Jak se po internetu pohybovat beze stop

Anonymní surfování

Kdykoli surfujete po internetu, zanecháváte za sebou stopy. Pokud si jich všimne někdo s nekalými úmysly, může se váš počítač ocitnout v ohrožení spywarem, spamem a nebezpečnými skripty. My vám ukážeme, jak se ve virtuálním světě účinně maskovat.

Internet používá odhadem asi 700 milionů lidí. Jste na omylu, pokud si myslíte, že se v této mase lidí pohybujete zcela anonymně. Při surfování totiž za sebou zanecháváte stopu, která vás může prozradit. Dokonce i váš prohlížeč ochotně sděluje podrobnosti o nastavení vašeho systému a pochlubí se klidně i tím, z jaké internetové stránky přicházíte a co jste právě hledali na Googlu. Podle vaší IP adresy vás může kdokoli jednoznačně identifikovat. Před tím vás sice chrání zákon na ochranu osobních dat, ale před sběrači dat, které používají internetoví obchodníci a inzerenti, se musíte chránit sami. V následujícím článku se dozvíte, kdo jaká data shromažďuje a jak se proti tomu můžete bránit.

SPYWARE, COOKIES A SPAM: ZAVŘETE PŘED SBĚRAČI DAT BRÁNU NA PETLICI

Na mnoha internetových stránkách platíte už za starého známého. Poznáte to například tak, že když se přihlašujete ke zvolenému účtu, objeví se automaticky vaše uživatelské jméno (například Amazon a spol. vás pozdraví vaším jménem). Takováto pozornost patří ještě k těm neškodným funkcím tzv. user trackingu, tedy protokolování a vyhodnocování uživatelských dat, a málokomu vadí.

Mnohem horší však je, když se poskytovatelé internetové reklamy vydají na lov pomocí cookies a spywaru. Bez vašeho souhlasu se celkem snadno dozvědí, jaké jsou vaše oblíbené stránky, co jste naposledy kupovali přes internet a jaký máte hardware a software. Z takto získaných údajů pak marketingové firmy, které působí po celém světě, vytvářejí podrobné profily uživatelů. A pak váš monitor začnou zaplavovat reklamní bannery s více či méně vhodnými nabídkami.

Při surfování po internetu se vyměňují a ukládají nejrůznější data, aniž byste si toho vůbec všimli. Server, na kterém je uložena stránka, kterou si na svém monitoru zobrazíte, se podle vaší IP adresy dozví, z které země pocházíte a kdo vám poskytuje připojení. V každém požadavku serveru jsou navíc skryty i údaje o vašem prohlížeči a operačním systému, o nastavení počítače a o tom, jakou internetovou stránku jste navštívili předtím. To ale není všechno. Velmi pravděpodobně uloží server na váš pevný disk cookie, aby v budoucnu věděl, jak jste se při minulých návštěvách na internetové stránce chovali. Nejvyšší čas přestat o sobě prozrazovat i to, co nemusíte.

SKRYTÍ IP ADRESY

Ve většině případů vám při každém připojení k internetu poskytovatel přidělí novou IP adresu (tedy samozřejmě pokud nemáte pevnou IP adresu). Internetový server si zaznamenává údaje o tom, jaká IP adresa požadovala jaká data. Nezná sice vaše jméno, ale protože si poskytovatel připojení vede záznamy o tom, kdy vám jakou IP adresu přidělil, lze v případě nutnosti snadno zjistit vaši totožnost. IP adresa dokonce omezuje pohyb po síti. Existují totiž internetové stránky, které odmítnou uživatele pustit dál, protože pochází z určité země. Jak se tomu dá zamezit? Surfujte přes proxy server!

IP adresa se nedá vymazat, protože je pro internetovou komunikaci nezbytná. Můžete ji však změnit odbočkou přes proxy server. Proxy server funguje jako mezipaměť. Přijme požadavek prohlížeče na zobrazení určité stránky a předá ho cílovému serveru. Odpověď serveru pak také putuje touto odbočkou. Server se tak nedozví vaši IP adresu, ale pouze IP adresu proxy serveru.

