Co všechno o nás ví Microsoft?

Máte představu, co všechno se dá z vašeho počítače zjistit? (CD)

DAVID ČEPIČKA, THORSTEN EGGELING, ANDREAS KROSCHEL A CHRISTIAN LÖBERING

Dnešní uživatel počítače je pro ostatní stále průhlednější. Firma Microsoft v současné době spolupracuje s předními výrobci hardwaru jako jsou AMD, HP či Intel na vývoji technologie NGSCB (*Next Generation Secure Computing Base*), která slibuje zabezpečení počítače na skutečně vysoké úrovni. Otázkou je, co se vlastně výrazem zabezpečení počítače myslí. Znamená to vyšší úroveň ochrany před viry, červy či spamem? Nikoliv, v první řadě jde o lepší ochranu výrobců softwaru a prodejců CD disků před neoprávněným kopírováním. Technologie NGSCB bude například použita už v příštím roce v nové verzi Windows, která se bude nazývat Longhorn. Stejně tak se předpokládá povinná certifikace v mnoha oblastech každodenního používání počítačů, a to na úkor soukromí uživatelů. Potřebné certifikáty totiž budou pravděpodobně integrovány ve formě dat do nějakého určitého systému.

Někdejší sci-fi představy jsou již dnes realitou

To, co dnes vypadá jako představy z říše science fiction, je však již dlouho připraveno a částečně je to už realitou. Spyware si vede záznamy o tom, na kterých stránkách se uživatel pohybuje, aby mu mohl v prohlížeči naservírovat pop-up okna s reklamou podle jeho zájmů. Windows XP při aktivaci systému přes internet přenáší data, která jednoznačně identifikují hardware v počítači. Stahování některých utilit a systémových vylepšení z webového serveru Microsoftu zase vyžaduje úspěšné ověření nainstalovaného operačního systému a zjistí-li, že používáte nelegální kopii Windows, pak je stažení softwaru odmítnuto s hlášením *Validation Failure*. Hudební skladby komerčních producentů jsou chráněny technologií DRM (*Digital Rights Management*) a dají se přehrát pouze na jednom počítači. Na jiném počítači se vám nahrávku přehrát nepodaří…

Všichni výrobci softwaru slibují, že se při procesech spojených s ověřováním pravosti nebudou přenášet žádné údaje, které by vás mohly jednoznačně identifikovat. Přesto – můžeme jim věřit? Na následujících stránkách si přečtete, jak daleko dnes Microsoft a jemu podobné firmy mohou zajít a jak lze zjistit, co všechno o vás může počítač prozradit.

Co o nás Windows prozradí

Ať už je řeč o aktivaci, instalaci záplat, stahování z webového serveru Microsoftu nebo přehrávání souborů ve Windows Media Playeru – při kterékoliv z těchto aktivit Windows rády posílají informace do internetu. V současné době nestačí přenášená data na to, aby jednoznačně identifikovala jednotlivou osobu, tedy vás osobně. I když i dnes existují výjimky. V této části článku budeme zkoumat činnosti na internetu, které se týkají prakticky každého uživatele počítače.

1. Aktivace Windows: celkem neškodná záležitost

Od verze Windows XP vybavuje Microsoft svoje operační systémy jakýmsi druhem časované bomby. Jde konkrétně o to, že pokud uživatel do 30 dnů od instalace Windows neoznámí tuto skutečnost výrobci programu a takto nabytou legální verzi Windows nezaregistruje, pak již svůj operační systém nespustí. Aktivace systému se provádí prostřednictvím souboru MSOOBE.EXE a parametru */a*. Zmíněný soubor se nachází ve složce **Windows\System32\oobe**.

Uživatel, který chce o sobě prozradit co nejméně, si vybere při aktivaci pravděpodobně možnost aktivace přes telefon. Při tomto způsobu registrace se call-centrum Microsoftu nedozví kromě 50místného číselného kódu nic dalšího.

Při aktivaci prostřednictvím internetu se toho posílá daleko více. Komunikace mezi vaším operačním systémem a serverem pro aktivaci probíhá přes šifrované spojení SSL (*Secure Sockets Layer*) – což je zabezpečená varianta přenosového protokolu HTTP. V redakci Tecchannelu (**www.tecchannel.de**) se pokusili data odesílaná při aktivaci zachytit a analyzovat. Operační systém kontaktuje aktivační server ve třech krocích, které musí být vždy aktivačním serverem potvrzeny. Přenášeno je identifikační číslo vaší kopie Windows (*Product-ID*), které je ostatně zobrazeno v dialogovém okně, jež uvidíte, pokud na pracovní ploše klepnete pravým tlačítkem na ikonu *Tento počítač* a z kontextového menu zvolíte příkaz *Vlastnosti*. Toto číslo se vypočítává z licenčního klíče (*Product-Key*), která zadáváte při instalaci. Od vydání Service Packu 1 se při aktivaci kromě licenčního klíče (*Product-Key*) přenáší i jazykové nastavení systému a informace o hardwarové konfiguraci. Tou se myslí například jednoznačná MAC adresa síťového adaptéru a sériové číslo procesoru.

