Nenápadné černé skříňky

Proč je novela zákona o Vojenském zpravodajství nebezpečná?

Vojáci usilují o prosazení zákona, který umožní odposlouchávat celý český internet, a to bez povolení soudu či jiných právních omezení.

HONZA ŠÍPEK

Ještě neutichly námitky proti sběru dat v rámci projektu EET, proti odesílání všech faktur podnikatelů státu v kontrolním hlášení DPH a proti centrálnímu registru bankovních účtů a politici z vládního ANO už přicházejí s daleko nenápadnějším, ale o to nebezpečnějším návrhem: chtějí dát vojenské tajné službě pravomoc umístit k poskytovatelům internetu „technické prostředky kybernetické obrany“, tedy „černé skříňky“, jež by mohly odposlouchávat, ale i modifikovat nebo blokovat provoz českého internetu. O novele zákona o Vojenském zpravodajství, která by dala vojákům široké pravomoci, se přitom skoro nemluví.

Kolize s ústavou

„Černé skříňky“ by mohly číst veškerý provoz na internetu a dále jej zpracovávat či ukládat: e-maily, zprávy v sociálních sítích, přehled o tom, jaké otevíráme stránky. Velká část dat je sice již šifrovaná, ale to se dá prolomit, anebo uložená data nechat na později, až bude dešifrování možné. Zákon to nijak neomezuje. Metadata – tedy údaje o tom, kdo s kým, kdy a odkud komunikoval – jsou navíc stále nešifrovaná. Přitom říkají často víc než obsah komunikace samotný. Prostřednictvím statistické analýzy lze velmi podrobně sledovat vztahy mezi lidmi, například zmapovat kontakty přátel, novinářů, aktivistů nebo politických stran či jejich odpůrců. Údaje o naší aktivitě na internetu navíc říkají nepříjemně mnoho o naší aktivitě v reálném světě: kde jsme, jak se pohybujeme, kdy chodíme spát, co nás zajímá.

Na zprávy přenášené internetem – ať šifrované či otevřené – se nicméně stále vztahuje listovní tajemství chráněné Listinou základních práv a svobod, která nám zaručuje právo na soukromí, i když připouští výjimky stanovené zákonem. Ty zde již máme: odposlechy policie i tajných služeb jsou možné na základě povolení soudem.

I současná praxe ale láká k pokusům o překročení hranic. „Teď se rozmohlo, že k nám opravdu často chodí policie. Víc než pětkrát týdně. Chodí kvůli klientům, chodí se na něco ptát, chtějí data, informace,“ říká Damir Špoljarič z hostingové firmy VSHosting v rozhovoru pro server Lupa. „Ve většině případů nesplňují to, co se po nich má chtít. My jsme provozovatel veřejné telekomunikační sítě, takže chceme soudní příkaz. Dost často se pak stává, že už se policie neozve.“ Tuto výpověď mimo záznam potvrzují i další provideři. Podle nového zákona však vojenské zpravodajství už nebude povolení soudu potřebovat, případně jej bude obcházet. Česká advokátní komora varuje, že novela „rozvolní ústavou zaručenou ochranu veřejnými sítěmi přenášených informací a vytvoří nástroj jejich možného zneužití bez efektivní kontroly ze strany nezávislého orgánu“. Zákon totiž nestanoví žádné limity. Suše říká, že „technické prostředky kybernetické obrany“ jsou umístěny na základě schválení vládou. Co bude rozvědka se sondami dělat, je již zcela v její moci.

Kybernetická obrana

Zákon se zaštiťuje nutností zavedení kybernetické obrany státu. Nikdo ale neřekl, jak by v tom sondy měly pomoci. Termín „kybernetická obrana“ navíc znamená něco jiného než „kybernetická bezpečnost“ – totiž „vojenské operace v kyberprostoru“. Kdyby stát chtěl bránit svou infrastrukturu, investoval by především do jejího „opevňování“ a „neprůstřelnosti“. Mohl by například provozovat kritickou infrastrukturu nezávisle na veřejné části internetu a komerčních poskytovatelích. Ani závažný výpadek veřejné sítě by pak neohrozil třeba řízení elektráren.

