Anonymně na webu

Zvoňte na poplach! Hackeři a stále častěji i firmy požadují přesnou informaci **TÝKAJÍCÍ SE VAŠICH SURFOVACÍCH NÁVYKŮ**. S naší pomocí ale můžete i nadále bezpečně posílat poštu a surfovat a zároveň i ochránit svá data...

MANUEL SCHREIBER

Jeli byste na motorce bez helmy? Pravděpodobně ne. Surfování po internetu bez jakéhokoliv „ochranného“ softwaru je však v současnosti stále ještě poměrně běžné. Důvod je zřejmý – v tomto případě nejde o záležitost života a smrti, ale „jen“ o vaše soukromí. Všichni ti, kdo surfují bez ochrany, doslova nabízejí svá data hackerům, reklamním firmám, úřadům a jiným čmuchalům. Kolik uživatelů ví, jak je za pomoci IP adresy, cookies či nastavení prohlížeče snadné zjistit si preference určitého uživatele?

Přitom ochrana soukromí není nijak složitou záležitostí – lze například použít anonymizační software.

Náš srovnávací test vám prozradí, zda vám nejnovější „anonymizéry“ skutečně poskytnou dokonalou ochranu. Navíc se v našem „workshopu“ dočtete, jak šifrovat své maily pomocí klíče, a na DVD najdete jako bonus také náš „protičmuchalský“ balíček.

Technologie: Jak fungují anonymizéry

Ačkoliv jednotlivé produkty používají odlišné technologie, všechny spojuje jedna věc: kdokoliv chce surfovat anonymně, potřebuje anonymní IP adresu.

Zde si uživatel může vybrat mezi třemi metodami: VPN (Virtual Private Network), onion routingem a kaskádovým mixem (viz diagram). V případě VPN si uživatel nejdříve musí nainstalovat softwarového klienta, který se integruje do systému a automaticky „zadrží“ všechny pakety odeslané do sítě. Dotazy tak směřují nejdříve přes šifrovaný tunel na VPN server, a teprve tento server směruje uživatele na příslušné webové stránky – už s novou IP adresou.

VPN servery jsou obvykle extrémně rychlé, ale mají podstatnou nevýhodu: klient musí svému poskytovateli služby důvěřovat. To proto, že ačkoliv uživatel surfuje navenek anonymně, kompletní data o jeho „toulkách“ jsou k dispozici na VPN serverech služby. Pokud se hacker prolomí do tohoto serveru, získá nejen IP adresu uživatele, ale obvykle i celou řadu dalších soukromých informací (například jméno, adresu nebo přístupové údaje k VPN klientu).

Teoreticky to mají lehké i úřady: zákon ve většině evropských zemí nutí providery, aby ukládali data o provozu ve svých sítích. Zda a v jakém rozsahu by to ale mělo být, nebylo dosud jednoznačně vysvětleno. Zajímavý obrat se například nedávno objevil u okresního soudu v německém Bambergu: soud rozhodl, že anonymizační služba nemůže být nucena, aby „bez rozlišení“ vydávala data svých klientů. Výjimku lze učinit pouze v případě nebezpečných trestních činů.

Onion routing, například síť TOR, má zcela jiný princip než zmiňovaná VPN anonymizace. U onion routingu uživatel