Všechny tyto údaje jsou více než dostatečné pro přesnou identifikaci uživatele počítače, ovšem tato data nejsou odesílána přímo, nýbrž před samotným odesláním prochází šifrováním hašovacím algoritmem. Výsledkem hašování je vygenerované číslo, které je sice pro každého uživatele jedinečné, nedá se však žádným způsobem zpětně dešifrovat na původní hodnoty jednotlivých komponent. Z toho všeho vyplývá, že Microsoft nemůže pomocí procesu aktivace vystopovat, jaké komponenty v počítači používáte a jaký software je na počítači nainstalován.

2. Windows Update posílá více než je třeba

Daleko otevřeněji než v předchozím tipu popisovaná aktivace se chová služba Windows Update. Pokud navštívíte WWW stránku **windowsupdate.microsoft.com** nebo použijete funkci *Automatické aktualizace*, pošle prvek ActiveX dotaz na server s updaty.

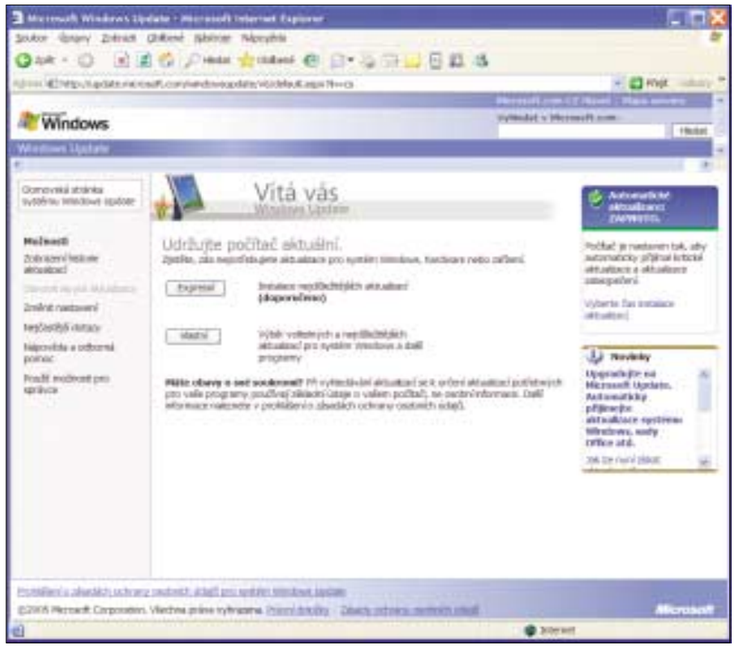
My jsme zjistili, že množství přenášených informací daleko přesahuje představy běžného uživatele. Vedle bezesporu nutných informací z registrů, jako je informace o verzi systému, verzi prohlížeče a o verzích jiných programů od Microsoftu, pro něž mohou být rovněž dostupné updaty, se přenáší i informace o jazykových nastaveních Windows, dále *Product-Key*, verze BIOSu a informace o již instalovaných updatech.

To vše by se snad dalo i tolerovat, ovšem prvek ActiveX přenáší i tzv. číslo **Guid** (*Globally Unique Identifier*), stejně jako IP adresu. V případě čísla **Guid** se jedná o hexadecimální hodnotu 32 znaků, která je pro každý počítač jiná. Za normálních okolností se sice toto číslo nedá jednoznačně přiřadit k vaší osobě, ovšem za jistých okolností to udělat lze. Je tomu tak v případě, kdy svoji instalaci Windows zaregistrujete (ne pouze aktivujete), nebo pokud si vyžádáte pravidelné zasílání novinek od Microsoftu. Pak totiž z technického hlediska není žádný problém, aby se například při updatu systému přenášená data přiřadila k vašim osobním údajům jako vaše jméno či adresa.

Vycházíme z toho, že v současné době zatím nemá využití těchto technik pro Microsoft žádný význam. Podle Microsoftu nashromážděné údaje stále slouží pouze ke statistickým účelům, zejména ke sledování a záznamu přístupu počítačů s určitou IP adresou na stránky Windows Update. Přesto považujeme nutnost registrace nebo pravidelné zasílání novinek z Microsoftu za záležitosti, bez kterých se snadno obejdeme.

3. Stahování ze stránek Microsoftu: jednoznačně nejednoznačné

V poslední době dělá firma Microsoft všechno pro to, aby ze svých řad vyloučila co možná nejvíce těch, kteří používají její operační systém nelegálně. Konkrétním případem je nejnovější akce *Genuine Microsoft Windows* (neboli *Je vaše kopie systému Windows originální?*) – v současnosti obsahuje ještě nepovinné ověření pravosti instalace Windows při návštěvě stránek Microsoftu se službou Stažení softwaru (**www.microsoft.com/downloads**). Pokud se zmiňovaná procedura stane v budoucnosti povinnou a váš systém touto zkouškou neprojde, budou pro vás tyto stránky nepřístupné.



▲ **Ochrana dat nebo spíše jejich krádež? Pokud budete svůj systém aktualizovat, pak si Microsoft nebude brát servítky a z vašeho počítače si vezme, co bude chtít.**

Prodejci to považují za službu zákazníkům, uživatelé se zase obávají ztráty soukromí. O čem to vlastně mluvíme? Přece o skutečnosti, že řada programů zasílá bez našeho vědomí informace z našeho počítače do internetu. Přečtěte si zde, jaká data se z vašeho počítače odesílají a jak se před přílišnou zvědavostí výrobců některých programů chránit.