„Černé skříňky“ by mohly odposlouchávat, ale i modifikovat nebo blokovat provoz českého internetu. Foto archiv VUF

Už dnes existují vládní i nestátní skupiny CSIRT, které kyberútoky monitorují, vyšetřují a navrhují obranná opatření. Sdružení českých internetových operátorů po velkých DDoS útocích v roce 2013 (viz A2 č. 7/2013) založilo Projekt Fénix, dobrovolnou „vnitřní síť“ operátorů, jež by měla masivním útokům odolávat. Kyberútoky jsou medializované, věnuje se jim specializovaný počítačový bezpečnostní průmysl i analýzy odborníků. Ale vojáci a politici nemluví o žádných konkrétních opatřeních ani neříkají, jak by svůj systém využili v obraně státu. Jejich příklady se týkají nejčastěji sběru informací: „V textu SMS nebo mailu může být slovní heslo, které systém rozpozná a upozorní na to, že komunikace je vedena na téma, které má bezpečnostní riziko,“ vysvětloval například obhájce zákona Bohuslav Chalupa v Událostech, komentářích. Namístě je tak obava, že půjde zejména o zpravodajskou činnost. A zatímco politici přirovnávají sondy k banálnímu úsekovému měření rychlosti a ministr obrany Martin Stropnický straší nedávným výpadkem Googlu, vojenští rozvědčíci již jednají s providery.

Muž uprostřed

Poskytovatelé internetu jsou nejvíce znepokojeni tím, že sondy kromě pasivního odposlechu budou moci provádět i aktivní zásahy. Obávají se, že jim vojáci můžou třeba i v důsledku chyby rozbíjet sítě. To je závažné riziko, které bezpečnost tuzemského internetu spíš ohrožuje. Aktivní sondy umožní vojákům i přímé útoky – například na protokol https pro šifrované brouzdání po webu. Na zámeček ve webovém prohlížeči, který svítí, když komunikujeme například s bankou, se dá zaútočit z pozice „muže uprostřed“ (man-in-the-middle). Mezi mne a banku se postaví někdo, kdo se na jednu stranu tváří jako banka, na druhou jako já, a má tak přístup k oběma stranám komunikace. Nástroje útoku existují, ale narážejí na „strom důvěry“ vestavěný do prohlížeče či operačního systému, který obsahuje seznamy „důvěryhodných autorit“, jež mohou vydávat certifikáty – a prohlížeč nás na problém upozorní. Ale také si do systému můžeme nevědomě zavléct autoritu „ne zcela důvěryhodnou“. Paranoidní uživatelé, kteří zámečky zkoumají pečlivě, to asi prokouknou. Ale lidé, kteří jen „odklikli divnou tabulku“, stěží.

„Muž uprostřed“ může také spolupracovat s některou z autorit již důvěryhodných a nechat si od ní vydávat falešné certifikáty (v českém prostředí se nabízí certifikační autorita PostSignum, provozovaná Českou poštou). Aktivní sondy mohou vyměňovat programy, jež si stahujeme, za „cinknuté“ či do nich schovávat zadní vrátka. Platí to i o automatických aktualizacích. Mohou také vytvářet falešné stopy a předstírat, že proběhla komunikace, která neproběhla, za někoho se vydávat nebo komunikaci blokovat. V extrémním případě by se sondy mohly stát i „velkým českým firewallem“. Jakousi variantu černých skříněk si stát ostatně již nechal vyvinout. Fakulta informačních technologií brněnského Vysokého učení technického z grantu ministerstva vnitra provedla velký výzkum prostředků pro boj s kybernetickou kriminalitou a výsledkem byl mimo jiné i prototyp „vysokorychlostní sondy“ pro monitorování síťového provozu. K tomu škola vyvinula i software Netfox Detective na analýzu zachycené komunikace. Tyto sondy sice nelze jednoznačně propojit s novým zákonem a říct, že vojáci budou používat právě je. Víme ale, co si stát nechal vyvinout a co si případně může objednat ve větší sérii od komerčního dodavatele. Z brněnské akademické sféry se odštěpila mimo jiné firma Flowmon Networks, která škatule a software pro zachytávání provozu a jeho analýzu prodává. Zařízení na různé odposlechy, filtrování, ukládání provozu i jeho analýzy v masovém měřítku jsou ale byznysem i mnoha dalších specializovaných firem. Pořídit lze také komerční zařízení, které automaticky útočí na šifrovanou komunikaci, například zmíněnou metodou „muž uprostřed“. Proto by drobná úprava zákona, jež by zakázala sondám „aktivní“ provoz, byla pro skutečnou bezpečnost velikou úlevou.