Nástroje pro maskování totožnosti: Připadá vám hledání vhodného proxy serveru příliš složité? Použijte některý z nástrojů pro anonymní surfování, například program Complete Anonymous Web Surfing (www.pcmesh.com) nebo Steganos Internet Anonym Pro (www.steganos.com). Tyto programy směrují požadavky automaticky přes proxy servery a dají se pohodlně a jednoduše ovládat a nastavovat. Bohužel jsou veřejné servery nastavené v těchto programech často přetížené, což snižuje rychlost připojení. Jestliže vás tyto programy zajímají více, určitě se podívejte na jejich "minitest" na straně 32.

BLOKOVÁNÍ COOKIES

Internetové servery neukládají data pouze na svých počítačích, ale dokonce i na vašem. Vytvářejí tzv. cookies, které jsou buď stálé, nebo se po ukončení připojení vymažou. Díky těmto malým textovým souborům vás například server při vaší příští návštěvě pozná. Cookies používají například on-line

obchody, aby vám po připojení mohly nabídnout zboží, které vás bude nejspíš zajímat. Umožňují také automatické přihlašování na stránku. V těchto případech mají svůj smysl a zjednodušují uživateli práci.

Nepříjemné je na nich ale to, že se toho o jejich ukládání a načítání moc nedozvíte. Na disk se uloží, aniž by se vás zeptaly. Také vám nic neprozradí o obsahu, účelu a době uložení. Navíc je na váš disk ukládají i servery s reklamními bannery. Protože se tyto reklamní bannery vyskytují na tisících internetových stránek, může se příslušný server snadno dozvědět, kde se po internetu pohybujete a co tam děláte. Této metodě sledování uživatele se říká user tracking. Pokud se pak ještě podaří propojit získaná data s osobními údaji, může to mít pro vás velmi nepříjemné následky.

Cookies se nedají jen tak jednoduše zablokovat. Pokud je úplně zakážete, znemožníte si zároveň přístup i na stránky, které jsou neškodné a které potřebujete. Nedostanete se pak třeba na svůj účet u eBay nebo do své poštovní schránky u Yahoo.

Existuje však několik metod, které vám pomohou získat nad cookies kontrolu...

Filtr cookies v prohlížeči. Novější verze běžně používaných internetových prohlížečů obsahují filtr cookies, který si může uživatel sám nastavit. Jakmile se server pokusí uložit cookie na váš disk, můžete mu to buď povolit, nebo zakázat. Prohlížeč si navíc nastavení pamatuje a také je obvykle možné vytvořit seznam serverů, které mohou cookies používat...

Mazání uložených cookies. Co ale dělat s cookies, které už máte na disku? Vymazat! V nabídce Internet Exploreru klikněte na "Nástroje", vyberte "Možnosti internetu" a klikněte na "Vymazat soubory cookie". Po tomto zásahu vás na žádném serveru nepoznají. Abyste odstranili všechny stopy beze zbytku, vymažte ještě soubor INDEX.DAT, do kterého si Windows zaznamenávají všechny přijaté datové pakety. Operační systém tento soubor chrání, a tak budete potřebovat nějaký vhodný nástroj, abyste ho mohli vymazat. Lze použít například TIF-Loscher, o němž jsme se zmiňovali v minulém čísle Chipu...

Při startu systému vytvoří program nový prázdný soubor INDEX.DAT a tím zamete i poslední stopy po cookies. Máme pro vás i malý trik: Pokud budete chtít blokovat cookies v budoucnu, můžete u souboru INDEX.DAT nastavit ochranu proti zápisu. Vyhledejte soubor v adresáři "Documents and Settings\[vaše uživatelské jméno]\Cookies". Pravým tlačítkem klikněte na symbol složky Cookies a ve "Vlastnostech" zaškrtněte "Jen pro čtení". Prohlížeč pak už nebude moci do souboru INDEX.DAT zapisovat. Počítač bude serveru předstírat, že cookie uložil na pevný disk. Vy můžete surfovat po internetu bez omezení a vaše chování už nikdo nebude sledovat.

IDENTIFIKACE PROHLÍŽEČE

V každém dotazu na internetový server posílá prohlížeč v hlavičce HTTP požadavku tzv. identifikaci prohlížeče. Internetový server se tak dozví, jaký prohlížeč a operační systém používáte, kterou máte verzi HTML a jak máte systém nastavený - včetně toho, zda máte povoleny cookies a Java skripty. Pokud se na internetovou stránku dostanete přes odkaz, obsahuje hlavička i informaci o tom, kde jste byli předtím.

