Jak uniknout digitálním slídilům

Velký bratr se dívá – a přesto nic nevidí. Pomocí našich triků a nástrojů totiž dokážete zmařit všechny snahy státu o vyčenichání vašich dat či identity. *Andreas Hentschel, autor@chip.cz*

V tomto článku najdete

Proč máte doma v oknech záclony? Cožpak musíte něco skrývat? Samozřejmě že ne. Závěsy vás chrání jenom před zvědavými pohledy zvenčí. Záclona, každým respektovaná, nikým nezpochybňovaná, tak představuje jakýsi počátek veškeré ochrany údajů. Je naprosto nemyslitelné, že by bylo možné zakázat záclony zákonem. A přesto se už něco takového děje – byť v přeneseném slova smyslu.

Co nás nemine

Když brouzdáte po internetu, telefonujete, posíláte SMS, rezervujete si letenku nebo nakupujete se svou platební kartou, už je záclona o hezký kus poodhrnuta. Státní úřady vám nahlížejí přes rameno – a brzy tak asi budou činit ještě důkladněji. Zřejmě není daleko doba, kdy se i u nás dramaticky posílí státní kontrolní kompetence. V sousedním Německu už se na takových opatřeních pilně pracuje. Jejich výčet není právě zanedbatelný: od 1. ledna 2008 se například spouští paušální sledování komunikace občanů. Kdo s kým a jak dlouho telefonoval, komu posílal e-maily, jak dlouho byl na internetu, to všechno se bude preventivně ukládat po dobu šesti měsíců.

Česká realita

Zdá se vám to absurdní a myslíte si, že se to u nás stát nemůže? Pak vám doporučíme text „Vyjednávání evropské legislativy o povinnosti operátorů a providerů uchovávat data o komunikaci svých klientů“, který najdete na **www.iure.org/539449**. Další překvapení čeká leckoho v archivu veřejných zakázek. Pod číslem 60004075 se skrývá „Systém pro monitoring internetu“, který zcela určitě přispěje k také zmiňovanému účelu „Posílení kapacity české policie v boji proti korupci a hospodářské kriminalitě“.

To všechno mohou být brutální zásahy nejen pro náruživé ochránce osobních údajů. Stále silněji kontrolujícímu státu však tak

9 ŠPIČKOVÝCH PROTI-ŠPIONÁŽNÍCH NÁSTROJŮ

Všechny programy zmíněné v tomto článku najdete na Chip DVD v rubrice Testy a praxe.

Najdete na Chip DVD

1. **Torpark**
   Browser založený na Firefoxu
2. **Souprava Tor & Privoxy & Vidalia**
   Anonymizér s blokováním reklam
3. **JAP**
   Brouzdejte internetem nepoznáni
4. **Cookie Cooker**
   Konec se špionáží pomocí cookies
5. **GnuPG**
   Šifrování mailů a dat
6. **TrueCrypt**
   Udělá z pevného disku datový trezor
7. **Jabbin**
   Messenger se šifrováním
8. **Stealther**
   Doplněk Firefoxu pro zahlazení stop po surfování
9. **Gpg4win**
   Šifrovací program pro e-maily

Docela obyčejné špehování

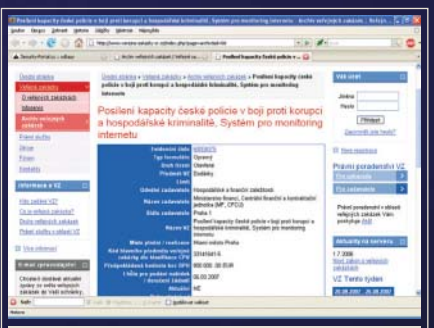
Snad všude na světě projevují státní úřady neuhasitelnou žízeň po vědomostech: na ulici, v letadle, při finančních transakcích – vždy se o vás někde něco zaznamenává. Přinášíme malý přehled, kde všude se o vás každodenně shromažďují nějaké údaje.

