Stopy našich dní

Jak můžeme být na internetu pod cizí kontrolou, když máme ke všemu hesla? Zjistit, co všechno o sobě prozrazujeme někomu technicky zdatnějšímu jenom tím, že strávíme hodinu na internetu, může znamenat pro humanitně vzdělaného čtenáře šok. Velmi užitečný šok.

HONZA ŠÍPEK

To, že jsi paranoidní, neznamená, že tě nedostanou.

(Počítačové přísloví)

Žijeme v demokratické společnosti, svůj stát máme rádi, firmy nás zásobují výrobky, banky nám dávají peníze a myšlenku, že by někdo mohl zneužívat všech těch elektronicky předávaných informací, které se o nás při styku s nimi tak nějak samy shromažďují, odmítáme jako absurdní. Všudypřítomné počítání bereme jako důsledek počítači prostoupeného světa. Musíme se ale naučit počítat i s tím, že spolu s informacemi, které posíláme prostřednictvím moderních technologií, dáváme někomu potenciální moc. Sledování jednotlivce je dnes snazší, než bylo kdy předtím. S každým zaplacením kartou, esemeskou nebo facebookovým statusem nabízíme informace o své momentální poloze, adrese domova, zájmech, finančních příjmech a výdajích, přátelích, sociálních vztazích a dokonce detailním obsahu naší komunikace komukoli, kdo se přičiní – ať už je to „korporace“, šikovný jednotlivec nebo „stát“. Kdo nedělá nic nelegálního, nemá se čeho bát, říkají často ti, kdo už se s tímhle hromadným sledováním smířují. Ale kdo nedělá nic nelegálního, měl by mít právo na to, aby ho nikdo nesledoval. Hromadné sledování, o kterém se často vůbec nedozvíme, dělá vlastně ze všech lidí podezřelé.

Iluze bezpečí

Nejsem paranoidní. Mluvím občas s hackery a ti jsou paranoidní, zatímco mne považují za upovídaného důvěřivce, který co neví, to neřekne. Ale při svých nočních běžích po síti zjišťuji hlavně to, že takzvaná počítačová bezpečnost je často jenom k pousmání. Medializovaných průniků je zlomek, ostatní mají dobré důvody zasažení ututlat, na většinu se ani nepřijde. Na Slovensku byli hackeři v síti Telecomu i tamějšího Národního bezpečnostního úřadu. Že se tam dostali za pomoci hesla NBUSR123, je provařená historka. Většina bezpečnostních průšvihů je jenom lemplovství správců. Dokonalá bezpečnost je snad právě jenom v rukou paranoiků, protože své drobné hříšky má každý.

Přemýšlím o datech, která mám na disku nešifrovaná. Jakou škodu způsobí v cizích rukou? Kde si udělat jejich zálohu pro případ, že mě vykrade zloděj, který pobere všechny „hi-tech krabičky“, aby je prodal do bazaru za zlomek ceny dat? Při pouhém „podezření“ z nějaké kriminální aktivity mi dnes policie může zabavit všechny počítače jako „důkaz“. Advokát Tomáš Sokol kdysi pro někoho uhádal, že zabavování počítače není nezbytně nutné k zajištění důkazu. Museli počkat na policejního experta, který přišel s mašinkou na duplikování disků. To je ale výjimka. Slyšel jsem také o právnické kanceláři, která zálohuje všechno na síťový disk zazděný do zdi, o němž vědí jenom oni – běžná síťová zásuvka do zdi třeba u nezvané osoby nevzbudí pozornost. Nejjistější je odeslat šifrovaným spojením data do geograficky oddělené lokality. Šifrovaným spojením, na šifrovaný disk. Klíč je v mojí hlavě.