Blokování identifikace prohlížeče: Údaje v hlavičce HTTP požadavku se nedají manuálně odstranit, lze je pouze změnit. K tomu potřebujete nějaký nástroj pro anonymní surfování. Význam těchto údajů ale není třeba přeceňovat. Podle informací o používaném internetovém prohlížeči vás ještě nikdo nemůže identifikovat. Potlačení identifikace prohlížeče může být v některých případech i na škodu, protože některé servery dokáží podle těchto údajů zobrazit verzi optimalizovanou pro váš prohlížeč.

Blokování odkazovače: Odkazovač (angl. referrer) používají provozovatelé internetových stránek ke statistickým účelům. V prohlížeči Opera se dá vypnout, Mozilla Firefox a Internet Explorer takovou možnost nenabízejí. Odkazovač sám o sobě až tak velkou hrozbou není. Většina provozovatelů internetových stránek tyto údaje používá pouze k tomu, aby zjistila, kde všude jsou odkazy na jejich stránky.

ANONYMNĚ POSÍLAT POŠTU

Poslat někomu anonym je jednoduché. Poslat anonymní e-mail už tak jednoduché není. Přitom občas potřebujete poslat zprávu, u které nelze zjistit osobní údaje o odesílateli. Anonymní e-maily navíc snižují riziko spamu.

JAK SE VYHNOUT SPAMU

Ten, kdo zadá svoji vlastní e-mailovou adresu například v diskusní skupině Usenet, může ji rovnou věnovat spammerům. Větší úspěch slibuje následující strategie.

Jednorázová adresa proti reklamnímu odpadu: Pořiďte si e-mailovou adresu, kterou použijete jenom jednou. Na internetu najdete takové adresy na www.spamgourmet.com. Nejprve zadáte některou

ze svých skutečných e-mailových adres a pak si vyberete uživatelské jméno. Když pak budete na nějaké internetové stránce vyzváni, abyste zadali e-mailovou adresu, vytvoříte falešnou v tomto tvaru: slovo.x.uživatelské_jméno@spamgourmet.com. "Slovo" může být jakékoli slovo, "x" označuje počet od 1 do 20, "uživatelské_jméno" je vaše uživatelské jméno pro přístup ke službě Spamgourmet. Číslo x vyjadřuje, kolik e-mailů má být doručeno na vaši skutečnou e-mailovou adresu. Všechny další e-maily se jednoduše smažou.

POSÍLÁNÍ POŠTY BEZ ODESÍLATELE

Někdy je dobré při rozesílání pošty skrýt svoji totožnost. Bohužel to nejde tak jednoduše, protože hlavička e-mailové zprávy obsahuje údaje, které odesílatele jednoznačně identifikují. Freemailové služby jako např. GMX nelze k anonymnímu rozesílání pošty použít, protože pokud uvedete při registraci nesprávné údaje, porušíte obchodní podmínky. Existují sice servery, které umožňují rozesílání anonymních e-mailů (například www.gilc.org/speech/anonymous/remailer.html), ale na takové e-maily nemůžete přijímat odpovědi.

Anonymní remailery: Tzv. remailerové systémy vymažou odesílatele ze záhlaví zprávy a nahradí ho jinou adresou. K odstranění odesílatele z e-mailové zprávy se používají různé technické prostředky, v principu však všechny vycházejí z jedné metody. Poštovní zpráva se neposílá mezi jednotlivými poštovními servery, ale podobně jako v případě programu JAP přes tři a více mixů. Důležitým předpokladem pro spolehlivost takové služby je prohlášení na stránkách remailerové služby, z něhož se mimo jiné dočtete, že si server neukládá žádné záznamy o datových přenosech. Výběr spolehlivého a důvěryhodného poskytovatele je ale stejně jako u proxy serverů jenom na vás. Zaručeně anonymně pracuje například Hushmail.com, freemailová služba, která kromě anonymizace nabízí i šifrování.

OCHRANA OBSAHU E-MAILOVÉ ZPRÁVY

E-maily se nešifrují, a tak si je může na jejich cestě mezi různými servery kdokoli přečíst, a dokonce je pozměnit.