■ **Dálniční mýto:** Mýtné brány na dálnicích mají vlastně sloužit jen pro výpočet poplatků pro nákladní automobily. Systém je ovšem schopen registrovat všechna vozidla. Je tedy nepochybně jen otázkou času, kdy se budou i tyto údaje shromažďovat, například pro potřeby kriminalistů.

MÝTNÉ BRÁNY V BUDOUCNOSTI: **Poněvadž dobře funguje rozpoznávání registračních značek, mýtný systém bude brzy registrovat všechna vozidla (a nejspíš jim i měřit rychlost, kontrolovat dálniční známky atd.)**

■ **Elektronický cestovní pas:** V nových typech cestovních pasů bude integrován RFID čip. V něm může být kromě základních údajů uložena i biometrická pasová fotografie a otisky prstů.

■ **Data z letecké dopravy:** O každého, kdo nastoupí do letadla, se zajímají americké tajné služby. Mezi EU a USA proto existuje zvláštní ujednání: jména a adresy svých pasažérů odesílají všechny evropské aerolinky rovnou přes Atlantik. A nejen to – také informace o tom, jak jste letenku rezervovali a platili a zda jste měli speciální přání při výběru občerstvení...



ČESKÁ REALITA: **Přinese „Systém pro monitoring internetu" více bezpečí?**

→ docela bezbranně vydáni všanc nejste. Chránit se můžete úplně stejně jako před profesionálními sběrateli dat a internetovými reklamními agenty, kteří se z údajů o vás snaží vytěžit nějaký zisk. Nabízíme vám několik triků, které vám pomohou se před zvídavými pohledy ubránit.

Informace, které zde najdete, jsou jen zlomkem možností, které můžete k ochraně svého soukromí použít. Zkušenějším uživatelům se znalostí anglického jazyka lze doporučit adresu **http://freehaven.net/anonbib/topic.html**, kde najdou celou řadu návodů a informací na toto téma. Česky mluvícím surfařům lze doporučit adresu **http://security-portal.cz**, kde najdou nejen informace o bezpečnosti, ale i o zmiňované anonymitě. Server se vyplatí navštívit už jen kvůli šikovným odkazům na seznam proxy serverů…

ŠIFROVÁNÍ

Datoví špioni bez šance

V našem všednodenním životě mají klíče své pevné místo – zásuvku psacího stolu zavíráme, dokonce i když je v ní třeba jenom propiska. Na svá data jsme daleko méně opatrní, ta často necháváme ležet na pevných discích nebo v USB „klíčenkách" bez jakéhokoliv zajištění. To je ale poměrně nebezpečné: jednak proto, že spousty trojských koní neustále pasou po heslech a transakčních číslech on-line bankovnictví, jednak proto, že drobná „fleška" se snadno ztratí – a všechna na ní uložená data si může kdokoli přečíst.

Skutečnost, že přesto jen málokdo svá data šifruje, má nejspíš na svědomí pojem „kryptografie", který zavání režimem příkazového řádku a pracně zadavatelnými příkazy. To je však pouhý předsudek. Například nástroj TrueCrypt (na Chip DVD) vaše data zašifruje po stisku tlačítka. Přitom je praktické, že v režimu „Traveller Mode" můžete program spouštět i z USB paměti. Pod Windows XP k tomu ovšem potřebujete oprávnění správce.

Při šifrování nástrojem TrueCrypt si můžete vybrat, zda chcete zašifrovat kompletní diskový oddíl, nebo vytvořit tzv. kontejner. Jak to podrobně funguje, to si přečtete v manuálu k programu – „pédéefko" v angličtině najdete po instalaci ve složce „Setup".

Na výběr jsou v principu dvě možnosti. V prvním případě TrueCrypt nově zformátuje kompletní logickou jednotku a pak při každém přístupu do ní běží paralelně →

BEZ REKLAM: **Browser Torpark vám nejen zajistí anonymitu, ale také vás zbaví reklamních bannerů.**

→ na pozadí. Tak sice ochrání kompletní obsah diskového oddílu před zvědavci, v praxi to má však i nevýhody: již existující oddíl nelze dodatečně zašifrovat, neboť při přeformátování by se všechna data ztratila – z tohoto důvodu je tabu také systémová partition. Druhým nedostatkem je skutečnost, že aplikace využívající zašifrovaná data běží pomaleji, neboť po jejich spuštění musí TrueCrypt nejprve všechny soubory dešifrovat, aby k nim mohl korektně přistupovat operační systém.