Aktivace Windows s využitím call-centra

Pokud se rozhodnete aktivovat svůj operační systém přes telefon, nadiktujete operátorovi jedno padesátimístné číslo. To se mimo jiné vypočítává z tzv. *Product-ID* a hašovací hodnoty (ta představuje kontrolní součet) a závisí na hardwarové konfiguraci vašeho počítače. Na telefonickém centru se toto číslo ověří a vy pak získáte kód, kterým provedete aktivaci operačního systému – tím, že jej zadáte do příslušného dialogového okna pro aktivaci Windows.

Povinný update

I když se vám myšlenka odesílání dat z vašeho počítače na server Microsoftu vůbec nelíbí, nic jiného vám stejně nezbývá. Pravidelné aktualizování systému je takřka nutné, neboť jinak otevíráte pomyslná vrátka do systému nejrůznějším virům a červům. V nejhorším případě může také dojít k tomu, že váš počítač takřka zmutuje do podoby zombie, rozesílající spam a nejrůznější informace lidem po celém světě. V tomto světle se pak myšlenka výměny dat mezi uživatelem a Microsoftem pro většinu z nás jeví daleko přijatelnější.

Zabiják nelegálních kopií

Každý Service Pack obsahuje jakousi černou listinu s ilegálními aktivačními čísly (*Product-Keys*). Ten, kdo vlastní systém s některým z těchto čísel, pak Service Pack nemůže nainstalovat. Totéž platí i při aktualizaci Windows a nyní už i při obyčejném stahování souborů. Microsoft svoji černou listinu neustále aktualizuje. Cílem této strategie je znemožnit uživatelům pirátských kopií Windows aktualizování systému. Operační systém s celou řadou bezpečnostních děr se pak dá použít pouze k pochybným účelům, například pro rozšiřování spamu – pro běžné používání se pirátské kopie Windows stanou prakticky nepoužitelné.

Plané řeči prohlížeče

Když si webový prohlížeč vyžádá od nějakého internetového serveru obsah WWW stránky, musí mu jako protislužbu odpovědět na několik otázek. Většinou se jedná o údaje jako název prohlížeče, jeho verze, nainstalované doplňky a jeho jazyková verze. Pokud se na internetovou stránku prohlížeč dostane nepřímo klepnutím na odkaz na jiné internetové stránce, pak prohlížeč prozrazuje internetovému serveru, z jaké stránky se na tento server dostal.

Napadení spywarem

Lze tvrdit, že spyware přednostně napadá Internet Explorer. To ale vůbec neznamená, že se do počítače může dostat pouze tímto způsobem. I uživatelem instalovaný software může obsahovat škůdce. Zvláště pozorní bychom proto měli být u programů pocházejících např. z výměnných sítí – v tomto případě je zde daleko více pochybných zdrojů než těch seriózních.

Pakliže v současnosti zkusíte stáhnout kupř. Windows Media Player 10, bude vám nabídnuto podstoupit zkoušku ověření pravosti. Při ověřování pravosti odesílá váš počítač podobně jako při provádění aktualizací na server Microsoftu informace o systému a verzi BIOSu, stejně jako *Product-ID*. Právě na základě naposledy zmíněné hodnoty testovací algoritmus zjistí, zda se jedná o legální nebo nelegální verzi Windows. Při přenosu dat je stejně jako při aktualizaci Windows přenášeno číslo **Guid** – tak je možné přenášená data dané kopii Windows jednoznačně přiřadit.

Upozornění! Číslo **Guid** se před stahováním odesílá i tehdy, pokud ověřování pravosti vaší kopie Windows (byť deklarováno jako nepovinné), odmítnete.

4. Windows Media Player: v současné verzi tolik neprozrazuje

Verze 7 a 8 programu Windows Media Player jsou při vložení hudebního CD disku skutečně upovídané. Při žádosti o informace o disku z internetové databáze CDDB se jen tak mimochodem odesílá i **Guid** vašeho operačního systému přímo na server Microsoftu. Novější verze programu 9 a 10 se v tomto bodě drží zpátky. Standardně přehrávač ve své nejnovější verzi zjišťuje u všech médií, která nejsou chráněna DRM (*Digital Rights Management*), pouze informace z databáze CDDB podle naprosto neškodného identifikačního čísla vloženého CD disku. Odeslání **Guid** je nyní pouze volitelné a dá se nastavit v menu *Nástroje/Možnosti* na záložce *Osobní údaje*, kde se skrývá pod volbou *Odesílat jednoznačné ID přehrávače poskytovatelům obsahu.* Celá řada služeb nabízejících stahování hudby totiž tuto informaci vyžaduje. Za normálních okolností ale neexistuje žádný rozumný důvod, proč byste tuto volbu měli povolovat.

▲ **Umlčený přehrávač: u Windows Media Playeru verze 9 či 10 je přenášení „jednoznačného ID přehrávače" standardně deaktivováno.**

Programy pro práci na internetu

Od internetového prohlížeče a programu pro práci s elektronickou poštou očekáváte, že už z principu budou stahovat a odesílat data z internetu – ostatně je to jejich úkol. Rozhodně to ale neznamená, že byste se museli vzdát ovlivňování toho, jaká data se mají z internetu stahovat a jaká do internetu odesílat. Nechcete-li kupř. do nějakého webového formuláře zadávat svoji pravou e-mailovou adresu, pak klidně můžete zadat nějakou smyšlenou – samozřejmě pokud na tuto adresu neočekáváte nějakou odpověď. Přesto mohou formuláře často obsahovat celou řadu neviditelných políček, která se s formulářem rovněž přenášejí.