NAJDETE NA CHIP DVD

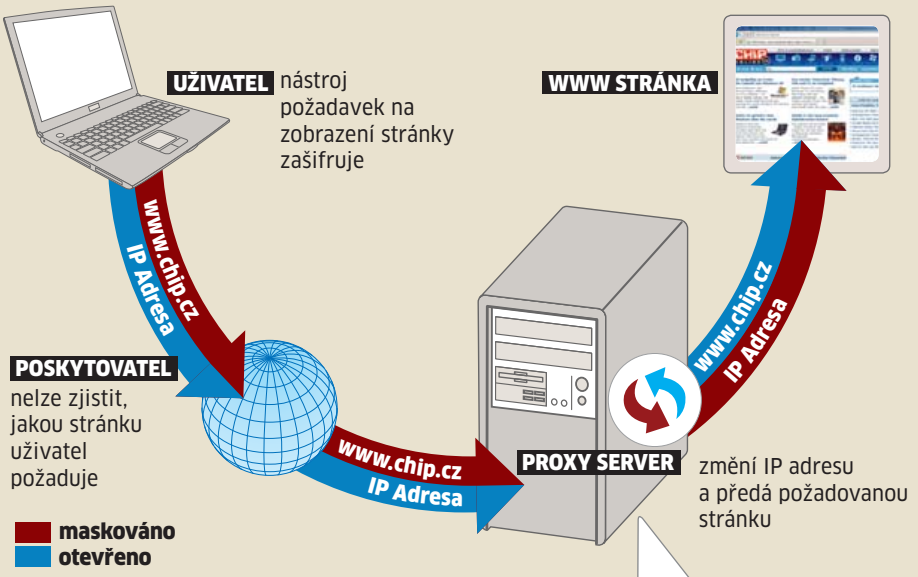
Neviditelné surfování

Mozilla Thunderbird ► alternativní poštovní klient
CyberGhost ► maskuje vaši IP adresu
CCleaner ► čistí zbytečné záznamy v PC
FoxyProxy ► doplněk Tor pro Firefox
Gpg4win ► vytváří bezpečné open PGP klíče
Hotspot Shield ► zabezpečuje Wi-Fi hotspoty
JAP/JonDo ► Anonymizer
JonDoFox ► kompletní ochrana pro Firefox
KeePass ► vytváří bezpečná hesla
Tor & Privoxy & Vidalia ► Anonymizer

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **ANONYM**.

Jak funguje maskování IP adresy

Uživatel se připojí k proxy serveru, kterému předá i svůj požadavek na zobrazení www stránky, server zároveň změní IP adresu uživatele.



ONION ROUTING

V případě této kombinace serverů je požadavek uživatele „veden" šifrovaným spojením tří náhodně zvolených uzlů.

VPN SERVER

Server poskytovatele provede „příkaz k načtení stránky", který obdrží přes zašifrovaný VPN protokol z počítače uživatele.

KASKÁDOVÝ MIX

Uživatel zašle žádost na specifický server a ten ho předá jiným serverům (tzv. kaskádový mix).

nemůže využít jeden konkrétní server, zde se pracuje s více „free proxy servery" (stanicemi) najednou. Například každý webový „dotaz" je zaslán přes několik TOR serverů, které se neustále mění a dotaz přešifrovávají v každé stanici.

Identifikovat určitého uživatele je tak v této síti nemožné – a to i díky kvalitní technologii.

TOR je síť tzv. onion routerů, které mezi sebou sdílejí veřejné šifrovací klíče všech nodů v síti a pomocí asymetrického šifrování si vyměňují dynamicky generované sdílené klíče pro jeden konkrétní řetězec ustavený klientem.

Ale i zde teoreticky existuje několik „zádrhelů": především uživatel nezná osoby stojící za jednotlivými servery. Pravda ale je, že ani pokus o monitorování spojení nevede k získání uceleného profilu uživatele, protože spojení se po nějaké době (nebo po určitém objemu dat) mění. Asi největší praktickou nevýhodou této sítě tak zůstává její rychlost. Chcete-li surfovat anonymně, pak rychle zapomeňte na teoretickou rychlost svého ADSL připojení...

Další (smutnou) nevýhodou je poměrně časté zneužívání sítě stahovači (což vede k rapidnímu zpomalení) a internetovými „výtržníky", což znamená, že celá řada serverů TOR blokuje...

Kaskádový mix funguje podobným způsobem jako onion routing. Jeho využití lze nalézt například v aplikaci JAP/JonDo: uživatel se při surfování pomocí programu připojí k serveru, který zašifruje dotaz a pošle ho na jiné servery (směšovače, označované také jako mix), až doputuje k požadované WWW stránce. V tomto případě ale místo využívání náhodných volných uzlů operátoři používají skupiny serverů. Data všech uživatelů, kteří surfují za použití stejných „mix kaskád“, jsou posílána stejnou cestu. Tímto způsobem lze mixovat datové spojení všech uživatelů, aby se dodatečně zkomplikovalo vysledování konkrétní osoby.