Šifrování e-mailů: Nejjednodušším způsobem, jak skrýt obsah e-mailu před nepovolanými osobami, je šifrování. Starší poštovní klienti šifrovat neumějí, takže u nich budete potřebovat zvláštní nástroj. Za standard je považován program Pretty Good Privacy (www.pgp.com), který je pro osobní používání zadarmo. Při této metodě se e-mailové zprávy šifrují dvakrát - jednou pomocí veřejného klíče a jednou pomocí soukromého klíče. Třetí osoby, které nemají vhodný klíč, tak nemají prakticky žádnou možnost zašifrovanou zprávu otevřít.

BLOKOVÁNÍ WEBOVÝCH ŠTĚNIC

Webové štěnice jsou obvykle průhledné obrázky ve formátu GIF, které se často ukrývají ve spamových zprávách a nepozorovaně tak "rozesílají" informace. Při otevření takové zprávy se údajný obrázek načte z internetového serveru, ale v e-mailu není vidět. Jaký to má smysl? Webové štěnice ukryté ve zprávě slouží například jako potvrzení pro odesílatele, že si adresát zprávu přečetl. Spammeři tímto způsobem zjišťují, které e-mailové adresy v jejich seznamech jsou ještě aktivní. Štěnice však mohou být ještě zákeřnější. Některé dokáží dokonce načíst cookies uložené na vašem pevném disku. Pokud by pak server mezi nimi našel i svůj vlastní "koláček", byla by to z hlediska ochrany dat přímo katastrofa. K vašemu uživatelskému profilu uloženému na serveru by pak totiž server mohl přiřadit i vaši e-mailovou adresu.

Blokování webových štěnic: Nevyžádanou poštu nikdy neotvírejte. Rovnou ji vymažte. Webové štěnice totiž umějí poslat potvrzení o přečtení zprávy i z náhledu. Jako preventivní opatření doporučujeme nastavit, aby se doručené zprávy zobrazovaly pouze jako textové soubory. Soubor ve formátu HTML, který v sobě může ukrývat štěnice, se pak zobrazí jako příloha. Outlook však toto nastavení umí až od verze 2000. Z tohoto hlediska je bezpečnější například Pegasus nebo Mail v operačním systému Mac OS X. Tyto programy se vás nejprve zeptají, jestli mají stáhnout i obrázky.

HUSHMAIL

ZADARMO, ANONYMNĚ A BEZPEČNĚ

Služba Hushmail umožňuje anonymní posílání šifrovaných e-mailů. Anonymní proto, že k založení účtu nemusíte zadávat žádné osobní údaje. Vyhnete se tak použití komplikovaného remaileru.

DVA KLÍČE PRO VYŠŠÍ ZABEZPEČENÍ

K šifrování e-mailů používá Hushmail standard Open PGP založený na metodě veřejného klíče. Každý uživatel používá dva speciálně pro něj vytvořené klíče - jeden veřejný a jeden soukromý. Veřejný klíč dostanou všichni uživatelé, kteří jsou oprávněni zprávu dešifrovat. Soukromý klíč zůstane uživateli. K zašifrování zprávy použije odesílatel veřejný klíč příjemce. Příjemce ji pak může rozšifrovat jedině použitím svého veřejného klíče.

Hushmail funguje stejně jednoduše jako běžný poštovní program. Můžete ho používat i přes POP3 s Outlookem nebo jiným poštovním klientem. Poněkud náročnější je práce s PGP, protože musíte nejdřív všem příjemcům zprávy poslat veřejný klíč.

Součástí bezplatného účtu u služby Hushmail jsou 2 MB prostoru na disku. Přechod na rozšířený účet Premium nemá smysl. Platí se pomocí kreditní karty, takže uživatel přijde o svoji anonymitu. 2 MB nejsou moc, ale chcete-li účet používat pouze k posílání důvěrné pošty, budou vám určitě stačit.

ANONYMNĚ STAHOVAT DATA

Uživatelé peer-to-peer programů eDonkey, Kazaa a spol. jsou znepokojeni. Už i německé sdružení hudebních vydavatelů si vzalo příklad ze svého amerického protějšku RIAA a podává hromadné žaloby na uživatele P2P v Německu. Služby tzv. file sharingu samy o sobě nelegální nejsou, takže pokud si stáhnete nejnovější distribuci Linuxu, nic vám nehrozí. Jestliže však na váš pevný disk proudí megabyty hudby a filmů, žalobě se zřejmě nevyhnete. Dá se proti tomu něco dělat?

