Vaše stopy v síti...

Být anonymní namísto sledovaný: nemusí každý vědět, které webové stránky navštěvujete – úřady, hudební průmysl, zasílatelé nevyžádaných e-mailů... Ukážeme vám, jak se stát na webu neviditelnými. *Fabian von Keudell*

V tomto článku najdete

Rok 1984 měl být teoreticky rokem „Velkého bratra“. Ale to, co George Orwell předvídal pro ony dny, má přijít až nyní, o čtvrt století později. Kroky vedoucí k neustálému monitorování sítě jsou patrné téměř všude, ale nejzřejmější jsou v sousedním Německu. Na základě rozhodnutí tamních zákonodárců je německý internet pod naprostou kontrolou. V případě obvinění mají policie i jiné úřady právo znát všechny detaily o vašem pobytu na internetu. Kontroverzní zákon týkající se „ukládání dat“ nařizuje německým poskytovatelům, aby evidovali „connection data“ po dobu šesti měsíců. Díky nim je pak jednoduché začít vás stopovat z kteréhokoliv daného bodu: z webové stránky, na které jste si četli, ze serveru, ke kterému jste se připojili, nebo ze sítě pro sdílení souborů, kterou používáte. Nemějte ale strach: nemusíte vstupovat do ilegality, abyste se ochránili. Dáme vám „neviditelný plášť“, díky kterému vás na internetu nikdo nevypátrá.

Onen „neviditelný plášť“ je vyroben z několika důležitých pravidel a nastavení pro váš standardní internetový software, jakož i z nástrojů, které roztříští váš „traffic“ na síti a pošle ho přes stovky serverů. To je sice pomalé, ale anonymní a bezpečné. Toužíte-li po vyšší rychlosti, nabídneme vám také nejlepší produkty, které jsou v prodeji. Pomocí linuxové distribuce Phantomix (o které píšeme v jiné části Chipu) pak budete anonymní dokonce i v internetové kavárně. To všechno je způsob, jak zabránit tomu, aby se rok 2008 stal novým „rokem 1984“.

TÉMĚŘ ANONYMNÍ

Jak umlčet browser

Když surfujete, všude po sobě zanecháváte „otisky prstů“ s celou řadou informací. Z technického hlediska jsou některé z nich důležité – jako v případě IP adresy. Avšak

cookies či referery jsou pouze důkazem jasné zvědavosti webových serverů. Zbavte se tedy zbytečných stop!

Cookies

Díky tomuto špehování vědí weboví operátoři, kdo jste a které webové stránky jste již navštívili. To je otravné: tolerantní základní nastavení všech prohlížečů umožňují úschovu těchto datových udavačů, aniž byste byli dotázáni. Je tedy nejvyšší čas tuto situaci změnit.

Internet Explorer: Cookie management v často plísněném IE7 je velmi pokročilý. Microsoft prohlížeč začlenil do nové verze „Platform for Privacy Preferences“ (P3P). Ta běží na pozadí a dohlíží na dodržování práva na soukromí – a povoluje či odmítá cookies. A takto to funguje: P3P je platformou standardizovanou WWW konsorciem pro výměnu informací týkajících se soukromí. Každý webový operátor, který se podílí na P3P, má privacy dohodu o svém serveru.

P3P klient integrovaný v Internet Exploreru si ji přečte a porovná s bezpečnostními požadavky, které jste specifikovali.

Vlastní úroveň soukromí si můžete nastavit pomocí nabídky *Nástroje* | *Možnosti Internetu* | *Osobní údaje*. Naše doporučení: posuvník, který je standardně nastaven na „Střední“, si nastavte na „Vysoká“. P3P privacy požadavky si lze přečíst na adrese **www.w3.org/p3p**.

