoři vůbec nevěděli.

Proto každý, kdo chce dokumenty ve Wordu posílat dále třeba přes e-mail či je vkládat přímo na WWW stránky, by je měl ze všeho nejdříve podrobit důkladné prohlídce. V tipu č. 1 se dozvíte podrobnosti. Mimo jiné poznáte i přesná místa, kde se takové skryté informace v dokumentu Wordu nalézají.

Ostatní uživatelé vědí, kde surfujete na internetu

Každý, kdo se o svůj počítač dělí s jinými osobami, ať to jsou členové rodiny či kolegové v práci, dává všanc kousek svého soukromí. Kupříkladu spousta programů si pečlivě poznamenává naposledy otevřené soubory (viz tip č. 7). Ostatní si zase uchovávají informace o tom, které stránky na internetu navštěvujete. Hlavními podezřelými v této nekalé činnosti jsou zejména funkce *Historie* v Internet Exploreru a také mezipaměť (cache paměť internetového prohlížeče). V tipu č. 3 se tak dozvíte, kam se přesně umisťují záznamy o navštívených stránkách a jak tyto informace odstranit.

Pornografické materiály a hesla na pevných discích

Máte-li v úmyslu prodat nebo darovat svůj pevný disk či rovnou celý počítač, pak byste určitě měli důkladně vymazat všechen jeho obsah. K tomuto účelu je funkce pro mazání souborů ve Windows stejně tak málo vhodná jako formátování disku či nové vytvoření diskových oddílů. Dokonce už i prostřednictvím freewarových utilit (viz tip č. 6) se dají taková data poměrně snadno obnovit.

Většina uživatelů to však očividně neví. Firma O&O Software (**www.oo-software.com/en/study/index.html**), zabývající se vytvářením nejrůznějších utilit, zkusila provést namátkový test u několika pevných disků, které prodávala v dražbě firma Ebay. Cílem tohoto testu byla snaha najít na těchto discích citlivé údaje. Výsledkem pak bylo množství soukromých či obchodních e-mailů, naskenované podpisy, plné moci k provádění bankovních operací, údaje pro přístup k internetu, hesla pro přístup k službám online bankovnictví včetně kódů transakcí, stejně jako pornografický materiál. Tato data buď vůbec nebyla smazána, nebo se dala za použití speciálního softwaru obnovit. Aby se vám nic takového nepřihodilo, nabízíme vám v tomto článku programy, s nimiž skutečně důkladně odstraníte jednotlivé soubory, ale samozřejmě pro ně nebude problém nenávratně promazat celé disky.

1) Jak nalézt a odstranit informace skryté v dokumentech vytvořených ve Wordu

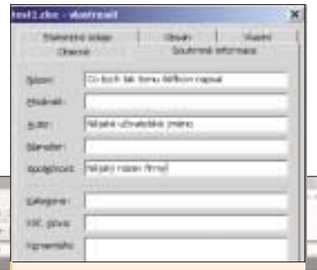
Otázka: ***Často posílám e-mailem dokumenty vytvořené ve Wordu, a to jak služební, tak soukromé. Představuje to pro mne bezpečnostní riziko?***

Odpověď: Zasílání takových dokumentů je z hlediska bezpečnosti riskantní. Dokumenty vytvořené ve Wordu jsou ve formátu obsahujícím čistý text (nezašifrovaný), čímž je jejich obsah přístupný všem, tedy i nepovolaným. Některé informace se dají získat poměrně snadno – například přes menu *Soubor/Vlastnosti*. Na záložce *Souhrnné informace* je kupříkladu uvedeno, kdo dokument vytvořil a v jaké společnosti pracuje.

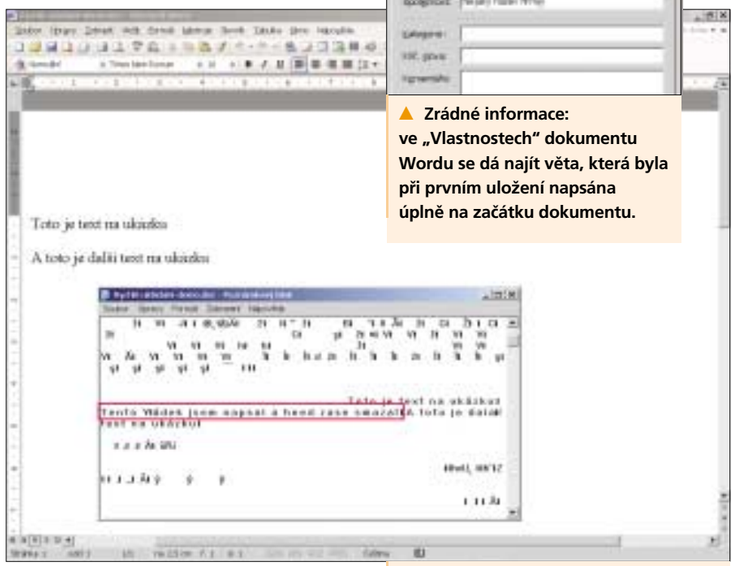
Tyto údaje vkládá Word automaticky do každého dokumentu. Jméno uživatele a název společnosti získává program z údajů, jež byly zadávány při instalaci Wordu, resp. celého balíku Office. Pokud jste tehdy při instalaci v rozčilení zadali nějaká nesmyslná či hloupá slova, jako „Blbeček" do políčka pro vaše jméno a „Kocourkov" jako název vaší firmy, pak to může být docela trapné, protože tato slova budou obsahovat všechny dokumenty Wordu, které jste vytvořili nebo nějak dále na počítači upravovali.