To však není jediný příklad. Při jakékoliv práci na internetu zasíláte na nějaký internetový server neustále celou řadu dat, ať se jedná o hesla pro přihlášení do nějakých internetových služeb nebo třeba heslo pro přístup do vaší e-mailové schránky. Například i při odesílání e-mailu je jeho text odesílán nešifrovaně, takže si jej teoreticky může na každém serveru, přes který k příjemci putuje, kdokoliv přečíst.

5. Skryté informace ve formulářích

Jestliže vyplníte políčka nějakého webového formuláře a poté jej odešlete, jste informováni o tom, jaká data odesíláte – nebo byste aspoň měli být informováni. Ve skutečnosti takové formuláře velmi často obsahují skrytá políčka.

Docela jednoduše si tento fakt můžete vyzkoušet v Googlu. Pro zobrazení všech políček, vyskytujících se na stránce **www.google.com**, budete potřebovat internetový prohlížeč Firefox. Přesuňte se k tomu účelu na zmíněnou internetovou stránku a do vyhledávacího políčka zadejte libovolný výraz, ale dotaz neodesílejte. Z menu *Nástroje* vyberte položku *Informace o stránce*. Na záložce *Formuláře* pak v horním poli vidíte všechny formuláře dostupné na dané stránce. U Googlu je to v tomto případě pouze formulář označený písmenem *f*. Když jej označíte, objeví se ve spodním poli všechna v něm obsažená políčka. Jedno z nich je označeno jako *hidden* (*skryté*). Přenáší řetězec **cs**, což můžeme považovat za neškodné. Google získává tuto hodnotu ze svých nastavení a používá ji, aby mohl výsledky vyhledávání zobrazit v češtině.

Kromě jiného zde rovněž můžete vidět tzv. *Radio Buttons* (přepínače, které se aktivují klepnutím) a dále tlačítka – to všechno jsou prvky formuláře. Dá se tedy říci, že i na internetových stránkách, které neobsahují žádná políčka, jež by se dala vyplnit, odesíláte stiskem patřičného tlačítka nějaký formulář.

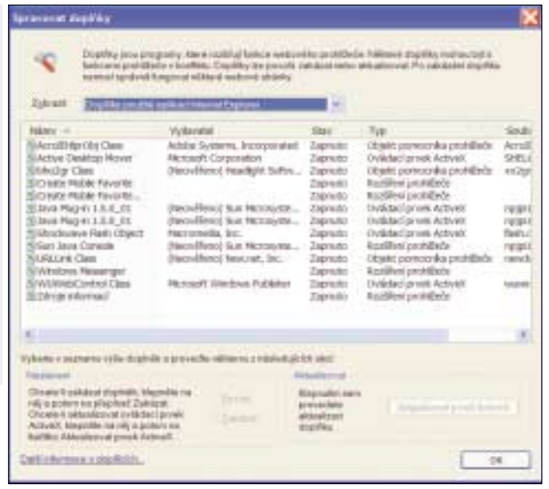
◀ **Formuláře pod lupou: políčka typu hidden jsou neviditelná. Přesto se jejich hodnota po odeslání formuláře objeví bez našeho vědomí na serveru.**

Na druhou stranu můžete prostřednictvím zmíněné metody před odesláním libovolného formuláře přes Firefox zkontrolovat všechna pole a údaje, které se budou případně odesílat.

6. Internetový prohlížeč: panely nástrojů a jejich rozšíření

Na začátku byl panel nástrojů Google. Tento praktický pomocník pro vyhledávání na internetu díky svému velmi jednoduchému ovládání významně přispěl k oblibě Googlu jako vyhledávače samotného. Mezitím se objevila celá řada dalších doplňků prohlížeče, z nichž většina měla právě formu nějakého panelu nástrojů. Následujících doplňků pak začala využívat celá řada spywaru, a to tak, že při zadání nějakého slova do vyhledávače bylo toto slovo zachyceno spywarovým programem, který je poslal na server, zabývající se cíleným zasíláním reklam a zobrazováním pop-up oken. Spyware dnes můžete odstranit řadou utilit, jednou z nejznámějších je **Ad-Aware**, který naleznete i na našem CD. Program dokáže rozpoznat a odstranit mimo jiné i škodlivé doplňky nainstalované do internetového prohlížeče.

Celkový přehled o všech instalovaných doplňcích nabízí Internet Explorer v operačním systému Windows XP Service Pack 2. V menu *Nástroje* klepněte na položku *Spravovat doplňky*. V seznamu *Zobrazit* si pak můžete vybrat mezi zobrazením všech dostupných a momentálně nahraných doplňků. Bohužel není možné přes toto okno daný doplněk odstranit. Stále však zůstává možnost doplněk deaktivovat, pokud upřednostňujete manuální odinstalování doplňků před jejich automatickým odstraněním prostřednictvím utilit typu Ad-Aware. Deaktivaci neznámého či podezřelého doplňku provedete volbou *Zakázat*.