Firefox: V tomto populárním „open-source“ prohlížeči bohužel nemohou být cookies samostatně zablokovány. Můžete pouze vybírat mezi vším a ničím: v nabídce *Nástroje* | *Možnosti* klikněte na *Soukromí* a zrušte zatržítko u položky „Povolit serverům nastavovat cookies“, abyste je všechny zamítli. Pomocí tlačítka „Výjimky“ můžete specifikovat adresy stránek, ze kterých cookies akceptujete.

Alternativa: cookie management s rozšířením „Remove Cookie(s) for Site“ (**https://addons.mozilla.org/firefox/1595**). Nainstalujte si tento doplněk browseru a při surfování pak na libovolné stránce klikněte pravým tlačítkem do webové stránky a zvolte „Remove Cookie(s) for Site“. Toto kliknutí vymaže všechna data, která si uložila vámi vyvolaná webová stránka.

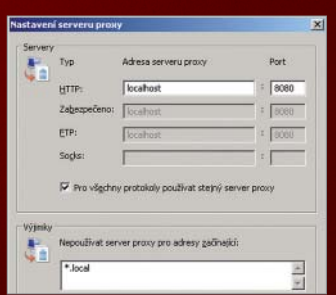
Opera: Jděte do nabídky *Tools* | *Preferences* a klikněte na položku *Cookies* v záložce *Advanced*. Pomocí volby „Accept cookies only from visited sites“ nejprve zablokujte všechna „datová cookies“ reklamních serverů. Pokud máte zásadně něco proti úschově těchto dat, zvolte „Never accept cookies“. Nevýhoda tohoto celkového zamítnutí je však zřejmá – funkčnost celé řady stránek se rapidně změní… Abyste tomu předešli, lze jednotlivým stránkám povolit, aby uchovávaly cookies, a to pomocí příkazu „Manage Cookies“.

Referer

Váš prohlížeč na vyžádání komukoliv v tzv. refereru sděluje informace o operačním systému a podporovaných aplikacích (ActiveX, Java atd.). Jako bonus navíc prozrazuje, které webové stránky jste předtím navštívili. Umlčte tohoto zbytečného žvanila!

IE a Firefox: K utišení refereru v IE a Firefoxu budete potřebovat nástroj Proxomitron, který si lze stáhnout například na adrese **www.buerschgens.de**. Po instalaci ještě bude nutné upravit nastavení prohlížeče: v IE jděte do nabídky *Nástroje* | *Možnosti Internetu* | *Připojení* | *Nastavení místní sítě* a zkontrolujte zatržítko před volbou „Použít pro síť LAN...“. Jako adresu vložte „localhost“ a „8080“ jako port. V nabídce *Upřesnit* aktivujte zatržítko u položky „Pro všechny protokoly použít...“. Ve Firefoxu v nabídce *Nástroje* | *Možnosti* | *Rozšířené* | *Síť* | *Nastavení* aktivujte volbu „Ruční konfigurace proxy serverů“. Zde nastavte jako adresu „localhost“ a „8080“ jako port pro všechny protokoly.

FILTR: Nástroj Proxomitron odstraňuje referery během surfování.



PRŮVODCE: Zde do prohlížeče zadejte adresu pro „přesun provozu“ na anonymní proxy server...

Opera: Pomocí klávesy [F12] otevřete tzv. rychlé předvolby a zrušte zatržítko před položkou „Enable referrer logging“.

IP adresy

Na webu může váš počítač komunikovat s ostatními počítači pomocí IP adresy. Protože poskytovatelé služby zapisují, které IP adresy byly přiděleny kterému uživateli a kdy, lze vystopovat, které webové stránky uživatel navštívil – a to i po uběhnutí několika měsíců.

Existují anonymní proxy servery, které nabízejí (zdarma) zamaskování IP adresy. Tyto servery „odkloní“ váš datový tok a změní tak vaši „viditelnou“ IP adresu.