Do řádku *Název* vkládá Word větu, která je při prvním ukládání dokumentu úplně na začátku textu. Zmíněná věta pak zůstane v tomto políčku i tehdy, když bude z původního textu dávno odstraněna. Ostatně si popisovanou větu můžete přečíst i tehdy, pokud v Průzkumníku přesunete ukazatel myši nad daný soubor.

Záložka *Statistické údaje* vynáší na světlo další údaje. Tak se kupříkladu dozvíte, který uživatel soubor naposledy ukládal. Pokud je zde uvedeno jiné jméno než na záložce *Statistické údaje*, je jasné, že na dokumentu pracovali minimálně dva uživatelé. Údaj *Číslo revize* vám udává, jak často byl dokument modifikován a kolikrát byl uložen. Pokud byl dokument i vytištěn, pak přesné údaje o tisku prozradí řádek *Vytištěno:*. Pakliže je ve Wordu aktivována možnost tzv. *Rychlého ukládání*, může se v souborech nalézat kvantum dalších zajímavých informací. V tomto případě totiž Word neukládá vždy znovu celý soubor, nýbrž připojuje k souboru pouze nově přidané znaky. Tuto činnost pak provádí automaticky na pozadí bez zásahu uživatele. Části textu, které odstraníte, tak Word označí jako odstraněné, přesto v textu nadále zůstávají. Pomocí textového editoru, jenž dokáže dokument vytvořený ve Wordu zobrazit v „hrubé" formě bez formátování, například v libovolném textovém editoru dodávaném ve Windows, pak můžete odstraněné části textu znovu vidět.



▲ **Zrádné informace: ve „Vlastnostech" dokumentu Wordu se dá najít věta, která byla při prvním uložení napsána úplně na začátku dokumentu.**



▲ **Riziko „Rychlého ukládání": pokud je tato volba povolena, zůstávají již smazané části textu v dokumentu. Zobrazit si je pak může kdokoli otevřením souboru v libovolném textovém editoru.**

▲ Vyčistěte dokument dokonale: Doc Scrubber zobrazí všechny skryté informace v dokumentech Wordu a pokud si to budete přát, rovněž je smaže.

Tato skutečnost ale může mít dalekosáhlé důsledky. Například se takto může zjistit, že si nějaký uživatel v dokumentu obsahujícím nějakou hodnotící zprávu trochu pozvedl svoji bilanci tím, že údaje uvedené ve zprávě vylepšil ve svůj prospěch a odstranil všechny kritické poznámky v dokumentu. Nebo další příklad: co když budete chtít poslat svým kolegům dokument, který jste trochu zcenzurovali, aby v se něm nevyskytovala skutečná jména aktérů? I v tomto případě nebude problém pro trochu zvídavějšího uživatele skutečná jména (vámi odstraněná) odhalit. Je pravdou, že hledání smazaných údajů v DOC souboru otevřeném v „hrubé" neformátované formě je poněkud zdlouhavější, ovšem v případě podezření na nějakou nekalost se může takto vynaložená námaha vrátit.

To samé platí i o funkci *Sledování změn* – jedná se původně o velmi užitečnou funkci, zejména tehdy, pokud na jednom dokumentu pracuje více lidí. Každý z nich totiž hned vidí, co jeho kolega provedl v dokumentu za změny a doplňky či naopak které pasáže z dokumentu vyškrtl. Ale pozor: dříve, než se dokument dostane na veřejnost, nesmí poslední uživatel dokumentu zapomenout vytvořenou historii provedených změn smazat (viz níže). Jinak by si mohl příjemce nějakého marketingového dokumentu docela slušně počíst v komentářích odkazujících na množství prodaných produktů. Proto je nutné pro odstranění všech nepatřičných informací klepnout na nabídku *Nástroje/Sledování změn*, a když se objeví nový panel nástrojů, pak z rozevírací nabídky vybrat položku *Konečný se značkami*.

Některé verze Wordu si navíc poznamenávají, pod jakými názvy a do jakých složek jste jednotlivé verze dokumentu ukládali. Z těchto údajů se dá také odvodit mnohé – co si pomyslíte, když jako první název dokumentu uvidíte název *Nudný marketingový text.doc* a když bude ležet ve složce *Problémové případy*?

Utilita **Doc Scrubber**, jež je pro soukromé použití zdarma, takové soubory Wordu analyzuje a ukáže vám údaje, které se dají zjistit, pokud někdo otevře dokument Wordu a z menu *Soubor* zvolí příkaz *Vlastnosti*. Rovněž poskytne řadu dalších informací – kupříkladu historii všech názvů souborů a verzi Wordu, v níž autor dokumentu pracoval.

Způsob ochrany

Pokud můžete ve Wordu některé jeho funkce bez problémů postrádat, existuje jednoduché řešení – budete-li dokument dále předávat ostatním ve formátu RTF, pak všechny výše popisované a utajované informace zmizí, až na jméno uživatele a název společnosti.

Pakliže pro své dokumenty upřednostňujete formát dokument Word, pak si nezapomeňte vždy zkontrolovat, zda vaše soubory neobsahují některé z údajů, které nechcete zveřejňovat a popřípadě je neváhejte smazat.

Další níže uvedené tipy se týkají Wordu 2003. V ostatních verzích Wordu jsou příkazy obdobné.