Spousta aplikací nechává na disku stopy po svém provozu, třeba Skype, podobně jako mnoho dalších, ukládá na disk přepisy textové komunikace. Jedinou obranou, jak chránit ukládané informace, je šifrování. Kdysi jsem četl zápisek hackera, k němuž přišla policie na razii. Odnesli si šifrované disky a od té doby mlčí, nenásledovalo žádné obvinění, nic se nestalo. Doba rozšifrování klíče školenými specialisty roste exponenciálně s jeho délkou. Pokud by nalezení klíče o délce 64 bitů trvalo na nějakém počítači 4 minuty 16 sekund, nalezení klíče o 128 bitech by na stejném stroji trvalo až 149,7 trilionu let. Lze nasadit drahou dešifrovací farmu, celý sál počítačů spojených dohromady, na týden, měsíc nebo rok. Pak už jim to ale musí stát za to. Síly šifer lze naštěstí z principu zvětšovat podstatně laciněji než síly dešifrovacího hardwaru. Ovšem stále platí pravidlo, že veřejně známé technologie jsou aspoň deset let pozadu za těmi tajnými. Průlom v dešifrování se očekává s příchodem kvantových počítačů, které jsou oficiálně stále v plenkách.

Šifrování se ale musí udělat dobře. Paranoidně. V zahraničí se už objevily zákony o povinnosti vydání klíče k šifrovaným datům, a pokud ho podezřelý neposkytne, pohlíží se na něj jako na vinného – jinými slovy zavádí se presumpce viny. Díky tomu se rozvíjí steganografie a technika jménem věrohodná popiratelnost. Jde o to šifrovat tak, aby data vypadala jako nešifrovaná. Například nástroj TrueCrypt nabízí šifrování přes dva klíče: každý odemkne jiný oddíl. Ten, který z vás útočník dostane dešifrovací metodou slangově zvanou „rubber hose cryptoanalysis“ neboli kryptoanalýza gumovou hadicí (mlátí vás gumovou hadicí tak dlouho, dokud nevyklopíte heslo), otevírá přístup k neškodným, ale realisticky vypadajícím datům. Ten, jejž si necháte pro sebe, otevírá data skutečná, která při analýze disku vypadají jako náhodná skrumáž znaků. Když vrchnost něco zakáže, přímo vyzývá poddané, aby se to učili obcházet. Tajné školy na středověkém venkově v Lotyšsku se maskovaly jako stodoly. Ilegální knihy se přesunuly z police za trám. Zakažte torrenty! Vyvinou se do podoby, ve které je nebude možné zastavit vůbec. Zaveďte kontroly počítačů na hranicích a lidi si budou schovávat miniaturní paměťové karty do dutých mincí. Tím, že zakážeme disent, podpoříme jeho konspirační metody. Ještě generace před námi to zažila. Stát rozvinul aparát sledování do té míry, že, jak řekl Egon Bondy, „obyvatelstvo je tradičně tak profízlované, že jeden udávaje druhého prostřednictvím třetího už udává sám sebe“. Přesto vycházely v podzemí zakázané knihy, kopírovala se muzika i neškodné americké akčňáky, které systém do země nepustil. A když už existovala infrastruktura na kopírování Ramba, dala se snadno použít i k šíření undergroundového „Originálního videojournalu“.

Ok(n)o prohlížeče

Je ráno, otevírám internetový prohlížeč a místo obvyklého rituálu čtení novin dnes otevřu okénko s historií adres. Funguje to jako mentální cvičení – čtu si svoji webovou historii a domýšlím, co by se o tomhle neznámém člověku dalo zjistit. Doporučuji to všem, kteří tvrdí, že nemají co skrývat. Vlakové spojení Nymburk-Praha. Hledání adresy na mapě v Praze-Vršovicích. Vida, je tam psychoterapeutická ordinace. Pak záznamy končí a pokračují až v 21.42. Hledání klíčových slov „úzkost“, „jak překonat úzkost“, „samota“, pak pětkrát dokola jméno nějaké holky. Server s pornografií a klíčová slova „blonde“, „petite“ a „czech“. Pak včerejší historie končí. Stopy našich dní.