Je tu však jeden problém: protože se veškerý provoz přesouvá přes jediný „uzel“, tento uzel vás opět může prozradit – pokud jednoznačně nevíte, že jde o spolehlivý server. To opět vrací snahy o anonymizaci na startovní čáru. A to je důvod, proč doporučujeme softwarový anonymizér, jako je JAP.

JAP

Anonymní surfování

Jediné skutečné řešení, které vám zaručí opravdovou anonymitu při surfování, má ale háček: je pomalé. Zatímco při použití proxy serveru probíhá celý data traffic přes jediný uzel, JAP rozseká data do stovek jednotlivých balíčků a pošle je přes různé servery. Výsledkem je rychlost na úrovni ISDN (64 – 128 Kb/s), a to dokonce i původně několikamegabajtovým ADSL. Snažit se připojení zrychlit je zbytečné: JAP stejně nezaručuje nic víc než oněch pomalých 64 Kb/s. To stačí maximálně na prohlížení jednoduchých WWW stránek.

JAP je klientem AN.ON – projektu University of Regensburg a Technické univerzity v Drážďanech. K anonymizaci užívá AN.ON nejméně tři servery jako mix proxy – počítače, které tento mix spravují, jsou důvěryhodné. Každý mix promíchá data v komplikované proceduře, díky čemuž nelze vystopovat, kdo „zažádal“ o jaká data. Dříve než se ale můžete cítit na webu bezpečně, musíte v programu upravit některá nastavení.

Začněte instalací JAP z Chip DVD. Aplikace vyžaduje Java Runtime – ten je již →

Profesionální nástroje: Anonymní a rychlé

Plná ADSL rychlost, a ještě zcela v bezpečí na webu? V současné chvíli je to možné jen prostřednictvím komerčních programů. Výrobci nabízejí své sítě serverů, ke kterým se bezpečně připojujete pomocí sítě VPN. Velkou výhodou je také to, že s těmito produkty fungují sítě pro sdílení souborů (např. i BitTorrent). Jsou zde také znát desítky hodin práce vývojářů – programy nabízí atraktivní rozhraní a snadno se obsluhují.

Anonymní na internetu – VPN

Info:
www.steganos.com
Cena:
80 eur za roční licenci s objemem dat 25 GB

Síťový tunel byl vybudován mezi domácím PC a serverem Steganos přes VPN. Všechny on-line aktivity se odehrávají přes tento tunel. Tunel zakóduje všechny informace pomocí bezpečnostního SSL spojení.

CyberGhost VPN

Info:
www.s-a-d.com
Cena:
70 eur za roční licenci s objemem dat 40 GB

Anonymizační technika v nástroji CyberGhost je úplně stejná jako technika v konkurenčním nástroji od firmy Steganos. I zde výrobci nabízejí svoje servery pro VPN připojení. Software se snadno ovládá a provoz je kódován pomocí 256bitového AES klíče.

ANONYMNÍ: Freeware JAP distribuuje datové toky na různé servery.

na CD integrován a nainstaluje se automaticky. Po nainstalování spusťte nástroj a zvolte „anonymizer server“. To uděláte kliknutím na *Services*, kde ve „Free mix cascades“ zvolíte server – *CCC cascade*. Pak už zbývá jen nastavit váš browser. Vložte údaje pro připojení: „localhost“ a jako port „4001“. Konfigurační stránky prohlížeče najdete zde:

Internet Explorer: Nejprve zkontrolujte, zda je v nabídce *Nástroje* | *Možnosti Internetu* | *Připojení* | *Nastavení místní sítě* aktivováno zatržítko u volby „Use a proxy server for your LAN“. Pak přejděte na kartu *Upřesnit* a zatrhněte zatržítko u položky „Pro všechny protokoly použít...“.

Firefox: V nabídce *Nástroje* | *Možnosti* | *Rozšířené* | *Síť* | *Nastavení* aktivujte volbu „Ruční konfigurace proxy serverů“.