Nejprve otevřete soubor Wordu a z menu *Soubor* si zvolte příkaz *Vlastnosti*. Nyní klepněte na záložku *Souhrnné informace* a zde odstraňte všechny údaje ze všech políček. Kromě toho před posledním uložením souboru zrušte zatržení políčka *Povolit rychlé ukládání* v menu *Nástroje/Možnosti* na záložce *Ukládání*. V opačném případě zůstanou smazané části textu obsaženy v dokumentu a dají se dohledat při otevření souboru v nějakém jiném textovém editoru.

Utilita **Doc Scrubber**, kterou naleznete NA NAŠEM CD, dokáže nejen zobrazit skryté informace obsažené v dokumentech Wordu, nýbrž je i odstraní. K tomuto účelu spusťte Doc Scrubber a stiskněte tlačítko *Scrub*. V dalším kroku si určujete, zda chcete „vyčistit" pouze jeden dokument Wordu nebo více. Nezapomeňte zatrhnout volbu *Save scrubbed file over original*. V opačném případě totiž Doc Scrubber vytvoří vyčištěnou kopii souboru, jež bude v názvu souboru obsahovat výraz SCRUBBED, a původní soubor nechá nedotčený. Klepněte na tlačítko *Next*. Nyní máte možnost vybrat si libovolný soubor Wordu, popřípadě složku tyto soubory obsahující.

V dalším dialogovém okně pak určujete, které informace má utilita ze souborů Wordu odstranit – kupříkladu datum vytištění, číslo revize dokumentu, celkovou dobu práce na dokumentu či historie jmen souborů. Po klepnutí na tlačítko *Next* pak začne program soubor Wordu čistit.

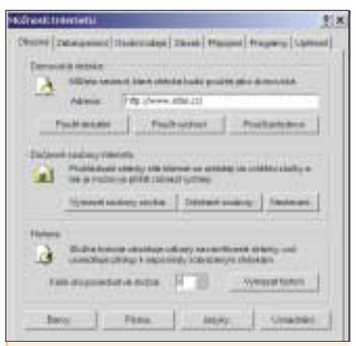
Historii úprav zaznamenanou pomocí funkce *Sledování změn* však Doc Scrubber odstranit nedokáže. Pro jejich smazání nejprve zmiňovanou funkci zapněte, a to přes menu *Nástroje/Sledování změn* (pokud ovšem již nebyla zapnutá). Objeví se nový panel nástrojů. V rozevíracím seznamu vyberte položku *Konečný se značkami*, abyste zobrazili historii všech úprav provedených v dokumentu. Tu pak smažete příkazem *Přijmout* všechny změny v dokumentu.

Pokud používáte Word XP nebo 2003, můžete rovněž použít zdarma dostupný nástroj Microsoftu s názvem **Remove Hidden Data Add-in** (naleznete jej NA NAŠEM CD). Ten dokáže odstranit veškerou historii úprav a odstraní všechny údaje, jež se nacházejí na záložce *Souhrnné informace*, kterou vyvoláte pro každý soubor z menu *Soubor/Vlastnosti*. Po instalaci doplňku jej můžete spustit z menu *Soubor/Remove Hidden Data*. Velmi nepraktická je ale skutečnost, že po vyčištění nějakého dokumentu se vás příště při jeho novém otevření Word bude dotazovat, zda jej chcete otevřít pouze pro čtení.

Číslo revize dokumentu a datum vytištění zůstává po vyčištění zmiňovaným doplňkem zachováno. Tyto údaje můžete následně odstranit programem Doc Scrubber.

2) Stopy po surfování: Které stránky si prohlíželi za mými zády a kdo?

Otázka: ***Jak mohu zjistit, zda někdo během mé nepřítomnosti nebrouzdal na mém počítači na internetu a jaké stránky si prohlížel?***



▲ Konec sledování: funkci Historie můžete nastavit tak, aby zaznamenávala a uchovávala navštěvované stránky na internetu pouze jeden den.

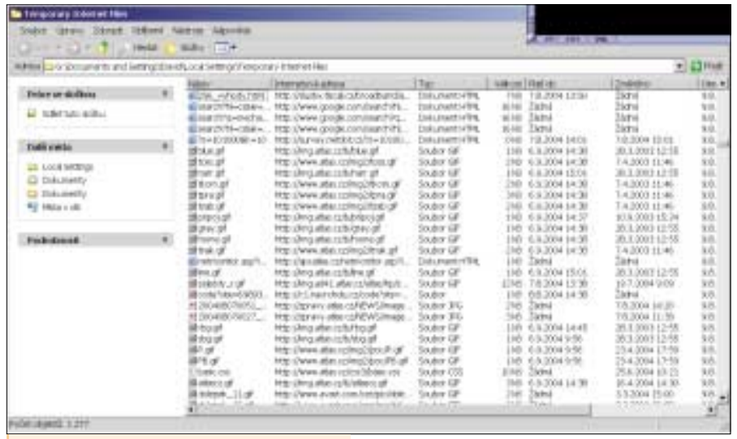
Odpověď: Internet Explorer si poctivě vede knihu záznamů o tom, kdy a které internetové stránky jste navštívili. Tak si kupříkladu můžete připomenout, jak se jmenovala stránka, kterou jste předevčírem otevřeli a mezitím jste její přesnou adresu zapomněli.