Druhou možností je praktičtější práce s „kontejnery". Zde TrueCrypt nejprve založí virtuální jednotku, v níž leží všechna zašifrovaná data. Tato jednotka se operačnímu systému jeví jako zcela normální soubor, který můžete libovolně nazvat a ukládat. Má-li do ní ukládat nebo z ní načítat data, TrueCrypt jednotku připojí. Ta je pak v Průzkumníku označena vlastním písmenem a můžete do ní přesouvat nebo v ní mazat data stejně jako u každé jiné jednotky. Šifrování a dešifrování přitom automaticky přebírá TrueCrypt na pozadí. Při práci s malými soubory, například dokumenty Wordu, si toho ani nevšimnete.

ANONYMNÍ SURFOVÁNÍ

Cestování po webu s utajenou identitou

Paradox: Anonymita na internetu je pouhá iluze – a přesto můžete zůstat nepoznáni. Zrádná je IP adresa, kterou vám přidělí váš provider, jakmile se přihlásíte k internetu – a která zřejmě bude providerem v budoucnu na určitou dobu ukládána. Která místa jste navštívili, to ovšem poskytovatel neví. Vaše cíle na webu lze vystopovat jenom z log souborů na serveru, v nichž jsou vyvolané stránky zaprotokolovány. Pouze ten, kdo má možnost tyto informace propojit s údaji zaznamenanými poskytovatelem připojení, dokáže zjistit vaše jméno – přinejmenším teoreticky. V praxi totiž můžete řetěz IP adres přerušit a zjednat si tak alespoň jistou míru anonymity.

Využívání hotspotů: Téměř anonymně lze brouzdat po webu s notebookem v nějakém bezplatném veřejném hotspotu bez registrační povinnosti. Zde surfujete pod IP adresou provozovatele hotspotu, který vás přitom ale nezná. Přehled takovýchto míst s bezdrátovým přístupem najdete na webové stránce **http://wifi.lupa.cz/** (pro ČR) nebo **www.hotspot-locations.de** (pro Evropu i svět).

Jedinou stopou, kterou po sobě při přihlašování zanecháte, je MAC adresa vašeho notebooku, tedy něco jako DNA u člověka. Aby se podle ní dal identifikovat majitel přístroje, znamenalo by to masové „genetické" testování veškerých notebooků – což je představa naprosto absurdní. Hotspotové řešení má ovšem zřejmou nevýhodu: nebydlíte-li v dosahu veřejné WLAN, musíte kvůli každé návštěvě internetu opustit domov.

Anonymizéry: Pohodlněji můžete zastřít svou totožnost pomocí proxy serveru. V protokolech webových serverů pak už nefiguruje vaše IP adresa přidělená poskytovatelem připojení, ale třeba adresa nějaké univerzity v Americe. Ale pozor! Nepřepojujte svůj prohlížeč manuálně na ledajaký volný proxy server, který jste nalezli na Googlu. Pokud nevíte, je-li jeho provozovatel dostatečně důvěryhodný, raději se takovému serveru vyhněte.

Důvěřovat můžete anonymizačním nástrojům Tor a JAP – oba najdete na Chip DVD. Také to jsou v podstatě proxy, ovšem s vysokou úrovní bezpečnosti. Tak například Tor směruje všechny požadavky na stránky a na zpáteční cestě jejich data zašifruje náhodně zvolenou trasou (posloupností serverů). Jelikož každý server zná jenom svého přímého souseda a posloupnosti serverů se neustále mění, v praxi nástroj zajišťuje dostatečnou míru anonymity. Pod názvem Torpark jsme pro vás na Chip DVD nahráli i (na Firefoxu založený) browser s integrovaným Tor klientem, který navíc blokuje reklamní bannery.