Opera: Označte zatržítko a vyplňte všechny položky v nabídce *Tools* | *Preferences* | *Advanced* | *Network* | *Proxy server*. Tyto položky musíte zadat dokonce i pro FTP připojení!

SDÍLENÍ SOUBORŮ

Anonymní sdílení

Ať jsou tvrzení hudebního a filmového průmyslu jakákoliv, sítě pro sdílení souborů mohou mít i legální obsah. Přesto chcete-li být na té bezpečnější straně, můžete anonymně použít BitTorrent & Co. Je tu však stejný problém s rychlostí.

BitTorrent & Co.

Pro základní anonymitu při surfování stačí použití proxy serveru. Pokud chcete být anonymní i ve výměnných sítích, je situace poněkud jiná. Tyto programy totiž obvykle musí být připojeny přímo k PC a nejsou dovoleny žádné „mezistanice“. Služba SecureIX (**www.secureix.com**) nabízí speciální proxy server, který dobře funguje s sharing nástroji. Má to však dvě nevýhody: první je rychlost 256 Kb/s. Uživatelé, kteří chtějí více, musí měsíčně zaplatit přibližně osm eur. Druhá nevýhoda je závažnější: protože jsou všechna data přenášena pouze přes jednoho providera, může tento provider teoreticky ukládat informace o přenášených datech.

Příští generace

Protokoly výměnných sítí příští generace jsou ale zcela anonymní a bezpečné. Kombinují decentrální síťovou strukturu BitTorrentu s anonymizačními technikami, jako jsou proxy a mixy – a navíc přenášejí data dobrou rychlostí. P2P od ANt (na Chip DVD) je považován za nejbezpečnější. Klient anonymizuje datové toky pomocí důmyslného routovacího systému. Na rozdíl od BitTorrentu zde není „datový tok“ přímo mezi účastníky, ale je veden přes servery. Zasilatel souboru neví, kam je poslán, a zároveň příjemce nemá ponětí o zdroji stahovaného souboru. A to je perfektní neviditelný plášť.

Fabian von Keudell

Jednodušší varianta

Pokud netoužíte stát se na webu zcela neviditelnými nebo dokonale zakrýt stopy své „podvratné“ činnosti, ale chcete jen z různých důvodů změnit svou IP adresu, máme pro vás několik řešení.

Pravděpodobně nejjednodušší možností je použití internetového anonymizéru. To je speciální stránka, kde stačí zadat adresu webu, který chcete navštívit (u pokročilejších ještě označit, které služby a informace chcete povolit), a provozovatel serveru stránku nahraje a „předá“ vám ji. Výhodou je tedy částečná anonymita (záleží na tom, jak důvěřujete majiteli anonymizéru), která pro většinu běžných aktivit naprosto stačí. Takovýchto stránek je celá řada – pro ukázku ale postačí jedna z nejznámějších: **www.anonymouse.org**. Na speciálních webech (**http://anoncheck.security-portal.cz/**) si pak můžete ověřit, jaké informace o sobě prozrazujete.

Druhou variantou je zadání adresy proxy serveru přímo do nastavení vašeho browseru. To je sice na první pohled elegantní řešení, problémem ovšem je, že tyto servery bývají často přetížené a najít fungující a zároveň takový, který vám nesníží rychlost surfování na desetinu, je malý zázrak. Své štěstí můžete zkusit na adrese **www.multiproxy.org**, kde najdete rozsáhlý seznam anonymních proxy serverů.

Dřív než se ale vydáte do anonymních hlubin internetu, promyslete si potenciální rizika. Obvykle totiž platí, že míra anonymity může být přímo úměrná nebezpečí: seriózní provozovatelé anonymizéru jsou relativně snadno donutitelní ke spolupráci (policie, soudy...), s rostoucí anonymitou zároveň roste i riziko kriminálního jednání provozovatele anonymizéru. Navštěvovat svou banku přes bezejmenný ruský anonymizér tedy není zrovna ideální nápad...