MASKOVÁNÍ IP ADRESY

Nejdůležitější poznávací značkou každého uživatele internetu je pro ochránce autorských práv IP adresa. Bez ní nelze po podání trestního oznámení zjistit pravou identitu uživatele. Trik s proxy serverem většinou nefunguje, protože proxy servery obvykle reagují pouze na dotazy portů, které se standardně používají pro internetové stránky. To znamená, že pokud hledáte soubory ke stažení přes port 6682, proxy server vás dál nepustí. A protože chcete, aby požadovaná data dorazila do vašeho počítače, nemůžete použít ani tzv. IP spoofing, tedy předstírání jiné IP adresy.

Stahování přes proxy server: Připojení přes proxy server, který maskuje IP adresu uživatele, využívá program pro výměnu souborů Earthstation 5 (www.earthstation5.com). Podle zpráv v tisku však provozovatelé programu Earthstation 5 pocházejí z nepříliš důvěryhodného prostředí on-line podvodníků a spammerů, což jednoznačně hovoří proti používání jejich programu.

MASKOVÁNÍ SOUBORŮ

V Německu a ve Spojených státech žalují zájmové svazy hudebního průmyslu především ty uživatele P2P systémů, kteří poskytují ke stažení velký počet souborů.

Šifrování souborů: Příznivce těchto výměnných burz by měl ochránit celkem jednoduchý nápad. Firma Steganos začala nabízet program Secure FileSharing 6 (www.steganos.de). Stojí 25 eur a jeho hlavním úkolem je zašifrovat veškerá data stažená z P2P sítě a uložit je do tzv. sejfu médií. Program Secure FileSharing je určen i pro nováčky, takže sám pozná, jaký program P2P používáte, a automaticky smaže všechny stopy, které po sobě při stahování dat zanechá.

Pocit bezpečí, který svým uživatelům program Secure FileSharing 6 slibuje, se však může rychle rozplynout. Program sice maskuje stahovaná data, ale IP adresu vidí všichni, kdo se do P2P sítě připojí. Podobnou funkci navíc nabízejí i další P2P programy, např. eMule. V nastavení programu si můžete určit, kdo si může prohlížet soubory, které nabízíte. V nabídce "Settings - Files" zaškrtněte položku "Show all offered files" a "Nobody". Nikdo pak už nezjistí, kolik souborů vlastně nabízíte.

JAK SE STÁT NEVIDITELNÝM

Absolutní anonymita existuje pouze v případě, že jsou stahovaná data šifrovaná a posílají se více než jednomu příjemci. V opačném případě by se totiž dal vypátrat cíl přenosu dat.

Aby se cíl přenosu dat nedal tak jednoduše zjistit, provádí Free Network Project (freenet.sourceforge.net) šifrování, stahování a přenos dat najednou. Projekt Freenet, jak je zkráceně označován, ale není klasickou P2P sítí. Jeho programátoři totiž pracují na anonymní náhradě internetu. Na jejich freenetu můžete anonymně publikovat internetové stránky a nabízet soubory ke stažení.

Zní to komplikovaně, ale funguje to docela jednoduše. Pokud chcete stáhnout nějaký soubor přes Freenet, začne se stahovat přes několik dalších uživatelů sítě P2P. Veškerá data jsou šifrována a ukládají se na pevný disk několika uživatelů, takže se už nedá jednoznačně prokázat, který uživatel sítě začal soubor stahovat.

FREENET

Už během instalace se vás Freenet bude ptát, kolik místa na pevném disku chcete dát síti k dispozici. Toto místo je důležité, protože právě ze sdílených megabytů vychází samotná podstata Freenetu. Software přebírá kontrolu nad sdíleným volným místem na disku a ukládá na něj data v zašifrované podobě. Uživatel tedy neví, jaké informace má ve svém počítači. Zároveň ani nemůže nijak zjistit, jaké soubory stahují ostatní uživatelé.