▶ **Doplňky internetového prohlížeče: původně tato rozšíření slouží k rozšíření možností Internet Exploreru, přesto se mezi ně může dostat i spyware.**

Pokročilejší uživatelé se pak mohou v tomto článku v odstavci **Analýza** poučit o dalších způsobech sledování podezřelých aktivit v systému. Pokud se u spywaru jedná o jeho podobu nainstalovanou jako doplněk prohlížeče, pak se program, který proti vaší vůli odesílá do internetu data z vašeho počítače, jmenuje IEXPLORE.EXE – jde tedy o Internet Explorer. Proto je nutno mezi všemi internetovými servery, které Internet Explorer kontaktuje, najít ten, jenž nemá s adresami zadávanými do panelu *Adresa* žádnou souvislost. Tímto způsobem pak naleznete buď někoho, kdo spyware financuje, nebo někoho nevinného, kdo se stal obětí šiřitelů spywaru.

A co Firefox? V současné době nejsou pro tento prohlížeč známa žádná rozšíření, která by obsahovala spyware. Technicky to samozřejmě možné je a zdá se, že je pouze otázkou času, kdy se nějaká objeví.

7. Nešifrovaná hesla pro přístup k e-mailovým schránkám

Většina poskytovatelů e-mailových schránek povoluje pro přihlášení jak šifrovanou, tak nešifrovanou variantu. Na tomto místě vás musíme va-

Zpětná kontrola vašich osobních dat

„Vážený pane X, dovolujeme si vám oznámit, že jste vyhrál v naší loterii milion korun." Taková oznámení nacházíme v poštovních schránkách docela často. Nevyžádané reklamní dopisy jsou ostatně fenoménem nejen počítačovým, nýbrž nás v nejrůznějších formách potkávají i v běžném životě. Jakým způsobem více či méně seriózní firmy přišly k našemu jménu a adrese, však zůstává jejich tajemstvím. Počínaje telefonním seznamem, firmami profesionálně se zabývajícími získáváním osobních dat a nejrůznějšími mafiemi konče, to vše jsou možné zdroje, kde se dají osobní data získat. Problém zneužití osobních dat se však nejčastěji týká lidí, kteří s nimi zacházejí velmi benevolentně. Nejrůznější hry, objednávky přes zásilkové služby, reakce na nejrůznější ankety – to vše by nefungovalo, aniž by zájemce na sebe nezanechal nějaký kontakt. Také se najde dost firem, které chybějící zatržítko před položkou *„Neposkytovat moje osobní údaje třetím osobám"* berou skutečně vážně. Důvěra je samosebou dobrá věc, ale kontrola je věc ještě lepší. Proto byste měli mít i nějakou možnost, jak možné neoprávněné zneužití vašich dat odhalit. Ve skutečnosti to ale není nijak složité. Pokud si něco objednáte nebo vyžádáte od firmy A, zadejte svoje osobní údaje ve tvaru *<jméno> A. <příjmení>*, v případě firmy B zadejte osobní údaje ve formě *<jméno> B. <příjmení>*. Při zasílání objednaného zboží zfalšované písmenko u druhého jména nečiní zpravidla žádný problém. Pokud později obdržíte na vaši adresu reklamní dopis ve tvaru *<jméno> A. <příjmení>*, vězte, že právě firma A vaši adresu zneužila. Z právního hlediska sice tato informace není nijak využitelná, ale firma, která důvěru svých zákazníků takto zneužila, zřejmě pro vás v budoucnu zajímavá nebude.

Rozšíření a doplňky

Rozšíření a doplňky jsou drobné programy, které neběží samostatně, nýbrž uvnitř internetového prohlížeče. Jejich úkolem je rozšířit jeho funkčnost. Bohužel je mechanismus, kterým jsou tyto doplňky spojeny s prohlížečem, velmi dobrým úkrytem pro malware. Minimálně doplňkům, které jsou uveřejňovány na CD PC WORLDu, můžete bez obav důvěřovat, neboť všechny důkladně prověřujeme.

Používání SSL

Protokol SSL není vhodný pouze pro šifrované přenosy dat, nýbrž umožňuje i ověření identity internetového serveru, a to pomocí certifikátu serveru. Proto až se vám na monitoru objeví dialogové okno s certifikátem, neodstraňujte ho okamžitě, nýbrž si celý certifikát projděte. Pokud si nejste jisti, že se připojujete k správnému serveru, raději spojení odmítněte.

E-mail je čitelný vždy

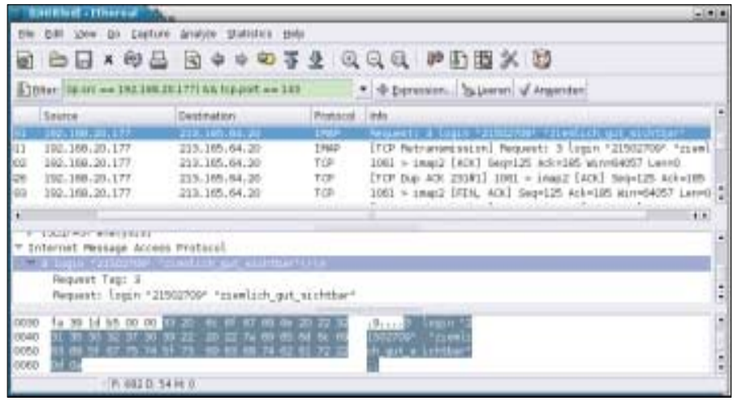
I při šifrovaném připojení k poštovnímu serveru se vlastní text e-mailu přenáší vždy v nešifrované podobě. To znamená, že jej kdokoliv může při cestě od odesílatele k příjemci na každém serveru, přes který putuje, zachytit a přečíst si ho. Každý e-mail by proto měl obsahovat pouze informace, které byste napsali třeba i na pohlednici. V opačném případě raději e-maily šifrujte, např. pomocí utility **PGP**.