Historii obvykle mažu, ale znamená to jenom to, že není uložena v počítači. Vidět je ovšem všude cestou. Na domácím wifi modemu, přes který jsem připojený k internetu. Mám ho sice pod kontrolou jenom já, ale celkem nedávno proběhla vlna virů, které infikovaly nezabezpečené modemy. Čínská firma Huawei přišla o hodně západních státních zakázek, když byla podezřelá, že zadělávala zadní vrátka do modemů a ty se pak používaly pro čínskou průmyslovou špionáž. Nahodit si z notebooku spadlou wifinu v kavárně není velký problém ani pro mne (proč je heslo k administrátorskému účtu tak často admin?), a to nejsem žádný hacker. I tak se ale mrknu na aktivitu ostatních připojených uživatelů, než si jdu po svém.

Také nevím, kdo má pod kontrolou wifi na druhé straně. Nejspíš poskytovatel internetu, jeho zaměstnanci, kdokoliv, kdo je zrovna „hacknul“, a ze zákona také policie a tajná služba. Nevím, co zaznamenávají, „logují“ nebo „nelogují“. Nedávná evropská vlna zákonů od „data retention“ přikazovala poskytovatelům internetu logovat povinně (v uvědomělejším Německu byly dvacetitisícové demonstrace), také u nás se v současnosti jedná o zákonnou povinnost. Kromě toho znají moje jméno, adresu a vědí, kde fyzicky jsem. První je patrné ze smlouvy, druhé z cesty signálu ke mně. Moje požadavky na webové stránky jsou spojené s jednou IP adresou, a co je horší, i s MAC adresou, která namísto bodu připojení jednoznačně identifikuje konkrétní počítač, ať už je kdekoliv. I ta jde samozřejmě změnit či falšovat, ale musíte vědět aspoň, že něco takového existuje. I když používám více e-mailových schránek na různá jména, hlásím se na všechny z adresy z jednoho počítače, čímž se anonymita ztrácí. Provozovatel e-mailu navíc dává moji IP adresu do hlavičky každé jednotlivé zprávy. Brněnští akademici Horyna s Hrochem by mohli vyprávět.

Co je logování

Pardon, neřekl jsem, co to je log a logování. Log je deníček, žurnál, záznam denního provozu. Strohý textový soubor, na každém řádku přesné datum a čas a pak údaje podle služby. Třeba adresa mého počítače a adresa webové stránky, kterou jsem otevřel. Někdy také technické údaje navíc. Ne všude, kde logy být můžou, skutečně jsou. A ne všude, kde jsou, je někdo čte. Ale v tom je právě jejich kouzlo, že se do nich dá dívat zpětně, hledat dlouho v historii, až tehdy, kdy je potřeba něco najít. Úsporný textový formát umožňuje na běžném disku bez problémů skladovat miliardy záznamů. Občas se na webovém serveru, který sám spravuji, dívám prostřednictvím logů na ty, kdo se dívají na mě. Na každém řádku je kromě adresy počítače, který se dívá, také URL mojí stránky a URL stránky, z níž vedl odkaz. Když je tou stránkou vyhledávač, najdu klíčová slova, která ten člověk hledal. Vystavili jsme pár článků z chystané knížky na web. Dívám se, co lidi hledali. Třeba tady: článek o kapesních práskačích, tedy mobilech. Dotazy přes Google: „policie odposlouchává okolní prostor mobilního telefonu“, „jak dlouho t-mobile archivují data“, „gsm rušička schéma odposlechové zařízení na společné anténě“ atd. U těch nejzajímavějších dotazů se mrknu na IP adresy. Přeložím je na „doménová jména“ a zjistím, ze které sítě jsou. Z mobilu od T-Mobile, z pevné linky od O2, tady někdo dokonce z práce, mám jméno jeho zaměstnavatele, poslední je z Matfyzu, z budovy kolejí v Troji, číslo pokoje nenajdu, ale někdy bývá. Nakonec neodolám zvědavosti, kdo chce stavět rušičku GSM, a přes GeoIP si vyhledám polohu té pevné linky od O2. Vida, Zahrada u Tišnova. Tam není moc baráků. Jak snadno se dostat do role sledujícího…