Stejně tak můžete snadno zjistit, které stránky má v oblibě váš syn či dcera. Pro zobrazení souboru těchto záznamů, v Internet Exploreru zvaných *Historie*, stačí klepnout do menu *Zobrazit/Panel aplikace Explorer/Historie*, nebo použít tlačítko se symbolem hodin na panelu nástrojů. Objeví se postranní lišta s jednotlivými dny v týdnu. Po klepnutí na libovolný den se pak ukáže seznam všech webových serverů navštívených v onen den. Klepnutím na název domény serveru se pak zobrazí všechny stránky otevřené na tomto serveru. Pokud budete chtít zjistit, kolikrát byla daná stránka navštívena a kdy byla naposledy otevřena, pak klepněte na danou stránku pravým tlačítkem myši a z kontextového menu zvolte příkaz *Vlastnosti*. Nad seznamem se také nachází tlačítko *Hledat*, s jehož pomocí můžete aktivovat u navštívených stránek vyhledávání podle klíčových slov vyskytujících se v URL adrese či v názvu v titulkovém pruhu okna.

S funkcí *Historie* je spojena funkce automatického doplňování adres. Když do řádku *Adresa* postupně píšete internetovou adresu, ukazuje Internet Explorer všechny již navštívené adresy obsahující stejné znaky. Pomocí kurzorových šipek si pak můžete vybírat v seznamu adres, čímž si ušetříte psaní celé adresy. Objeví-li se v seznamu adres nějaká, kterou neznáte, pak ji na vašem počítači otevíral někdo jiný.

Další stopy po surfování někoho jiného se dají najít v mezipaměti (cache) prohlížeče. Internet Explorer totiž na pevný disk ukládá obsah navštívených stránek (výjimkou jsou zabezpečené stránky *https*).

Pokud jste nic neměnili, nemusíte při příští návštěvě nějaké stránky tuto celou znovu stahovat. Cache paměť prohlížeče zabírá okolo tří procent kapacity disku, na němž jsou nainstalována Windows. U velkých disků tak může kapacita mezipaměti dosahovat i několika gigabajtů. Díky tomu není nic složitého zjistit stránky navštěvované i před delší dobou. Pokud v prohlížeči klepnete do menu *Nástroje/Možnosti Internetu* a přesunete se na záložku *Obecné*, kde stisknete tlačítko *Nastavení*, dostanete se do dialogového okna, v němž si stiskem tlačítka *Zobrazit soubory* zobrazíte obsah složky **Temporary Internet Files**, která je mezipamětí prohlížeče. Nyní klepněte v okně složky **Temporary Internet Files** do menu *Zobrazit/Podrobnosti*. Ke každému prvku se vám zobrazí internetová adresa, z níž pochází, a datum otevření, což je datum, kdy byla tato adresa naposledy prohlížena.



▲ Internet Explorer ukládá v paměti cache všechny prvky naposledy navštívených WWW stránek – jejich seznam si můžete setřídit třeba podle stránek, k nimž patří.

Když klepnete na záhlaví sloupce s názvem *Internetová adresa*, seřadíte všechny prvky podle URL adres. Při klepnutí na záhlaví sloupce *Otevřeno* setřídíte seznam podle data otevření, takže okamžitě vidíte, kdy byly které internetové stránky otevřeny. Při poklepání na libovolný prvek, třeba obrázek, se tento otevře, aniž by bylo nutné být připojen k internetu.

V seznamu dočasných souborů se rovněž v mezipaměti nacházejí tzv. cookies. Jsou to speciální textové soubory, jež WWW servery posílají na váš počítač, na němž se pak ukládají. Mohou například obsahovat jedinečné číslo, na něž může WWW server při vaší další návštěvě odkazovat. Tak si mohou provozovatelé WWW serveru vést poměrně přesnou statistiku návštěvnosti svých stránek a třeba v případě internetového obchodu mohou zobrazit obsah vašeho nákupního košíku při vašem posledním nákupu.

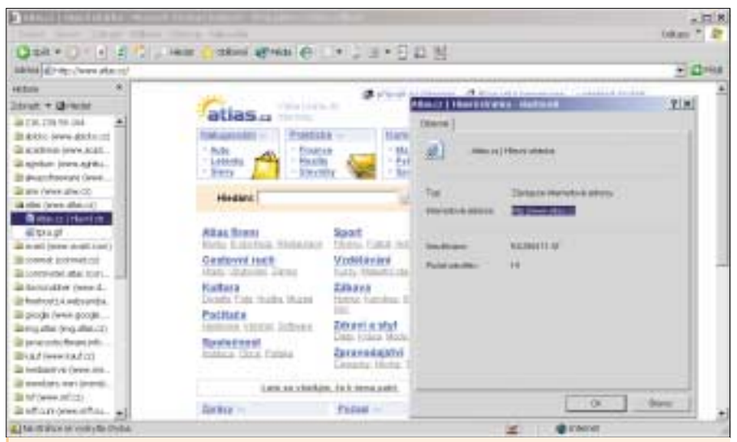
Na rozdíl od dočasných souborů internetu nemají cookies žádná omezení týkající se kapacity, která je pro ně vyhrazena – proto jsou na vašem počítače vlastně trvale. Podíváte-li se na obsah cookies, nenaleznete nic příliš zajímavého, jen několik číslic a změť písmen. V seznamu dočasných souborů se ale cookies zobrazují s internetovou adresou, z níž pochází, a s datem posledního přístupu k serveru. Takže i kdyby byla cache paměť prohlížeče smazána, můžete díky cookies přesto získat informace o tom, zda někdo jiný na vašem počítači surfoval na internetu. Ovšem je zároveň třeba poznamenat, že cookies ukládají na váš počítač pouze některé stránky.