Cesta bitů s neznámým cílem

Stahování dat ze sítě Freenet je maskováno ještě dalším způsobem. Neznámý není jenom obsah datových paketů, ale i cíl, kam mají být pakety doručeny. Jak to funguje? Jakmile požádá uživatel A o určitý soubor, který se nachází na pevném disku uživatele B, netečou požadovaná data přímo od uživatele B k uživateli A, ale oklikou přes počítače několika dalších uživatelů, například uživatelů C a D. Nikdo pak nedokáže určit, zda soubor začal stahovat uživatel B, C, nebo D.

Chcete Freenet vyzkoušet? Nejprve si musíte stáhnout a nainstalovat klienta Freenetu (freenet.sourceforge.net). Na podstránce "Tools" najdete seznam důležitých doplňků, např. Freesite Insertion Wizard (freesites jsou internetové stránky v síti Freenet). Oblíbený je také Freemail. Je to nástroj, který umožňuje posílání a přijímání e-mailů ve Freenetu se všemi výhodami šifrování a anonymity.

Příznivci P2P sítí by měli vyzkoušet nástroj Frost. S tímto chytrým prográmkem mohou ve Freenetu vyhledávat a stahovat soubory.

Andrea Hentschel, Markus Schmidt, autor@chip.cz

WEBOVÉ ŠTĚNICE

Jak pracují tajní čmuchalové spammerů

Jsou neviditelní, ale dokáží napáchat velké škody. Řeč je o webových štěnicích, drobném obtížném hmyzu, který zamořuje internet. Spammeři je do svých e-mailů vpašovávají jako miniaturní obrázky ve formátu GIF. Jakmile otevřete e-mailovou zprávu, načte se obrázek ze serveru. Server tak zjistí, že jste si zprávu přečetli, a spammer ví, že adresa, na kterou zprávu poslal, je stále aktivní. Obrázky bývají do e-mailu vloženy jako odkazy. Teprve po otevření e-mailu se načtou ze serveru odesílatele. Webové štěnice jsou miniaturní obrázky o rozměrech 1 x 1 pixel. Nevidíte je ani v čistě textové zprávě. Při otevření zprávy se na spammerův poštovní server odešle požadavek na stažení obrázku. Spammer tímto způsobem zjišťuje, zda je uložená adresa ještě platná a aktivní.

PROGRAM JAP PRO ANONYMNÍ SURFOVÁNÍ (anon.inf.tu-dresden.de/index_en.html)

SPOLEHLIVÁ ANONYMITA ZADARMO

Nástroje pro anonymní surfování směrují data přes více či méně důvěryhodné proxy servery. Program JAP funguje jinak. Tok dat se dostane přes zabezpečené připojení na servery provozovatele této služby, zakóduje se a předává dál na tzv. mixy. To jsou počítače firem a organizací, které provozovatel služby JAP považuje za důvěryhodné. V nich se doručené datové pakety od všech uživatelů pomocí složité metody promíchají a odešlou přes kaskádu několika počítačů, kde se znovu a znovu míchají.

Teprve poslední mix zná klíč, podle kterého klubko dat zase rozmotá. Kromě mixu tak nikdo nedokáže zjistit, která data pocházejí od kterých uživatelů. Přestože je tato metoda velmi složitá, ovládání programu JAP je relativně jednoduché. Nastavení prohlížeče probíhá automaticky. Pouze pokud se povinně připojujete přes proxy server, musíte zadat jeho adresu manuálně v Možnostech programu.

Míra ochrany: Čím více uživatelů bude program JAP používat, tím vyšší bude anonymita každého z nich a ručička ukazatele se bude vychylovat více doprava.

Pořadí kaskády: Zde se zobrazuje pořadí anonymizačních počítačů. Pořadí může uživatel libovolně měnit.

Možnosti: Pokud je připojení příliš pomalé, můžete v Možnostech najít rychlejší a bezpečnější cestu na internet.

PROXY SERVER

MASKOVÁNÍ IP ADRESY PŘIPOJENÍM PŘES PROXY SERVER

Surfování bez maskování: Jakmile uživatel zadá adresu internetové stránky, předá server poskytovatele připojení požadavek příslušnému internetovému serveru, a to včetně IP adresy uživatele. Internetový server pak požadovaná data pošle přímo uživateli. Surfování s maskováním: Pokud chce uživatel surfovat anonymně, musí zvolit okliku přes proxy server. Ten skryje jeho IP adresu a internetovému serveru s požadovanou stránkou pošle místo ní svoji IP adresu.