Když byl kamarád na návštěvě u konkurence, otevřel tam webové stránky své firmy, nepřihlašoval se, ale byla to malá firmička, a za chvíli mu zvonil telefon: „Hele, že ty jsi tam a tam?“ Velké hostingové firmy, to budou miliardy řádků a z nich už se dá rekonstruovat velká část virtuálního pohybu jednotlivce. Google určitě smutnil, že vidí jen to, co lidé právě hledají, a ne co dělají potom – už i to je ale hodně, vezmeme-li v úvahu, do jaké míry nás definuje to, co na internetu hledáme. I proto asi vznikla služba Google Analytics, sledující statistiky návštěvnosti. Pěkné, barevné, hýbající se, přehledné. Stačí dát do těla vlastních stránek malinký kousek

Průvodce praktického paranoika po internetovém soukromí

kódu, který se každému návštěvníkovi načítá už nikoliv ode mne, ale ze serveru Googlu, a Velký bráška se už postará o zbytek. Subjektů, které stojí o záznamy provozu všude na síti, je hodně.

Takové kódy třetích stran mají v sobě vložené nejrůznější weby. Nejen Analytics, ale i reklamy, jiné statistické servery jako Toplist atd. Na jedné webové stránce jsou jich klidně i desítky. „Kam čert nemůže, tam nastrčí tlačítko Like," je nové počítačové přísloví, odkazující ke snaze Facebooku o totéž. Když začal v profilech uživatelů zveřejňovat adresy, které si prohlíželi i *mimo* sociální síť, byl z toho poprask. Jejich zobrazování pod tlakem veřejnosti raději vypnuli, což ale neznamená, že pohyb svých uživatelů jinde po síti masivně nesledují dál. Kdekoliv na internetu spatříte modré tlačítko „Like", můžete si být jisti, že Facebook právě skrytě zaregistroval váš pohyb. Nejste přihlášeni? Nevadí. Stačí, že jste byli. Což řeší takzvané sušenky, cookies, kousky kódu, které jsou prý nezbytné k tomu, abychom se mohli někam přihlásit, a ukládají se na disk počítače. Server si o ně může zpětně říct a prohlížeč mu je ochotně pošle, takže nenápadně identifikují, že se dívám ze svého notebooku, ať už se připojím odkudkoliv. Kdysi, když to začínalo, jsem se divil, když mi Amazon říkal „Hello, Jan Sipek", aniž bych se přihlásil. To je deset patnáct let. Ještě dneska je někdo překvapený, že od Googlu dostává jiné výsledky vyhledávání než kamarádi. Cookies mám vypnuté (lze nastavit), a není-li zbytí, pečlivě až nutkavě je mažu hned po použití. A to prosím nemám účet na Gmailu a sociálním sítím se vyhýbám jako čert kříži!

Pocit bezpečí

Existuje Tor, anonymizační síť založená nadací Electronic Frontier Foundation, která funguje na principu kryptografického předávání požadavků mezi stroji, takže při pohledu zvenčí není jasné, kdo se kam dívá. Tor je sice pomalý a má své slabiny, ale zatím je to nejlepší, co máme. Mimo jiné umožňuje i anonymizaci zdroje informací, serveru, takže je jen velmi obtížné ho vystopovat. Existují i webové anonymizéry. Člověk zadá do okénka na anonymizační webové stránce (třeba Anonymouse) adresu a dostane se na ni, aniž by ho provozovatel cílové stránky mohl identifikovat. Zná ho ale provozovatel anonymizátoru, takže kdybych byl tajná služba, určitě nějaký provozuju. Jak snáz se dostat k lidem, kteří chtějí něco skrývat? I zde platí, že si nemohu být jistý technologií, kterou nemám pod svou kontrolou.