Způsob ochrany

Principiálně jsou pro nás zajímavé pouze stopy, které při surfování zanechá Internet Explorer. Pomocí funkce *Historie* naleznete zapomenuté stránky, mezipaměť vám zase poslouží k rychlejšímu načítání již navštívených internetových stránek. Pokud počítač používáte sami a nikdo jiný k němu nemá přístup, pak si nemusíte kvůli ochraně dat dělat žádné starosti.

Jakmile svůj počítač sdílíte s ostatními kolegy v práci nebo doma se členy rodiny, pak je nutno provést několik opatření, aby se nikdo nepovolaný k vašim datům nedostal. Ve Windows 2000 a XP zřiďte několik uživatelských účtů. Pro každého uživatele se pak budou cache paměť Internet Exploreru, cookies a stránky pro funkci *Historie* ukládat do speciální složky. Výše napsané ale platí pouze tehdy, pokud budete používat systém souborů NTFS a nikdo jiný kromě vás nebude mít k počítači práva správce počítače. V opačném případě může každý takový uživatel pomocí Průzkumníka prohlížet složky ostatních uživatelů.

Jiný způsob: všechny stopy za sebou vždy zametete, neboli nakonfigurujte Internet Explorer tak, aby ukládal pokud možno co nejméně dat.



▲ Internet Explorer vás prozradí: pomocí funkce Historie si prohlížeč zaznamenává, kdy a které WWW stránky jste navštívili.

Začněme třeba seznamem všech navštívených stránek. Klepněte v Internet Exploreru do menu *Nástroje/Možnosti Internetu*. Na záložce *Obecné* je dole nastaveno, kolik dní mají být adresy uloženy v *Historii*. Tuto hodnotu nastavte na nulu. Funkce *Historie* sice nebude úplně vypnuta, ale budou ukládány pouze adresy, které jste navštívili během jednoho dne surfování na internetu. Pokud sázíte na jistotu, pak po každém surfování klepněte na výše popsanou záložku *Obecné* a stiskněte tam tlačítko *Vymazat historii*. Na stejné záložce najdete tlačítko *Odstranit soubory*, jímž vymažete obsah cache paměti prohlížeče. Aby v budoucnu Internet Explorer do mezipaměti ukládal co nejméně souborů, nastavíme velikost cache paměti na 1 MB, a to stiskem tlačítka *Nastavení* na stejné záložce. Hodnotu 0 MB bohužel Internet Explorer neakceptuje.

Určitě pohodlnější je, když se smaže obsah *Historie*, mezipaměti a cokies jedním stiskem tlačítka myši. K tomu slouží utilita **Ii System Wiper**, kterou popíšeme v tipu č.7.

3) Ukrytí stop po surfování na zašifrovaném disku

Otázka: ***Chtěl bych surfovat na internetu, aniž bych po sobě zanechal nějaké stopy, které by byly viditelné pro ostatní uživatele mého počítače. Ovšem nechtěl bych postrádat žádnou z komfortních funkcí, jako jsou oblíbené odkazy, historie, automatické doplňování internetových adres a používání mezipaměti prohlížeče. Jde to nějak zařídit?***

Odpověď: Zřiďte si virtuální zašifrovaný disk, na který budete mít po zadání hesla přístup pouze vy. K tomuto účelu se dá kupříkladu ve Windows 2000 a XP použít zdarma dostupná německá utilita **Global Safe Disk AES**, kterou naleznete NA NAŠEM CD.

V případě Internet Exploreru je však poněkud komplikovanější provést nastavení tak, aby se všechny stopy po surfování na internetu nacházely na zašifrovaném disku, neboť informace, které jsou součástí funkce *Historie*, cookies apod. jsou ukryty hluboko v registru.

Způsob ochrany

Zkuste proto použít zdarma dostupný internetový prohlížeč **Firefox**, který naleznete i NA NAŠEM CD. Firefox je založen na prohlížeči Mozilla, je však oproštěn od všech k obyčejnému surfování nepotřebných komponent, takže postrádá např. funkce pro práci s elektronickou poštou nebo pro chat. Díky tomu je ve srovnání s Mozillou rychlejší.

Aby Firefox ukládal svoje data na zašifrovaný disk, klepněte v nabídce *Start* na položku **Mozilla Firefox** a tam na zástupce **Profile Manager**. V něm smažte existující profil a vytvořte nový. Potom zadejte jako disk pro umístění složky pro data uživatele písmenko zašifrované diskové jednotky.

4) Outlook Express: smazané e-maily se ještě dají obnovit

Otázka: ***Dají se v Outlook Expressu smazané e-maily ještě nějakým způsobem obnovit, nebo jsou nenávratně ztraceny?***

Odpověď: E-maily, které odstraňujete, se standardně umisťují nejprve do složky *Odstraněná pošta*. Tam je lze i nadále prohlížet, přesunout do jiné složky nebo smazat – ovšem ani pak nejsou nenávratně pryč. V Outlook Expressu se sice již nezobrazují, přesto se dají znovu obnovit. Všechny e-maily v dané složce Outlook Expressu (*Doručená pošta*, *Odstraněná pošta* atd.) jsou uloženy v jednom souboru se jménem **<název složky>.DBX**. Z důvodu větší rychlosti Outlook Express odstraněné e-maily v DBX souboru pouze označí jako smazané, místo aby po každém smazání e-mailu vytvářel nový soubor DBX. Takže jak v DBX souboru s názvem odpovídajícím původnímu umístění smazaného e-mailu, tak i v souboru pro složku *Odstraněná pošta* jsou všechny zprávy stále obsaženy a lze je otevřením DBX souboru v libovolném textovém editoru přečíst.

