

Co dělat po PRISM?

Vítejte v době informační normalizace

Nedávné odhalení masivních odposlechů a archivace dat v kauze Snowden není první podobného druhu a jeho důležitost spočívá spíše v potvrzení předpokladu, že na šmírování s vládami spolupracují velké firmy. Otázka, jak se podobnému tlaku lze bránit, je stále aktuálnější.

HONZA ŠÍPEK

Před měsícem prozradil whistleblower Edward Snowden veřejnosti existenci amerického systému PRISM. Americká vojenská tajná služba NSA nejen že se snaží odposlouchávat a uchovávat veškerou internetovou a telefonní komunikaci, ale podle Snowdena jí naše data poskytují přímo velké IT společnosti, miláckové Silicon Valley, mezi nimiž nechybí Microsoft, Yahoo!, Google, Apple, Skype ani Facebook.

Dotčené společnosti nejprve jakoukoliv spolupráci vyvrátily a zdálo se, že se obvinění nepodaří prokázat. Pak se ale do obhajoby systému pustil i prezident Obama, ve Velké Británii byl odhalen spolupracující sledovací systém Tempora (a další podobné ve Francii a Německu) a opozice se začala ptát, proč výzvědné systémy míří proti vlastním občanům. Tehdy začalo být pravděpodobné, že PRISM skutečně existuje.

Cirkus kolem Snowdena

Snowden však není první, kdo o masivním sledování ze strany NSA promluvil. Už loni v březnu popsal americký časopis Wired ohromné datové centrum NSA, budované v Bluffdale v Utahu. Celé věže serverů mají běžet na 2 323 čtverečních metrech. Kapacita je odhadovaná v řádech zettabytů nebo dokonce

podle časopisu Wired obstarávat propojení mezi těmito výpočetními centry. Dalším ze subdodavatelů má být firma Endgame Systems, která se snaží udržovat celosvětovou databázi všech zařízení připojených k internetu včetně jejich fyzického umístění, běžícího softwaru a seznamu potenciálních bezpečnostních děr.

Bývalí zaměstnanci NSA William Binney, Thomas Drake a J. Kirk Wiebe na podezřelé praktiky upozornili už v roce 2002. Kryptograf Binney paradoxně vystoupil hlavně proto, že systém dodávaný do NSA považoval za pře-dražený, odfláknutý, a tedy i korupční. Drake proto, že systém, který měl sledovat „zahraniční cíle“, protiústavně sledoval občany vlastního státu. Všichni tři měli vážné problémy, byli zadrženi, stanuli před soudem (Drake dokonce za špionáž), později našli zastání u organizace na podporu whistleblowerů a nakonec byli očištěni. Rozdíl oproti Snowdenovi je v tom, že se na média obrátili až v okamžiku, kdy vyčerpali všechny možnosti domoci se nápravy u svých nadřízených. Přesto jim světová média věnovala minimální pozornost a ve srovnání s ohlasem, kterého se dostalo Snowdenovi, považují sami sebe za neúspěšné. Způsob, jakým NSA odposlouchává internetový provoz, popsali Drake a Binney loni v prosinci na hackerské konferenci 29c3 v Berlíně. Masivní odposlech komunikace tedy není nic nového (například systém Echelon vybudovaly Spojené státy a jejich spojenci již během studené války), Snowden však poprvé promluvil o tom, že v této hře spolupracují s tajnými službami i internetové a telekomunikační firmy.

Celý cirkus kolem „disidenta Snowdena“ i vystoupení předchozích whistleblowerů mohou být samozřejmě zpravodajskou hrou. Touha mocných po kontrole nad elektronickými komunikacemi je ale logická a bylo by s podivem, kdyby neprobíhala. Navíc recepty, jak se sledování bránit, mohou mít příjemné vedlejší

moci koncentruje v rukou jednoho subjektu (který, i kdyby byl sám o sobě desetkrát svatý, může být ovládnut někým zlým). Internet by měl být podle mého co nejvíce decentralizovaný a systémy by měly fungovat co nejvíce autonomně a nezávisle na svém okolí,“ popisuje svoji motivaci. Experiment, který si málokdo z nás dovede představit, dopadl konstatacím „přežil jsem to v pohodě“ a radami, jak se službám Googlu vyhnout.

S nápady na decentralizovanější využívání Internetu přišla i Nadace elektronického pohraničí (EFF.org). Na jednoduché a přehledné stránce PRISM-Break.org zveřejnila možné náhrady za produkty ohrožené sledováním nebo se na sledování podílející. Windows a MacOS – které s „domovskou stájí“ Microsoft nebo Apple komunikují hned po instalaci – navrhuje nahradit Linuxem. Telefonní operační systém Android plně otevřeným Replicantem a iPhone radí zcela nepoužívat. K populárním sociálním sítím, které „v tom jedou s NSA“, nabízí deset otevřených alternativ.