Když nepoužívám šifrovaný protokol (třeba HTTPS), všechno, co si s nějakým serverem povídám, si může číst kdokoliv cestou. Ani s šifrováním bohužel není jistota stoprocentní, nedávno právě Electronic Frontier Foundation, která je snad největší organizací strachující se o naše soukromí v digitálním světě, zveřejnila souhrnný přehled útoků na certifikační autority a vyplývá z toho jenom to, že i ono S připojené k HTTP dává pocit bezpečí spíše iluzorní. V prohlížeči se sice rozsvítí pěkný zámeček, že je spojení šifrované, ale (částečnou) jistotu, že někdo nepodniká útok zvaný man-in-the-middle, získá člověk jen pečlivou kontrolou.

Uf. Domýšlet pár pohybů myší do důsledku je docela vyčerpávající. Vlastně takhle nechci přemýšlet. Je to nějak choré. Možná je lepší nevědět. Ale vzpomenu si na citát Starého mistra: „Brát mnohé na lehkou váhu způsobuje četné problémy. Moudrý se na ně dívá jako na problémy, a proto je nemá." Ne, nemám se bát. Jenom si být vědom toho, co se děje. Whitfield Diffie, jeden z autorů asymetrického šifrování, napsal v knížce *Privacy on the Line* (Soukromí na lince, 1998), že naše společnost je společností nejsilnějšího dohledu, který kdy byl. O to hůř, že si to obvykle neuvědomujeme. To, že stát k téměř totálnímu dohledu ještě nepřidává totální moc, je zatím jenom shoda okolností.

Hromadné maily

Otevírám mail. Ten „oficiální", co mám na svém serveru. Připojím se šifrovaným spojením. Dovnitř vidím jenom já – tedy pokud nám server někdo „nehacknul" a nekouká mi pod ruce. Ne každý si může ten luxus dovolit: vlastní server stojí čas a peníze, ale je to lepší než vědět, že se mi maily systematicky, strojově, aniž bych to tušil, někdo prohrabává. Třeba i bez zřejmého úmyslu, jen proto, že může. Nebo aby doplnil mail, který čtu, reklamou, která reaguje na jeho obsah. Nebo kvůli „anonymním statistikám". Někdo, kdo má k dispozici všechny e-maily třeba několika milionů lidí. Seznam má 7,5 milionu uživatelů, Google 423 milionů, Yahoo 320 milionů. Například od ledna do června 2012 vydal Google soudu za účelem dokazování jenom v USA přes patnáct tisíc účtů a čísla každým rokem rostou. Zmínili jste se v mailu, že nejste tak hloupí, abyste platili daně? Očividný důkaz. Provozovatel může všechno, ale k ničemu se nezavazuje. Když účet zruší, protože jste údajně „porušili podmínky služby", nedovoláte se nikoho, přijdete nejspíš o archiv pošty, kontakty, a kdo vám napíše, dostane zpátky lakonickou odpověď, že neexistujete. Vizitky s natištěnou adresou můžete hodit do koše. Pro příklady nemusíme chodit až do Číny. Ochota internetových korporací spolupracovat se státem i bez soudních nařízení se vyjevila v kauze Wikileaks, když služby whistleblowerskému serveru naráz zrušila americká hostingová firma Amazon, registrátor domény, platební služba PayPal i klasické bankovní společnosti.