Slídiči

Programy pro sledování síťového provozu, jako například **Ethereal**, dokáží zobrazit údaje obsažené v libovolném datovém paketu komukoliv. Velká část dat, která přes síťové rozhraní putuje, však slouží pouze k udržování spojení. Například webový server a internetový prohlížeč musí, než spolu začnou komunikovat, nalézt společný způsob této komunikace. Sledování určitého přenosu dat pak vyžaduje mnoho času a trpělivosti.

Winpcap

Winpcap je zdarma dostupný ovladač, který využívá řada programů k analýze síťového provozu. Tento ovladač se umístí mezi sledovanou aplikaci a ovladač síťové karty. Přitom odposlouchává veškerý provoz v počítačové síti. Sledovaná aplikace si tohoto ovladače ani nevšimne a ani výkon sítě jím není nijak negativně ovlivňován. Vzhledem k tomu, že Windows považují nainstalovaný modem za virtuální síťový adaptér (s připojením typu PPP), je i v tomto případě možné sledování síťového provozu. Při použití nejnovější verze ovladače **3.0** (najdete ji i NA NAŠEM CD) je však toto sledování možné pouze ve Windows 95/98/ME. V betaverzi **3.1** je již zabudována, zatím z pokusných důvodů, podpora pro připojení typu PPP i pro Windows 2000/XP/2003. Bohužel betaverze ovladače, kterou jsme testovali, si s verzí Etherealu 0.10.11 příliš nerozuměla.



▲ **Sousedi naslouchají: heslo pro přihlášení do e-mailové schránky posílané v nešifrované podobě je snadno zachytitelné. Totéž platí i pro uživatelské jméno.**

rovat před poslední zmíněnou možností. Heslo sice zasíláte pouze k poskytovateli služby, ovšem nějaký zlomyslný kolega či třeba spolubydlící vaše heslo může snadno zachytit – sledování provozu sítě funguje i v lokální počítačové síti. Hrozí zde nejen zachycení hesla, ale i dalších přihlašovacích údajů – vašeho uživatelského jména a jména serveru, na němž je schránka zřízena, což může vést i k tomu, že vaše schránka může být používána někým jiným, neboli ji lze takto velmi snadno zneužít.

Proto doporučujeme, abyste při odesílání nebo přijímání elektronické pošty měli heslo zašifrované. V Outlook Expressu to zařídíte tak, že klepnete v menu *Nástroje/Účty*, označíte postupně každý účet a stisknete tlačítko *Vlastnosti*. Potom stačí na záložce *Upřesnit* povolit možnost *Tento server požaduje zabezpečené připojení (SSL)*. Většina podobných programů pak poskytuje podobné položky.

Totéž platí i pro webové formuláře: pokud máte možnost výběru mezi šifrovaným a nezašifrovaným připojením, pak jednoznačně volte zabezpečení šifrované přes protokol SSL. Tento způsob připojení poznáte podle ikonky žlutého visacího zámku na stavovém řádku prohlížeče.

Analýza

Updaty, aktivace, registrace, digitální práva, spyware… už dnes toho pro každý počítač existuje tolik, co vyžaduje stahování dat z webu. Co všechno se ale při takových přenosech přesně děje, zůstává pro většinu obyčejných uživatelů záhadou. Přesto existuje prostředek a způsob jak zjistit, který program právě odesílá data, o co se daný program zajímá a kolik toho skutečně ví. Ostatně žádný program toho nemůže poslat víc, než kolik toho ví. Těmito cestičkami se pak ubírá pátrání po špiónech v našem počítači.

8. Které aplikace používají připojení k internetu?

Pokud chcete zjistit, které programy využívají připojení k internetu pro přenos dat, pak je nejlepším řešením instalace některého ze softwarových firewallů. Po spuštění aplikace vyžadující přístup do internetu se okamžitě ozve firewall a zeptá se vás, zda chcete této aplikaci přístup k internetu povolit nebo zablokovat. Řada firewallů se však u každého programu automaticky neptá. Tak kupříkladu **McAfee Personal Firewall** prohledává on-line databázi známých aplikací a automaticky tato povolení na základě této databáze přiřazuje. Samozřejmě je zde možné

▲ **Blokování přístupu: firewally dokáží zablokovat jakémukoliv programu přístup k internetu.**

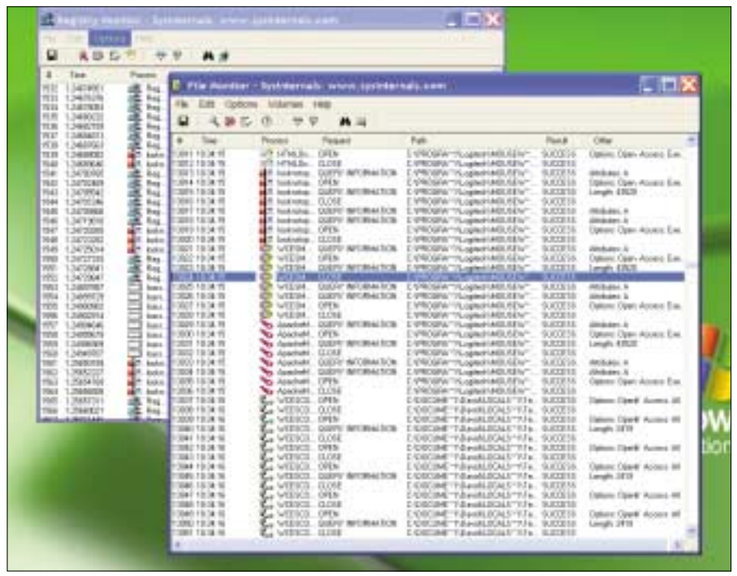
nastavit, podobně jako u ostatních firewallů, aby se dotazoval při spuštění každé aplikace a aby on-line databázi nepoužíval.