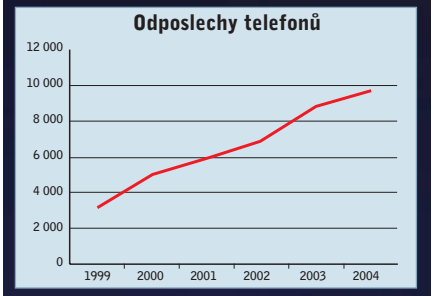
Trochu jinak než Tor pracuje JAP: klient projektu AN.ON Technické univerzity v Drážďanech se ve vašem počítači nainstaluje jako proxy a datový provoz vede přes tzv. smíšené kaskády. To jsou za sebou seřazené servery, v nichž se – velmi zjednodušeně řečeno – datové proudy zašifrují a navzájem promíchají. Pokud se na této mixáži podílí dostatečný počet uživatelů, na výstupu už nelze zjistit, který požadavek na stránku pochází od kterého uživatele.

Blokování cookies: Ani ta nejefektivnější anonymizace není nic platná, když ve vašem počítači uložené cookies prozradí, kdo jste. Nejjednodušší řešení – zákaz cookies – ale bohužel silně omezuje surfovací komfort. Lepší je proto nasadit inteligentní správu cookies: použijte k tomu Cookie Cooker z Chip DVD, který vám pro ukládání cookies umožní definovat individuální pravidla.

Odposlechy „stále populární"

Odposlouchávaná telefonní spojení

Rok	GSM	Pevná síť	Celkem
1999	n/a	n/a	3116
2000	4030	989	5019
2001	5258	649	5907
2002	6527	403	6930
2003	8405	439	8844
2004	n/a	n/a	9660



Tabulka ukazuje data pouze do roku 2004, pak došlo ke změně metodiky měření počtu odposlechů. Poté došlo k mírnému poklesu na cca 7700.
Viz: **www.mvcr.cz/zpravy/2007/odposlechy/analyza.pdf**

Zdroj: www.mvcr.cz/2003/aktualit/2004/1027pp_policie.html

ELEKTRONICKÁ POŠTA

Bezpečné zprávy bez odesilatele

Ukládání informací o tom, s kým si kdo vyměňoval e-maily, se dříve či později asi dočkáme i u nás. A na základě soudního rozhodnutí jistě budou vyšetřovatelé moci elektronickou poštu i číst. Následující triky jim to však dokonale znemožní.

Anonymní poštovní účet: Poslat anonymní e-mail je dnes už stejně jednoduché jako poslat anonymní dopis. Dokonce i u vyhlášených freemailových služeb jako Seznam nebo Google si můžete zřídit účet, aniž byste museli prozradit své jméno. Problémem není ani druhý účet vedený pod pseudonymem. Pokud z tohoto účtu nepřenášíte došlé zprávy lokálně do svého →

Jak chránit svá data

Nezřídka bývá samotný uživatel PC právě tím největším šiřitelem údajů o sobě samém. S následujícími jednoduchými triky už toho o sobě tolik neprozradíte.

- **Zvýšit úroveň zabezpečení:** V Internet Exploreru je úroveň zabezpečení standardně nastavena poněkud nízko. Klikněte proto na *Nástroje* | *Možnosti Internetu* | *Zabezpečení* a posuvník přesuňte nahoru na úroveň „Vysoká". Tak například zablokujete cookies z webových stránek bez směrnice ochrany dat.
- **Vypnout samočinné doplňování hesel:** Automatické vyplňování uživatelských jmen a hesel je velmi pohodlné (ale také nebezpečné). Pokud není možné toto nastavení chránit centrálním heslem, nedoporučujeme jeho použití…
- **Vymazat historii:** V každém prohlížeči můžete jedním či dvěma kliknutími myší odstranit stopy po svém surfování. Pokud tak neučiníte, všechny dříve navštívené webové stránky zůstanou kompletně uloženy v lokální cache.
- **Nežvanit:** Sítě jako Lidé.cz nebo Nyx.cz slouží k navazování kontaktů a sdílení informací milionům účastníků. Nebuďte však příliš sdílní! Celá řada uživatelů používá tento typ sítí jako zdroj zneužitelných informací.
- **Různá uživatelská jména:** Pro každou webovou službu volte jiné uživatelské jméno. Jinak může čtenář vašeho oblíbeného fóra rychle zjistit, co právě prodáváte v internetovém bazaru.