Probírám se mailem. Velký podíl zabírají maily z konferencí (systém jedné adresy, z níž se došlá pošta automaticky rozesílá všem ostatním přihlášeným). Některé z nich nemají svůj webový archiv, takže co nezachytíte, jako by neexistovalo. Třeba ten s provokativním názvem Al-Qaeda, který se zabývá právem na soukromí a svobodu projevu. Říká se tomu Dark Web – je to polosoukromá část internetu, trochu jako temná hmota ve vesmíru, normálně není vidět. Na Arizonské univerzitě nedávno vydali knihu, jak do Dark Webu vysílat automatizovaně své roboty a sbírat data. V rámci boje proti terorismu, jak jinak. Roboti automaticky infiltrují mailing list nebo skryté webové diskusní fórum pouze pro členy. Občas je potřeba lidský zásah nebo lstí získat heslo, ale pak už jede všechno automaticky: získávání informací, jejich analýza, analýza obsahu, takzvaná sentiment analýza, která umožňuje zjišťovat naladění k různým tématům, a také analýza autorství na základě často používaných obratů a jazykové struktury textu, takže ani používání několika různých jmen nepomůže.

Seznam příjemců hromadného mailu v jeho hlavičce milují spameři i spywary, infekční programy, které možná infikovaly váš počítač a snaží se majiteli posílat vaši komunikaci. Je rok 2012 a spousta lidí se ještě nenaučila používat slepou kopii (Bcc:) a s každým odeslaným mailem dávají všem ostatním k dispozici celý svůj adresář. Já se jenom dívám, občas najdu adresu, která se může hodit, a občas mě překvapí, že odesílatel zná někoho jiného, koho znám taky, ale netušil jsem, že se znají oni dva. Takové zjištění není tak triviální, jak by se mohlo zdát. Aniž bychom totiž museli znát obsah komunikace, můžeme si z pouhého souhrnu údajů o tom, kdo komu psal, udělat úhledný graf sociální sítě. Ze skupinek, které se znají, vzniknou takové pěkné shluky, a to i v případě, že komunikace probíhá přes prostředníky. Sociometrické hvězdy, „huby", budou svítit jako vysoce propojené uzly – to jsou ti, kteří mají vliv a na které se vyplatí cílit marketing nebo je zavřít, když se něco semele. Existují na to speciální programy. Kupují si je třeba banky, telefonní operátoři nebo tajné služby. Jak je asi jasné, jde taková mapa udělat i z jiných než poštovních logů – například z telefonního provozu nebo z výpisů pohybů na bankovních účtech. Nebo přeposílání esemesky, která vybízí k účasti na demonstraci. Oblíbená otázka teoretiků, kteří se sítěmi zabývají, zní: Kolik procent uzlů musím odebrat, aby se síť rozpadla na vzájemně izolované nekomunikující ostrůvky? Nebo aby se síť tak zpomalila, že nebude k ničemu?

S pohledem na tato metadata teprve začíná skutečná paranoia. Pokud identifikujeme strukturu sociální sítě a jsme schopni identifikovat i vlny probíhajících hnutí a revolucí a pokud bychom zároveň měli pod kontrolou médium typu Twitter nebo Facebook, je teoreticky možné tyto události nepostřehnutelným způsobem akcelerovat nebo zpomalovat. Albert Lázsló Barabási, průkopník v oblasti teorie sítí, zmiňuje, že například ekonomická krize v roce 1997 začala krachy několika malých, ale vysoce propojených asijských firem. A teď ta paranoidní úvaha: Kdo má k dispozici dostatečné množství ekonomických dat, a ta se běžně prodávají, může tyto neuralgické body za pomoci matematiky a statistiky identifikovat a pohybem pověstného motýlího křídla vyvolat i rozsáhlý propad celé ekonomiky.

Autor je dokumentarista.

Musíme se naučit počítat s tím, že spolu s informacemi, které posíláme prostřednictvím moderních technologií, dáváme někomu potenciální moc. Foto Honza Šípek

Text je redakční koláží z připravované **Nebezpečné knihy**, jejíž vydání chystá nakladatelství Dokořán. Ukázky najdete rovněž na adrese eldar.cz/kniha.