MANUÁLNÍ NASTAVENÍ PROXY SERVERU

Chcete-li surfovat anonymně přes proxy server, klikněte v nabídce svého prohlížeče na nabídku Nástroje/Možnosti internetu a v kartě "Připojení" na "Nastavení místní sítě", zaškrtněte "Použít pro síť LAN server proxy" a zadejte IP adresu proxy serveru. Najít nějaký vhodný proxy server není těžké, ale bude vás to stát trochu času. Na internetu sice najdete seznam proxy serverů (např. www.multiproxy.org nebo www.atomintersoft.com), ale tyto servery jsou často přetížené a dokáží vaše připojení výrazně zpomalit, občas až o 75 procent. Doporučujeme proto vybraný proxy server nejprve vyzkoušet.

Ne všechny proxy servery také nabízejí naprostou anonymitu. Některé z nich přidávají do požadavku http proměnnou HTTP_X_FORWARDED_FOR s vaší IP adresou. Jiné sice identifikaci odesílatele blokují, zato si však zaznamenávají veškerý přenos dat.

Proxy servery jsou v seznamech často rozdělovány do kategorií anonymity, např. "Anonymous" nebo "High Anonymity". Toto hodnocení vychází z analýzy datového toku přes proxy server, takže mu můžete důvěřovat. Přesto leží rozhodnutí, který server nakonec zvolíte, pouze na vás. Můžete tak maximálně zjistit, kdo server provozuje (např. na www.hexillion.com).

Jakmile najdete vhodný proxy server, změňte nastavení ve svém prohlížeči. Pokud proxy server podporuje i zabezpečené připojení SSL a protokol ftp pro přenos souborů, nezapomeňte zadat jeho adresu i pro tyto protokoly, jinak o anonymitu přijdete.

OBSAH

Občas slouží osobní údaje i ke kontrole přístupu na internetové stránky. Například program americké televizní stanice Showtimechannel je určen pouze americkým divákům. Všem ostatním se při pokusu vstoupit na příslušné stránky zobrazí lapidární upozornění "These pages are intended for access only from within the United States" ("Tyto stránky jsou určeny k přístupu pouze ze Spojených států"). Co proti tomu můžete udělat, se dozvíte na str. 25.

V rukavičkách zrovna nepracují ani spammeři. Pomocí odkazů skrytých do miniaturních obrázků (tzv. webových štěnic) se například dozví, zda a kdy jste jejich e-mail otevřeli a zda je vaše e-mailová adresa ještě platná. V nejhorším případě mohou spammeři pomocí tohoto triku přiřadit k vaší e-mailové adrese předem sestavený profil uživatele. Jak můžete svoji poštu a poštovní schránku chránit před nepovolanýma očima, se dozvíte na str. 28.

Pokud používáte k výměně souborů nějakou peer-to-peer síť, můžete si být téměř jisti, že vaši aktivitu někdo sleduje a protokoluje, například vydavatelé hudebních nosičů. Služby tohoto typu však nejsou nelegální za podmínky, že stahujete nebo nabízíte soubory, které nejsou chráněny autorským právem, tedy například open source software nebo upoutávky na filmy. Pak na vás nikdo nemůže. Jak se v těchto sítích stát neviditelným, se dozvíte na str. 30.

OCHRANA OSOBNÍCH ÚDAJŮ NA INTERNETU

Když odšroubujete poznávací značku z auta, hrozí vám problémy s policií. Co se však stane, když budete anonymně surfovat po internetu? Zakázáno to není.

Zákon sice dovoluje poskytovateli ukládat údaje o spojení s uživatelem, ty však mohou být využívány pouze k vyúčtování služby a poté musejí být vymazány. V ostatních případech nařizuje zákonodárce "nezískávat žádné osobní údaje, nebo pokud možno co nejméně osobních údajů". Údaje o užívání služby musejí být mimochodem ihned po použití služby vymazány. Někteří poskytovatelé se tím ale neřídí, takže v praxi lze ve většině případů zjistit, kdo a kdy se po internetu pohyboval. Poskytovatelé totiž vedou záznamy o tom, jaká IP adresa byla komu a kdy přidělena. Záznamy na internetových serverech zase obsahují údaje o tom, jaká stránka byla jakou IP adresou požadována. Podle těchto záznamů vás pak může třeba policie celkem snadno najít.