LEPŠÍ OCHRANA: **Úroveň zabezpečení standardně nastavenou v Internet Exploreru raději zvyšte.**

→ poštovního programu, k webovým mailovým službám se přihlašujete anonymně a maily píšete výlučně on-line, těžko vás někdo dokáže identifikovat.

Tip: Poněvadž většina freemailových služeb ve vašem počítači zanechává cookies, měli byste používat již zmiňovaný nástroj Cookie Cooker. V poštovním programu Thunderbird také můžete zprávy posílat a přijímat přes anonymizující síť Tor, pokud si nainstalujete plug-in Torbutton (**https://addons.mozilla.org/cs/firefox/addon/2275**). Pro jistotu však připomínáme, že použití tohoto doplňku má smysl jen tehdy, pokud vaše mailová adresa rovnou neprozrazuje, kdo jste.

Šifrování mailů: Není samozřejmě nutné šifrovat každou soukromou zprávu přátelům a známým. Avšak v případě důvěrných sdělení advokátům či firemním partnerům byste na tuto ochranu rozhodně neměli zapomenout. Svou elektronickou poštu můžete zašifrovat programem Gpg4win (na Chip DVD). Nástroj používá otevřený standard GnuPG, který zprávy šifruje dvěma klíči – veřejným a privátním. Když napíšete zprávu, GnuPG její obsah zašifruje veřejným klíčem příjemce a vaším privátním klíčem. Dešifrovat ji pak může jenom příjemce svým privátním klíčem. Takto zašifrované maily nemůže na přenosové cestě číst nikdo třetí, neboť mu chybí →

TELEFONNÍ ZPROSTŘEDKOVATEL:
Telefonáty uskutečněné prostřednictvím webové služby Jajah nelze zpětně vystopovat.

→ příslušný privátní klíč. Zašifrovaná zpráva je bezpečná před nežádoucím přístupem i tehdy, je-li uložena v lokálním počítači. GnuPG funguje s poštovními programy Outlook, Outlook Express, Thunderbird, Eudora a Pegasus. „Windows Mail" integrovaný ve Windows Vista však GnuPG nepodporuje.

TELEFONOVÁNÍ

Snadná obrana proti odposlechu

Pokud jde o telefonování, i tady projevují některé státy značnou zvídavost a mnohé ukládají údaje o uskutečněných spojeních. U mobilních telefonů to jde dokonce ještě dál: operátoři jsou nebo brzy budou povinni protokolovat, z které telefonní buňky účastník se svým mobilem telefonoval. Tak bude nejen lokalizovatelný, ale bude dokonce možné sestavit kompletní profil jeho pohybů.

Voice over IP: Pokud svou telefonickou komunikaci prostě přenesete na internet, pak seznam vašich hovorů u O2 zůstane prázdný. To ale automaticky neznamená bezpečí…

Všichni větší internetoví poskytovatelé již dnes nabízejí softwarové telefony, jimiž se dá „voipovat" prostřednictvím náhlavní soupravy. Už i takováto spojení se dají rekonstruovat jen s nejvyšším úsilím – pracným skládáním všech IP adres, které se na komunikaci podílely. Pokud přejdete k mezinárodnímu poskytovateli, jako je Skype, bude to ještě obtížnější. A svou anonymitu můžete ještě dále prohloubit: se svým partnerem se po internetu můžete spojit také prostřednictvím webové služby Jajah (**www.jajah.com**). V protokolu spojení se pak namísto jeho telefonního čísla objeví jen nic neříkající číslo služby Jajah.

Mobilní telefon: Mobily jsou přímo rozsévači údajů o vaší osobě – a to i když vůbec netelefonujete. Přijde doba, kdy váš operátor bude muset protokolovat, ve kterých GSM buňkách se nacházíte – bez ohledu na to, zda telefonujete, nebo ne. Proti takovému špehování pak už pomůže jen jediné: mobil vypnout a zapínat ho, jen když chcete telefonovat. Účinná je samozřejmě také velmi prostá metoda – používat předplacené mobily bez smlouvy. Pak se totiž vašemu telefonnímu číslu nedá automaticky přiřadit jméno a prakticky zůstáváte v anonymitě.