Umístění souborů s poštou ve vašem počítači zjistíte přímo v Outlook Expressu, pokud klepnete do menu *Nástroje/Možnosti* a na záložce *Údržba* klepnete na tlačítko *Složka úložiště* a v dalším dialogovém okně stisknete tlačítko *Změnit*. Poznačte si cestu ke složce a zavřete všechna dialogová okna stiskem tlačítek *Storno*. Ve Windows 2000 a XP je tato složka skrytá, takže abyste k ní získali přístup, musíte nejprve v Průzkumníku v menu *Nástroje/Možnosti složky* na záložce *Zobrazení* povolit položku *Zobrazovat skryté soubory a složky*.

Způsob ochrany

Abyste smazané e-maily skutečně navždy odstranili, smažte všechny položky ve složce *Odstraněná pošta* a následně klepněte do menu *Soubor/Složka/Zkomprimovat všechny složky*. Tím dosáhnete toho, že se všechny soubory obsahující e- maily vytvoří znovu a všechny e-maily označené jako smazané konečně zmizí.

Profesionální slídiči po datech

V situacích, kdy se jedná o počítačovou kriminalitu, přichází ke slovu vskutku profesionální utility. Stanovení postihu v této oblasti je založeno na využití speciálního softwaru vyvinutého pro získání důkazů a objasnění trestných činů. Jedním ze zástupců programů tohoto druhu je **Encase**, který je nasazován jak vnitrostátně, tak mezinárodně příslušnými úřady. Takovým softwarem se však vybavuje rovněž stále více a více firem, a to proto, aby odhalilo nekalé úmysly svých neloajálních zaměstnanců.

Pomocí Encase se tak kupříkladu dá vytvořit obraz pevného disku pozůstalé osoby. Tento obraz je tak přesný, že obsahuje dokonce i zdánlivě prázdné sektory, obsahující již smazané soubory. Nakonec se opatří ochranou proti zápisu, aby se vyloučily možné další manipulace.

Jakmile je obraz disku vytvořen, lze ho pomocí Encase velmi podrobně analyzovat. Software například dokáže najít všechny obrázky a zobrazit je jako miniatury. Zdánlivě nebo omylem špatně nastavené přípony souborů Encase nijak nevyvedou z míry, neboť utilita vždy analyzuje hlavičku každého souboru.

Otázkou několika sekund je vyhledání e-mailů – například kdy a komu byly zaslány e-maily obsahující určitou přílohu. Soubory smazané před krátkou dobou se zpravidla dají bez problémů obnovit. V mnoha zemích jsou důkazy v digitální formě vytvořené nástrojem Encase soudy zpravidla bez výhrad uznávány.

Pro firmy existuje speciální verze nástroje Encase, která dokáže vytvářet obraz disku za běžného provozu či umožňuje některé pracovníky nepozorovaně sledovat. Tak se dají třeba odhalit někteří spolupracovníci, kteří si ve svůj poslední pracovní den před propuštěním ze zaměstnání ještě narychlo kopírují tajná firemní data na svůj soukromý USB disk.

Například v Německu Encase prodává firma **Ontrack** (**www.ontrack.de/encase**). Cenu aplikace pro firmy lze zjistit na internetových stránkách výrobce **www.guidancesoftware.com**. Dalším poskytovatelem softwaru pro poskytování materiálů k soudnímu řízení je například firma **Vogon** (**www.vogon-forensic- hardware.com/forensic-systems.php**).

5) Riziko: uložená hesla je možné zjistit prostřednictvím freewarových utilit!

Otázka: **Windows na několika místech nabízejí uložení zadávaných hesel. Naneštěstí jsem ztratil přehled o tom, jaká hesla jsem do jednotlivých instancí zadal. Dají se tato hesla nějak zjistit?**

Odpověď: Prostřednictvím utility **Protected Storage Passview**, kterou najdete NA NAŠEM CD, si přehled jistě udržíte. Ukáže vám všechna uživatelem zadaná data u všech poštovních schránek zadaných v Outlooku nebo v Outlook Expressu. Dále zobrazuje všechna hesla, jimiž se přihlašujete na určitých WWW stránkách a která máte uložena v Internet Exploreru. Utilita s vámi dokáže komunikovat i v češtině, pokud si do ní doinstalujete český jazykový modul, který rovněž naleznete NA NAŠEM CD. Instalace se provede rozbalením archivu a přesunutím souboru PSPV_LNG.INI do složky, v níž máte utilitu nainstalovanou.

Ve Windows 95/98/ME ale utilita ukazuje pouze ta hesla, která jste právě napsali do příslušného formuláře na internetové stránce. Data, jež uživatel zadá do zvláštních dialogových oken, zviditelníte prostřednictvím utility **Win9x Passview**, kterou rovněž naleznete NA NAŠEM CD. To, která z výše uvedených metod se použije pro přihlašování k internetovým službám, závisí právě na samotné internetové službě.