9. Metody zjišťování přenášených dat jednotlivými programy

Problém zjištění toho, který program používá připojení k internetu a jaká data přitom přenáší, není bohužel vůbec triviální. Takzvaná přímá meto-

da využívá záznam všech odeslaných dat. Problém ale spočívá v tom, že těchto dat je velké množství a jejich analýza je poměrně obtížná. Pokud jsou data šifrována, pak z nich logicky nepoznáte vůbec nic. V každém případě ale zjistíte, kolik dat daný program na který server zaslal. Pokud se jedná například o několik stovek bajtů, pak tento program dozajista neposílá žádné rozsáhlé seznamy hardwaru či softwaru nainstalovaného v počítači. Pakliže nějaký program kontaktuje nejen server svého výrobce, ale i servery jiných firem, může to být indicie na možný špionážní software.

Nepřímou metodou zjišťování aktivit programů je záznam všech přístupů k souborům a registru. Tím se dá přesně zjistit, o jaké informace se daný program zajímá. Tak je například velmi podezřelé, pokud nějaký doplněk, který má optimalizovat schopnosti Internet Exploreru, přistupuje ke klíči **Hkey_Local_Machine\Software\Microsoft\Office**. Naproti tomu u utility určené pro MS Office to nic podezřelého není.



▲ **Zahrajte si na detektiva: prostřednictvím utilit Regmon a Filemon zjistíte, ke kterým klíčům v registru a ke kterým souborům sledovaný program přistupuje.**

10. Možnosti záznamu přístupu do registru a k souborům

Firewall je bezesporu velmi užitečný nástroj proti útokům z internetu, bohužel nedokáže rozlišit, zda se při požadavku na přístup z internetu do počítače či naopak jedná o požadavky oprávněné nebo neoprávněné. Možný pokus o špionáž tak zablokuje, stejně jako například pokus o zjištění aktualizací nainstalovaných na vašem počítači. Pokud máte u nějaké aplikace podezření, že neoprávněně odesílá data uložená na vašem pev-

Zdarma dostupné utility proti špionáži

Utilita	Cena	Operační systém	Název a velikost souboru	WWW stránky	Jazyk
Ad-Aware SE Personal Edition 1.06	zdarma pro soukromé použití	Windows 98/ME, NT4, 2000, XP	AAWSEPERSONAL.EXE (2,72 MB)	www.lavasoft.com	anglicky
Ethereal 0.10.11	zdarma	Windows 98/ME, NT4, 2000, XP	ETHEREAL-SETUP-0.10.11.EXE (9,31 MB)	www.ethereal.com	anglicky
Filemon 7.0	zdarma	Windows 2000, XP	FILEMONNT.ZIP (120 KB)	www.sysinternals.com	anglicky
Regmon 7.0	zdarma	Windows 2000, XP	REGMONNT.ZIP (108 KB)	www.sysinternals.com	anglicky
Winpcap 3.0	zdarma	Windows 95/98/ME, NT4, 2000, XP	WINPCAP_3_0.EXE (430 KB)	www.winpcap.org	anglicky

ném disku na nějaký internetový server, pak musíte její chování otestovat sami.

1. Přístupy do registru můžete zaznamenávat pomocí utility **Regmon 7.0**, kterou naleznete NA NAŠEM CD. Tento program nevyžaduje žádnou instalaci. Jednoduše rozbalíte instalační archiv do libovolné složky a program spustíte poklepáním na spouštěcí soubor. Protokolování registru začíná okamžitě po spuštění programu Regmon. Vzhledem k tomu, že operační systém i aplikace přistupují k registru prakticky neustále, zaplní se okno programu rychle většinou nezajímavými informacemi. Proto klepněte v panelu nástrojů na ikonu *Capture*, popřípadě stiskněte klávesovou zkratku <Ctrl><E>. Tím zastavíte proces protokolování. Poté klepněte na ikonu *Clear*, čímž záznamy z okna programu vymažete.

Nyní klepněte na ikonku *Filter/Highlight* (můžete použít klávesovou zkratku <Ctrl><L>, která má stejnou funkci) a zadejte do políčka *Include* jméno programu, který budete chtít sledovat. Regmon se bude řídit podle jména spustitelného souboru, který představuje tato aplikace. Pokud se spouštěcí soubor aplikace jmenuje například FOOBAR.EXE, postačí zadat název foobar. Velikost písmen v názvu programu nehraje žádnou roli. V poli *Highlight* pak můžete zadat kritérium, podle něhož se budou záznamy filtrovat, například jméno nějakého klíče registru. Pokud se pak v záznamech objeví položka se jménem zadaného klíče, bude zbarvena červeně. Nyní nastavené parametry uložte stiskem tlačítka *OK* a klávesovou zkratkou <Ctrl><E> spusťte monitorování. Nakonec spusťte program, který budete chtít sledovat. V okně programu se začnou objevovat všechny přístupy do registru ze strany této aplikace. Získaný záznam pak můžete uložit do souboru pomocí menu *File/Save*. Uložený soubor lze otevřít v libovolném textovém editoru, kde je také možné jednotlivé záznamy daleko lépe prohledávat.