Tato varianta je přibližně stejně rychlá jako síť TOR (zde by se spíš hodilo označení „pomalá“), ale je méně známá a používaná.

Test: Několik kliknutí k neviditelnosti

Přes použití rozdílných technologií jsou naše kritéria pro test všech anonymizérů stejná: klient musí spolehlivě skrýt IP adresu, zabezpečit prohlížeč a mít jednoduché ovládání.

Zvláštní důležitost jsme kladli na rychlost surfování, protože i ta nejlepší ochrana není k ničemu, když se rychlost blíží nule…

V případě programů Steganos, S.A.D. a ArchiCrypt funguje anonymizace zcela automaticky – jednoduše je jen nainstalujte a pak restartujte počítač. Naopak u některých programů jsme museli manuálně zadat nastavení na proxy serveru – a to konkrétně u programů Tor a JonDo Premium. Ve druhém případě to ale příliš obtížné není: JonDo při svém prvním spuštění uživateli ukáže, kde je třeba provést změny. Navíc program nabízí zdarma stažení balíčku JonDoFox. Tento doplněk Firefoxu zahrnuje bezpečnostní nástroje jako Adblock Plus, NoScript a CS Lite, které umožní jednoduché filtrování reklamních bannerů, blokování cookies a deaktivování javaskriptu. Navíc balíček doplňku vytváří ve Firefoxu nový profil uživatele. Při spuštění prohlížeče si tudíž uživatel může pohodlně zvolit mezi svou standardní konfigurací a surfováním pomocí nástroje JonDo. Obecně lze říci, že nastavení všech nástrojů je opravdu jednoduché.

S jistotou na internet: JonDo Premium nabízí několik filtrů. Uživatel si může zvolit, přes které servery chce surfovat.

Důležitou otázkou je, jak anonymně ve skutečnosti surfujeme. Výsledek je zklamáním: ačkoli každý program spolehlivě skryje IP adresu, všechny ostatní informace zůstávají odkryté. Informace o odeslaných datových paketech (jako je použitý prohlížeč, operační systém a nastavení jazyka) lze tudíž přečíst z informací v záhlaví. Zachována jsou i uložená cookies a nová se přijímají bez jakýchkoli námitek. Zkrátka – ukládá se stále ještě velké množství informací, které mohou sloužit k identifikaci počítače a uživatele.

Všichni, kdo opravdu chtějí být při surfování „chráněni“, si musí dodatečně manuálně nakonfigurovat prohlížeč. Bohužel poskytovatelé na to neupozorňují a nenabízí ani žádnou pomoc. Výjimka: Díky doplňku umožňuje JonDo troufnout si anonymně na internet a „cookie-free“ – ale pouze s Firefoxem.

Při používání internetu však není jediným „slabým místem“ browser. Osobní informace mohou být také prozrazeny pomocí nástroje pro práci s torrenty nebo prostřednictvím instatnt messengeru. V této oblasti nabízejí VPN programy rychlou ochranu – navzdory tomu však dopadly v testu různě, a to kvůli odlišnému objemu stažených dat a neustále kolísající rychlosti. TOR a JonDo nabízí podobnou ochranu, uživatel však musí nastavení pro každý program samostatně nakonfigurovat, což může být pro začátečníky dost komplikované.

Slabým místem téměř všech anonymizérů jsou e-maily. Kdokoli používá e-mailového klienta, musí deaktivovat VPN program a v sekci „Exceptions“ zadat URL pro e-mailový server, jinak odesílání pošty selže. Výrobci zkrátka anonymní zprávy nepodporují, především proto, aby eliminovali

INFO

Šifrování a bezpečné posílání e-mailů

S trochou šikovnosti může téměř kdokoliv bez problémů číst nechráněné e-maily. Pokud chcete, aby vaše zprávy dorazily k cíly bez prozkoumání třetí osobou, měli byste každý dopis zašifrovat. To lze udělat několika způsoby – my vám ukážeme, jak to lze provést s balíčkem Gpg4win, který najdete na našem DVD. Prvním krokem by mělo být vytvoření veřejného a soukromého klíče. Pro generování klíčů využijte dalšího programu z naší „nabídky“ – WinPT. Po jeho spuštění klikněte na tlačítko »Key | New« a zadejte své jméno a e-mailovou adresu. Poté zadejte heslo a potvrďte dotaz programu, zda chcete vytvořit zálohu.