Hesla uložená v aplikaci *Telefonické připojení sítě*, například pro vytáčené připojení k internetu, pomůže odhalit zdarma dostupná utilita **Dialupass**, kterou najdete NA NAŠEM CD. Zobrazí vám všechna telefonická připojení nakonfigurovaná ve vašem počítači, včetně uživatelského jména a hesla. Pokud jste v nějakých dalších aplikacích taktéž zadávali nějaká hesla, pak si je můžete zobrazit prostřednictvím utility **Password Finder**, jež je rovněž k dispozici NA NAŠEM CD.

Způsob ochrany

Obecně by se v počítači žádná hesla ukládat neměla – a to nejen z bezpečnostních důvodů. Každé heslo, které často nezadáváte, rychle zapomenete a v případě nouze pak máte problémy se vůbec přihlásit.

Důležité utility na zahlazení stop

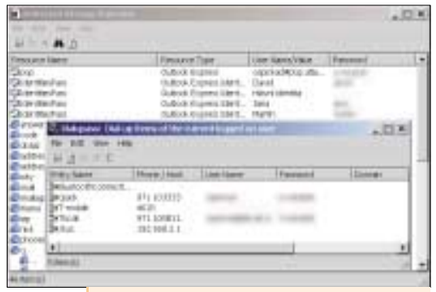
Program	Kategorie	Cena	Operační systém	Internetová adresa (Download)	Jazyk
Dialupass 2.42	utilita pro zjišťování hesel	zdarma	95/98/ME/NT4/2000/XP	**nirsoft.cjb.net** a NA NAŠEM CD (DIALUPASS.ZIP, 41 KB)	anglický
Doc Scrubber 1.1	zametač stop	pro soukromé použití zdarma	95/98/ME/NT4/2000/XP	**www.docscrubber.com** a NA NAŠEM CD (DOCSCRUBBERSETUP.EXE, 820 KB)	anglický
Firefox 0.9.3cs	internetový prohlížeč	zdarma	95/98/ME/NT4/2000/XP	**www.firefox- browser.de** a NA NAŠEM CD (FIREFOXSETUP-0.9.3-CSCZ.EXE, 5,43 MB)	český
Global Safe Disk AES 1.93.1	utilita pro šifrování disku	zdarma	2000, XP	**www.download.de/downloads/d_beitrag_10621010.html?tid1= 15361&tid2=22427** a NA NAŠEM CD (SETUPAES.EXE, 7,45 MB)	německý
Ii System Wiper 2.4	zametač stop	zdarma	98/ME, 2000, XP	**www.iisoftware.net** a NA NAŠEM CD (CLEAN.EXE, 452 KB)	anglický
Password Finder 2.0	utilita pro zjišťování hesel	zdarma	95/98/ME, NT 4, 2000, XP	**www.svenbader.de/e_index.html** a NA NAŠEM CD (PASSWORD.EXE, 533 KB)	německý
PC Inspector E-Maxx 1.0	zametač stop	zdarma	MS-DOS	**www.pcinspector.de** a NA NAŠEM CD (PCI_EMAXX.EXE, 733 KB)	anglický
PC Inspector File Recovery 3.0	záchrana dat	zdarma	95/98/ME, NT4, 2000, XP	**www.pcinspector.de** a NA NAŠEM CD (PCI_FILERECOVERY.EXE, 3,79 MB)	anglický
Protected Storage Passview 1.61	utilita pro zjišťování hesel	zdarma	95/98/ME, NT4, 2000, XP	**nirsoft.cjb.net** a NA NAŠEM CD (PSPV.ZIP, 32 KB; český jazykový modul PSPV_CZECH.ZIP, 1,03 KB rovněž NA NAŠEM CD)	český
Remove Hidden Data Add-in	zametač stop	zdarma	Word XP, 2003	**www.microsoft.com/downloads/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&displaylang=en** a NA NAŠEM CD (RHDTOOL.EXE, 259 KB)	anglický
Win9x Passview 1.1	utilita pro zjišťování hesel	zdarma	95/98/ME	**nirsoft.cjb.net** a NA NAŠEM CD (WIN9XPV.ZIP, 18,3 KB)	anglický

Pro vymazání všech uložených hesel proto postupujte následovně: nejprve si pomocí výše uvedených utilit zobrazte, kde všude máte ve svém systému hesla uložena.

Pak spusťte odpovídající aplikace, přesuňte se do dialogového okna pro nastavení uživatelských dat, odstraňte heslo a zrušte možnost (pokud existuje), umožňující pamatovat si heslo. V Internet Exploreru zakážete zapamatování hesel v menu *Nástroje/Možnosti internetu* na záložce *Obsah*, když stisknete tlačítko *Automatické dokončování* a v dialogovém okně zrušíte zatržítko u položky *Uživatelská jména a hesla na formulářích*. Nyní ještě stiskněte tlačítko *Vymazat hesla*, čímž odstraníte všechna již uložená hesla, která jste kdy do nějakých formulářů psali.

Pro odstranění všech hesel zadávaných při přihlašování do systému spusťte ve Windows 2000 nebo XP program **Protected Storage Passview**, který najdete NA NAŠEM CD, a označte v něm všechny položky a smažte je stiskem tlačítka <Delete>.

V systémech Windows 95/98/ME smažte soubory **<uživatelské jméno>.PWL**, které se nacházejí ve složce Windows. Tím navíc odstraníte i všechna hesla pro *Telefonické připojení sítě* a pro přístup ke sdíleným prostředkům v síti.