V každém případě budou vojáci řešit buď problém, jak zpracovat ohromný tok dat v reálném čase, nebo problém, kam všechna ta data uložit, než je budou schopni zpracovat. Není to nic triviálního, ale také nic, co by se nedalo koupit za hodně peněz. Až „muž uprostřed“ přijde, budeme už muset umět šifrovat zatraceně dobře. Kdo z nás to umí?

Autor je dokumentarista.

napětí

Podle zpravodajství NBC News je možné, že Barack Obama ještě před odchodem z prezidentského úřadu omilostní bývalou vojenskou analytičku Chelsea Manningovou, která v roce 2010 poskytla 700 tisíc tajných vojenských a diplomatických dokumentů serveru WikiLeaks. Manningová byla za předání dokumentů a vyzrazení státního tajemství odsouzena na 35 let odnětí svobody, přičemž jí hrozil dokonce trest sta let vězení. Petici za její propuštění dosud podepsalo 116 tisíc lidí. Manningová byla odsouzena jako Bradley Manning, ale v průběhu výkonu trestu změnila jméno a podrobila se hormonální léčbě, která předchází změně pohlaví.

Běloruská spisovatelka Světlana Alexijevičová, která je držitelkou Nobelovy ceny za literaturu z roku 2015, vystoupila z ruského PEN klubu na protest proti tomu, že odmítl podpořit ukrajinského režiséra Oleha Sencova, jenž je od loňského roku vězněn v Rusku. Ze stejného důvodu již dříve opustilo řady PEN klubu několik desítek dalších ruských literátů. Sencov byl odsouzen za údajnou přípravu teroristických útoků na Krymu ke dvaceti letům vězení. O jeho propuštění žádá mnoho lidskoprávních organizací včetně Amnesty International.

Turecký prezident Recep Tayip Erdoğan pokračuje v čistkách proti svým politickým protivníkům a lidem, které považuje za nepohodlné. Tentokrát se výnosem tří prezidentských dekretů zaměřil především na turecké občany, kteří žijí v zahraničí. Řada z nich je ve své vlasti vystavena zpolitizovaným obviněním a podle nového nařízení se musí do tří měsíců od zahájení trestního stíhání vrátit do Turecka, jinak budou zbaveni státního občanství. Dále pokračuje propouštění státních zaměstnanců, policistů a akademiků, které se týká tisíců lidí.

Izraelci arabského původu 11. ledna neotevřeli školy, obchody a další veřejné podniky na protest proti cíleným demolicím arabských domů, jež provádí izraelská armáda. Stát tímto způsobem ničí domy postavené bez povolení – to je ale takřka nemožné získat. Naposledy došlo k podobné demolici v arabském městě Kalansuva, kde bylo zlikvidováno jedenáct domů. Ty sice neměly povolení, ale byly postaveny na pozemcích patřících jejich majitelům. Izraelští Arabové v současném Izraeli tvoří zhruba pětinu občanů.

Stát Izrael snížil svůj každoroční příspěvek OSN o šest milionů dolarů, protože nesouhlasí s nedávnou rezolucí Rady bezpečnosti OSN, která židovský stát nabádá, aby okamžitě přestal s výstavbou osad na okupovaném palestinském území.

–lr–