POUŽITÍ V THUNDERBIRDU

Aby bylo možné klíče integrovat do Thunderbirdu, budete potřebovat nástroj Enigmail z Chip DVD. Nainstalujte ho v Thunderbirdu v nabídce »Tools | Add-ons | Install…«. Po restartování e-mailového klienta najdete v nabídce novou položku – „OpenPGP“. Klikněte na něj a poté na »Extras | Accounts | OpenPGP security«. V okně, které se objeví, ještě aktivujte zatržítka u položek „Activate OpenPGP support for this identity“ a „Use the email address of this account to identify OpenPGP key“. Nyní mohou být vaše e-maily šifrovány – nejprve ale musíte také odesílateli poslat veřejný klíč. To provedete kliknutím v Thunderbirdu na »OpenPGP | Manage key« a poté na »File | Send public key via email«. Pokud obdržíte klíč vy, klikněte na něj pravým tlačítkem a zvolte položku »Import OpenPGP key«

ZABLOKOVANÝ OUTLOOK

OpenPGP nelze integrovat do aplikací Outlook a Windows Mail. Existuje sice alternativa v podobě GpgOL (součást GPG-4win), ta je ale určena pouze pro pro Outlook 2003 SP2 a její použití je velmi omezené. My doporučujeme použití verze Steganos Privacy Suite.

Postupujte takto: Spusťte program a klikněte na »Email encryption«. Privacy Suite otevře textové pole, do kterého napište svou zprávu. Poté klikněte na tlačítko »Send encrypted « a zadejte heslo. Zpráva je nyní předána do Outlooku a přidána k e-mailu jako příloha. K jejímu přečtení potřebuje příjemce klíč…

Jako alternativu lze také použít program GPGrelay, který se „umístí“ mezi klienta a poštovní server, nicméně konfigurace nepatří k nejsnadnějším a vyžaduje dobrou znalost problematiky…

spamové maily – pro e-mailového klienta lze použít pouze TOR.

Vysoká rychlost: Stálé spojení

Nic není otravnější než vysokorychlostní spojení, které kvůli anonymizéru padá do úrovně „doby modemové". Abychom zjistili rychlost surfování, několikrát jsme změřili dobu nahrávání tří komplexních webových stránek a vypočítali jsme průměrnou hodnotu – s překvapivým výsledkem: všechny komerční programy využívají tak rychlých serverů, že jsme nedokázali určit žádný znatelný rozdíl při anonymním surfování. Pouze bezplatná síť TOR je bolestně pomalá. I zde ale došlo ke zlepšení: pokud někteří klienti měli v minulosti problémy při vytváření spojení, ty už se nyní neobjevují. Všechny nástroje byly stabilní a fungovaly bezchybně.

Ovládání: Značné rozdíly

Pokud jde o rozsah funkcí, zde se nic nezměnilo – klienti stále nabízejí pouze spartánské funkce: klasikou je nástroj S.A.D., který zobrazuje jen nejdůležitější informace, jako IP adresu a status spojení. Nenabízí žádné možnosti nastavení kromě automatického přihlášení a varovné zprávy v případě přerušení spojení. V případě Steganosu a programu ArchiCrypt je rozhraní ještě skromnější: programy „neodkrývají" o mnoho víc informací, než je IP adresa a údaj o datovém provozu. Oba nástroje jsou identické i v dalších oblastech: výrobci sdílejí rozhraní stejně jako VPN servery. Navzdory tomu si programy v testu vedly odlišně, a to jak kvůli lišícímu se objemu přenesených dat, tak i kvůli kolísající rychlosti. JonDo je rozporuplný: na jedné straně je ovládání programu poněkud zmatečné, na straně druhé si uživatel může zvolit mezi několika „profily" a na první pohled vidí zemi příslušného mixu. Náročnější uživatel se také může ponořit hlouběji do programu a přidat různé filtry, nastavující například minimální rychlost přenosu.