▲ **Nejistá výhoda: i když se to zdát velmi pohodlné, neukládejte do počítače žádná hesla. Pomocí freewarových utilit se totiž dají velmi snadno odhalit.**

6) Smazané soubory se dají snadno obnovit

Otázka: ***Mohu si být skutečně jistý, že všechny soubory, které smažu, jsou nenávratně pryč?***

▲ **Nespoléhejte se na odstraňování souborů prostřednictvím funkce ve Windows: pomocí speciálních utilit, jako je např. PC Inspector File Recovery, se dají smazané soubory ve většině případů docela jednoduše obnovit.**

Odpověď: Na tuto otázku lze jednoznačně odpovědět „ne“. Při mazání jsou odstraňované soubory nejprve umisťovány do Koše, z něhož se dají velmi snadno obnovit. Ale i když Koš vysypete nebo když budete při odstraňování souborů držet stisknutou klávesu <Shift>, aby se mazané soubory do Koše neumisťovaly, nejsou mazaná data s konečnou platností odstraněna. Dokud Windows uvolněné místo nepřepíší jinými daty, dají se smazané soubory buď úplně, nebo alespoň částečně obnovit. Umožňuje to speciální software pro záchranu dat, například **PC Inspector File Recovery**, který naleznete i NA NAŠEM CD.

Dokonce i když aplikace pro obnovu dat nenaleznou žádný soubor, jenž by se dal obnovit, nemusí to znamenat, že jsou všechny smazané soubory v nenávratnu. Ve speciálních laboratořích firem (například **Ontrack – www.ontrack.cz** či **Datarecovery – www.datarecovery.cz**) zabývajících se obnovou dat dokáží specialisté prostřednictvím zvláštních, často časově velmi náročných metod i v takových případech data zrekonstruovat do původní podoby.

Způsob ochrany

V žádném případě neodstraňujte citlivé soubory pomocí funkce pro mazání souborů ve Windows, nýbrž používejte speciální software. Vhodným nástrojem je například **Global Safe Disk AES**, jenž disponuje všemi potřebnými funkcemi. Najdete jej i NA NAŠEM CD. Pokud po instalaci programu klepnete na odstraňovaný soubor pravým tlačítkem myši, objeví se vám v kontextovém menu příkaz *Sicheres Vernichten*. Pro mazání si můžete vybrat ze tří variant, z nichž sice nejbezpečnější, ale zároveň nejpomalejší je metoda Gutmannova. Při ní jsou soubory 35× přepisovány, takže se nedají obnovit ani ve speciálních laboratořích zabývajících se záchranou dat.

Soubory, které jste smazali již dříve pomocí funkce pro odstraňování souborů ve Windows, máte možnost navždy zlikvidovat pomocí funkce *Ungenutzte Festplattenbereiche säubern*.

Pokud budete chtít vyčistit kompletně celý disk, třeba když jej budete prodávat, nestačí jej jen zformátovat a vytvořit nové oddíly. Data se totiž dají obnovit i po těchto zásazích. Namísto toho použijte nástroj **PC Inspector E-Maxx**, který je dostupný zdarma a který naleznete i NA NAŠEM CD. Ten dokáže váš disk důkladně pročistit. Při instalaci utility se vytvoří i spouštěcí disketa, obsahující instalovaný program. Pomocí této diskety spustíte počítač a potom budete krok za krokem vedeni dále. V závislosti na velikosti disku může celá operace trvat až několik hodin. Pokud ve vašem případě nehraje čas roli, povolte funkci *Triple Flux*. Pak je jisté, že mazaná data nikdo nikdy neobnoví ani v té nejlepší laboratoři vybavené pro záchranu dat. K tomu účelu otevřete v libovolném textovém editoru ještě před spuštěním počítače ze spouštěcí diskety soubor EMAXX.SCR a v něm nahraďte řetězec „**write**“ za výrazem „**operationType=**“ řetězcem „**secureWrite**“ a odstraňte symbol křížku (**#**) před výrazem „**secureWritePasses=3**“.

7) Další zrada: seznam naposledy otevřených souborů

Otázka: ***Jak se mohu dozvědět, zda někdo během mé nepřítomnosti neotevíral nějaké soubory nebo nespouštěl nějaký program?***

Odpověď: Prakticky každý program si poznamenává, které soubory v něm byly naposledy otevřeny. Tyto údaje se zpravidla nacházejí úplně dole v menu *Soubor*. Klepnutím na ně má uživatel okamžitý přístup k těm souborům, s nimiž naposledy pracoval. Pokud by se tu ocitly položky, které vám nic neříkají, pak věřte, že s programem pracoval mimo vás ještě někdo jiný. Dokonce i samotná Windows si sama zapisují, které soubory byly naposledy otevřeny, jejich seznam lze nalézt v nabídce *Start* pod položkou *Dokumenty*.

Způsob ochrany

Pakliže po sobě nechcete zanechat žádné stopy, použijte zdarma dostupnou utilitu **Ii System Wiper**, kterou naleznete NA NAŠEM CD. Ta maže seznam naposledy otevřených dokumentů u mnoha aplikací, počínaje programem Acdsee přes Word až po Winzip. Na základě vašeho požadavku rovněž dokáže zamést stopy i po surfování – vyčistí cache paměť prohlížeče, cookies a historii navštívených stránek. Při prvním spuštění programu přesně specifikujete, které stopy se mají po vás zamést. Toto nastavení se následně uloží a při dalším spuštění programu stačí pouze klepnout na tlačítko *Start* a všechny stopy po vás jsou zahlazeny. 4 0488/OK ❑