Umění války

Obecně by se obrana proti PRISM dala přirovnat ke konzumeristickému hnutí. Po vpádu hypermarketů na lokální trhy se stalo moderním, ba módním – ale ještě více snad zodpovědným – nakupovat zeleninu od místních zemědělců a při nákupu v obchodě se podívat, odkud zboží pochází.

Sledování nejlépe minimalizujete, když se prostě vyhnete firmám, které se na něm podílejí. Je třeba hledat alternativy za Google, Facebook, Twitter a používat něco jiného. Pít něco jiného než coca-cola a jíst něco jiného než McFlouštíky. Neukládat si nic do cloudu. Zvážit, které internetové služby používáte dennodenně, a uvědomit si, kdo za nimi stojí. Nainstalovat si do internetového prohlížeče doplňky, které omezují sledování. Vedlejším efektem je pak navíc výrazné omezení reklam. Ti pokročilejší, nebo paranoidnější, se mohou pokusit korporace ze svého osobního počítače vyštvať. Nainstalovat firewall a bránit všem pokusům o to, aby se počítač za našimi zády připojoval tam, kam nechceme.

Ještě pokročilejší si patrně nainstalují některou z variant Linuxu – k uživatelské přívětivosti se za poslední roky udělaly velké kroky a systémem se u nás začíná s úspěchem používat i na základních školách. Software, který má otevřené zdrojové kódy, je pod veřejnou kontrolou, a kdo chce, může přezkontrolovat, co vlastně s jeho počítačem provádí. Je to srovnatelné se situací, kdy stát zveřejňuje všechny uzavírané smlouvy nebo příjmy poslanců. Oproti tomu uzavřené operační systémy lze přirovnat k firmám anonymních akcionářů, které dostávají tučné zakázky od státu, s odvoláním na obchodní tajemství nezveřejňují detaily a říkají: „Všechno je v pořádku, nám můžete věřit.“

Nejpokročilejší uživatelé zašifrují své pevné disky a povedou všechnu komunikaci dovnitř i ven šifrovanými kanály. Použijí anonymizační služby jako Tor nebo VPN, platit budou Bitcoinem (viz Bitcoin: Bez vlád i bankéřů, A2 č. 3/2013) a budou provozovat vlastní servery, jimž budou vládnout jenom oni. Server může být i notebook ve spíži. Má malou spotřebu a nechcípne, když vypnou elektriku. Hackeri mezi tím vyvinou technologie umožňující další skrývání. Veřejnost je otestuje, projdou evolucionálně – a buď se ujmou, nebo zaniknou.

Reakcí na útok je hledání obrany: na šmírování oknem stačí záclony, proti odposlechu se lze bránit šifrováním, odpovědi na zákaz šíření informací je samizdat. Možná po období „informační revoluce“ vstupujeme do fáze informační normalizace. Jak říká mistr Sun: „Odhalíš-li rozmístění a záměry nepřitele, sám však pro něj zůstaneš neviditelný, tvé síly se mohou spojit, zatímco jeho budou roztříštěné.“ Autor je dokumentarista.



Je třeba hledat alternativy za Google, Facebook, Twitter a používat něco jiného. Foto Honza Šípek

yottabytů. Jsou to jednotky, které zatím příliš neslycháme. Zettabyte je tisíc exabytů, tedy milion terabytů. Yottabyte je ještě tisíckrát tolik. Pro srovnání: loňský provoz celého internetu je odhadován na 528 exabytů, na rok 2015 se předpokládá 966 exabytů ročně. Už jen plánovaná spotřeba elektriny výpočetního supercentra je 65 megawattů, tedy pro srovnání více než polovina výkonu elektrárny Hodonín. Dokončení areálu je údajně plánováno na letošní září.

Další výpočetní centrum má stát ve Fort Meade, sídlo NSA, svá centra vybudovali i subdodavatelé armády jako General Dynamics či Boeing. Firma Booz Allen Hamilton, která zaměstnávala právě Snowdena, měla

účinky: kromě ochrany před běžným špiclováním ze strany konkurence nebo policie a větší odolnosti proti spywaru a virům také decentralizaci informací. A ta se může hodit i v případě průšvihů jiného druhu, například při masivním blackoutu nebo kybernetickém útoku.

Lze žít bez Googlu?

Po odhalení projektu PRISM se média věnovala hlavně bizarnímu příběhu „viníka úniku“. Odborníci mezitím začali hledat nápady, jak se sledování vyhnout. Český technologický blogger „Franta“ již loni popsal své zkušenosti s experimentem „Týden bez Googlu“: „Nejde primárně o to, zda je Google ‚hodný‘ nebo ‚zlý‘ – problém vidím už v tom, že se příliš mnoho