VERDIKT: Všichni ti, kdo si přejí surfovat co nejvíce anonymně, by měli volit balíček JonDo Premium a nainstalovat si volitelný JonDoFox.

Žádný jiný klient nenabízí uživateli tak transparentní službu a různorodá nastavení. Dalším plusem jsou kaskádové mixy, které mohou být distribuovány i přes několik zemí. I vytrvalí čmuchalové mají tedy sotva šanci odfiltrovat určitého uživatele. Dokonce i JonDo má však své nevýhody: nastavení neběží automaticky a klient by mohl být přehlednější. Ostatní placené programy se stěží liší jeden od druhého: klienti od Steganosu, S.A.D. a ArchiCrypt běží rychle, sami se konfigurují a šifrují kompletní datový provoz. Nenabízejí však bezpečné nastavení prohlížeče. Všichni ti, kdo surfují pomocí těchto nástrojů, by měli rozhodně doladit svůj přístup na síť pomocí doplňků, jako je například JonDoFox. Koneckonců efektivní blokování čmuchalů dat neznamená mít jen anonymní IP... 

AUTOR@CHIP.CZ

VÍTĚZ TESTU 11/2009

CENOVÝ TIP 11/2009

POŘADÍ	1. MÍSTO	2. MÍSTO	3. MÍSTO	4. MÍSTO	5. MÍSTO
Produkt	JonDo Premium + JonDoFox [2]	Steganos Internet Anonym VPN	S.A.D. CyberGhost VPN [2]	ArchiCrypt Stealth VPN	Tor
Internet	www.jondos.de/en/	www.steganos.com	www.cyberghostvpn.com	www.archicrypt-shop.com	www.torproject.org
Cena (přibližně)	10 euro	12 eur za měsíc	10 eur za měsíc	12 eur za měsíc	zdarma
Celkové hodnocení	88,7	77	75,6	75,6	53,8
Bezpečnost (50 %)	87	63	63	63	66
Rychlost (35 %)	99	94	90	93	35
Ergonomie (15 %)	70	84	84	77	57
Bezpečnost					
Proxy	kaskádový mix	VPN server	VPN server	VPN server	veřejný server
Šifrování IP v browseru	manuální	automatické	automatické	automatické	automatické
Maskování OS a browseru	maskuje všechna data	nemaskuje žádná data	nemaskuje žádná data	nemaskuje žádná data	nemaskuje žádná data
Instalace P2P / chat / IM	manuální	automatické	automatické	automatické	manuální
Blokování cookies	●	–	–	–	–
Deaktivace: Java a Flash	●	–	–	–	–
Šifrování e-mailu	–	–	–	–	●
Šifrování ftp/https	●	●	●	●	●
Blokování reklamy	●	–	–	–	–
Rychlost					
Průměrná rychlost nahrání stránky [1]	4,4 sekundy	4,9 sekundy	5,3 sekundy	5,0 sekund	225 sekund
Spolehlivost	žádné problémy	žádné problémy	žádné problémy	žádné problémy	žádné problémy
Ergonomie					
Rozhraní	jednoduché, občas zmatené	jednoduché a přehledné	jednoduché a přehledné	jednoduché a přehledné	nepřehledné
Instalace	uživatel musí ručně nastavit server	automatická	automatická	automatická	uživatel musí ručně nastavit server
Možnosti nastavení	mnoho	téměř žádné	téměř žádné	téměř žádné	několik
Povolený datový tok (za měsíc)	1,5 GB (celkově)	50 GB	40 GB	25 GB	neomezeno
Další služby	–	–	2 GB prostoru na internetu	–	–

[1] bez šifrování stránka nahrána za 4,2s

[2] nabízena i bezplatná služba s omezenými funkcemi a rychlostí

● Špičková třída (100–90,0) ● Vyšší třída (89,9–75,0)
● Střední třída (74,9–45,0) ● Nelze doporučit (44,9–0)
Všechna hodnocení v bodech (max. 100)

● ano
– ne