2. Přístupy k souborům lze analyzovat pomocí programu **Filemon 7.0**, který rovněž naleznete NA NAŠEM CD. I u této utility postačí rozbalit archiv do libovolné složky a následně spustit EXE soubor. Ovládání programu je podobné jako u aplikace **Regmon**. I zde pozastavíte monitorování klávesovou zkratkou <Ctrl><E>. Dialogové okno pro nastavení filtru pak vyvoláte klávesovou zkratkou <Ctrl><L> a do políčka *Include* zadáte název spouštěcího souboru aplikace. Políčko *Highlight* opět slouží ke zvýraznění položek splňujících určité další kritérium. Po provedení všech nastavení dialogové okno uzavřete a klávesovou zkratkou <Ctrl><E> spusťte monitorování. Nakonec vyvolejte sledovanou aplikaci.

11. Kompletní sledování provozu na síti

Pro sledování síťového provozu je velmi oblíbená zdarma dostupná utilita **Ethereal 0.10.11**, kterou rovněž naleznete NA NAŠEM CD. Ve Windows XP bohužel zmíněný program pracuje pouze se zařízeními, které se dokáží chovat jako síťové karty, konkrétně PCI karty typu Ethernet (přípojky DSL), bezdrátové LAN karty, popřípadě externí síťové adaptéry. S klasickými modemy si bohužel program nerozumí. Pokud používáte Windows 98/ME, výše uvedená omezení v těchto systémech neplatí.

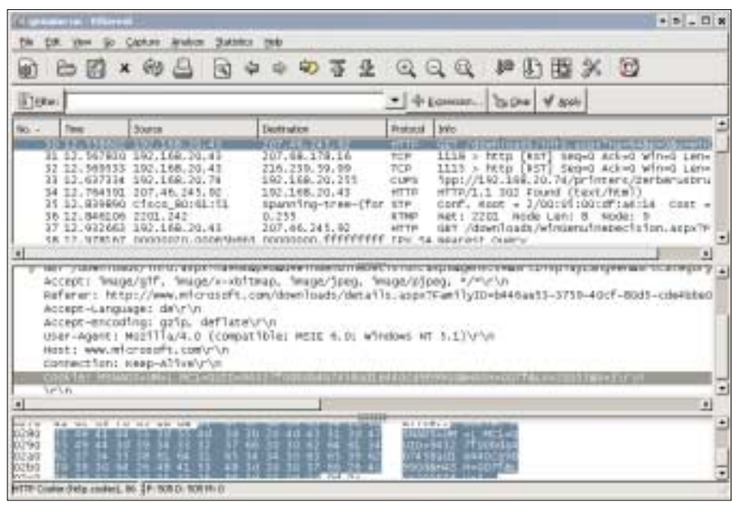
Ethereal potřebuje ke své činnosti nainstalovaný ovladač **Winpcap 3.0**, který rovněž naleznete NA NAŠEM CD. Jak Ethereal, tak Winpcap se instalují bez problémů. Vzhledem k tomu, že Ethereal je utilita pocházející původně ze světa Linuxu, je její menu uspořádáno poněkud jinak, než jak je většina z nás zvyklá.

Sledování síťového provozu se spustí přes menu *Capture/Start*. Objeví se dialogové okno, v němž si můžete pod položkou *Interface* vybrat síťový adaptér, jehož provoz chcete sledovat.

Pokud se připojujete k internetu pomocí modemu či ISDN linky, vyberte položku *PPP-Adapter* (pouze ve Windows 98/ME). Pokud máte v seznamu dva PPP adaptéry a ani s jedním Ethereal nepracuje, pak je potřeba v Ovládacích panelech poklepat na ikonu *Síť* a odstranit položku *Telefonické připojení sítě#2*, neboť pro připojení k internetu stačí nainstalovat pouze jeden adaptér pro *Telefonické připojení sítě*. Pak by měl Ethereal již pracovat bez problémů – to se projeví tak, že se v hlavním okně aplikace začnou objevovat všechny datové pakety, které přes vaše síťové rozhraní procházejí.

Standardně Ethereal zobrazuje všechna data, která váš počítač odesílá a přijímá. Proto doporučujeme kvůli větší přehlednosti ukončit všechny programy, které přistupují k internetu, a nechat spuštěny pouze ty, jejichž činnost chceme analyzovat. Ovšem upozorňujeme rovnou, že pro získání nějakých relevantních informací je třeba vynaložit hodně úsilí, mít značné detektivní vlohy a hlavně se obrnit velkou dávkou trpělivosti.

5 0455/OK ❑



▲ **Sledování síťového provozu: prostřednictvím Etherealu můžete sledovat veškerý síťový provoz, který probíhá mezi vaším počítačem a okolím. Pokud však komunikace probíhá šifrovaně, pak z těchto dat stejně nic nevyčtete.**