VÝMĚNA DAT

Legální filesharing pro pozvané

Bezpečnostní složky vyspělých zemí své občany neustále ujišťují, že jejich sledovací protokoly poslouží jen k odhalování teroristů a těžkých zločinců. Je však mnoho oprávněných důvodů k obavám, že tato opatření mohou být snadno použita také k jiným účelům. Například zmiňované protokoly providerů mohou vyvolávat „žádostivost" hudebního a filmového průmyslu, který se živě zajímá o informace, kdo se kdy napojil na nějakou výměnnou burzu.

Legální sdílení souborů: Tomuto obecnému podezření se můžete vyhnout velice snadno. Ke sdílení hudby, videí a obrazů používejte vlastní výměnné platformy jako Service Pownce (**www.pownce.com**). Na rozdíl od burz typu eDonkey zde své obsahy poskytujete jen těm uživatelům, které jste výslovně pozvali – nikdo jiný tyto soubory stahovat nemůže. Pokud takto autorizujete skutečně jen několik známých či příbuzných, rozšiřujete de facto privátní kopie – a to je dovoleno.

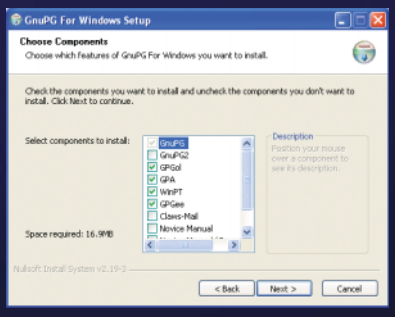
Anonymní výměnné burzy: Nejznámější a nejoblíbenější filesharingový systém BitTorrent můžete rovněž využívat prostřednictvím sítě Tor. Doporučit to však nemůžeme: uživatelé Toru už tak jako tak trpí pomalým spojením, a pokud by měl takto běžet celý datový provoz výměnné burzy, systém by se dostal na pokraj kolapsu. ANts P2P a Mute jsou další výměnné sítě, které své účastníky poměrně spolehlivě drží v anonymitě. Ovšem i zde je spojení mimořádně pomalé.

Andreas Hentschel

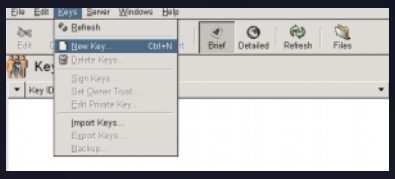
WORKSHOP

Šifrování e-mailů

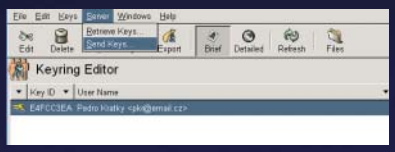
Chcete své elektronické dopisy uchránit před zvědavými pohledy? Pak tu pro vás něco máme. Z Chip DVD si nainstalujte software Gpg4win. Po několika kliknutích budou vaše maily v bezpečí.



1 Generování klíče: Spusťte „GNU Privacy Assistent", klikněte na *Keys | New Key* a pak zadejte jméno a mailovou adresu, pro které má klíč platit. Zvolte heslo a akceptujte doporučení, abyste si uložili kopii klíče – nejlépe do USB paměti.



2 Zveřejnění Public Key: Kdo vám chce poslat zašifrovaný mail, potřebuje váš veřejný klíč. Klikněte na *Server | Send Keys*, načež bude tento klíč poslán na předem nastavený klíčový server. Standardní klíčový server můžete změnit prostřednictvím *Edit | Preferences*.



3 Nastavení Outlooku: Plug-in GPGol, který se zároveň nainstaloval, samočinně začlení GnuPG do Outlooku. V případě potřeby můžete změnit nastavení pod *Nástroje | Možnosti* na nově zřízené záložce „Gnu PG". Standardně se zašifrovávají všechny nově napsané maily.