Tisková zpráva Digitální bezpečnost a soukromí

Praha, 30. 1. 2017

Experti: Novela zákona o Vojenském zpravodajství je nebezpečná, umožní na internetu sledovat všechny.

Sněmovna bude v druhém čtení projednávat novelu zákona o Vojenském zpravodajství. Ta dává vojenské tajné službě pravomoc umístit na internetové linky „černé skříňky“, jež by mohly odposlouchávat, ale i blokovat, či měnit provoz českého Internetu. Podle vojáků opatření pomůže kybernetické obraně státu. Počítačoví odborníci, právníci i poskytovatelé internetu však považují návrh zákona za zneužitelný. Ohrozí podle nich ústavní práva na soukromí i svobodu projevu a bezpečnost sítí může paradoxně výrazně zhoršit.

Novelu její překladatelé obhajují nutností kybernetické obrany státu. „Jsme přesvědčeni o tom, že nový zákon ve skutečnosti obraně nijak nepomůže a že jejím hlavním účelem je sběr informací. Pokud má Ministerstvo obrany nebo Vojenské zpravodajství pocit, že dokážou soukromé sítě firem bránit lépe než jejich specialisté, mohou jim například radit. Na to nepotřebují šmírovací novelu,“ říká Štefan Šafár, odborník na bezpečnost IT z platformy „Digitální bezpečnost a soukromí“ (DBaS), stojící za výzvou Přichází rozvědka [1], již k dnešnímu dni podepsalo přes 1400 signatářů.

„Nemáme nic proti tomu, aby si stát umístil technické obranné prostředky před sítě zajišťující státem provozovanou infrastrukturu a mohl tak chránit jím provozované služby i data, která o občanech potřebuje mít uložená. Perimetr takových sítí je nejlogičtějším místem, kde lze útoky na státem provozovanou infrastrukturu detekovat a reagovat na něj,“ říká odborník na počítačovou bezpečnost Pavel Růžička z iniciativy DBaS. „Stát má již teď spoustu jiných možností reakce na probíhající útok, např. spoluprací s bezpečnostními týmy CSIRT, či za pomoci NCKB. Pokud chtějí vojáci provádět odvetné kybernetické útoky, mohou si pronajmout linku coby běžný zákazník ve zvláštním režimu a se zvláštními podmínkami. S čím však nesouhlasíme je umisťování státem provozovaných zařízení do sítí soukromých subjektů, především pak takových, které fungují na principu masivního dohledu nad vším provozem,“ popisuje.

„Navrhovaná novela umožní vojenskému zpravodajství především sledovat občany. Nepomůže mu bránit český internet, ten si velmi dobře ve vlastním zájmu brání samy firmy, které sítě provozují. Rozhodně souhlasíme s tím, že je nutné řešit kybernetickou obranu, ale současně nesmíme udělat to nejhorší, co je možné. V podstatě jediný efektivní způsob obrany je široká spolupráce,“ doplňuje Šafár.

Zneužitelnost k odposlechům

K instalaci „černých skříněk“ (v novele definovaných pouze jako „prostředky kybernetické obrany“) by vojákům stačilo rozhodnutí vlády. Problém je v tom, že skříňky tak uvidí do veškeré internetové komunikace a efektivně tak umožní její odposlech. Soukromá komunikace je v ČR chráněna Listinou základních práv a svobod a každé narušení tohoto práva, stanovené zákonem, se váží na lékárnických vahách. Dosud byly odposlechy ze strany policie či tajných služeb možné pouze s povolením soudu, na základě prokazatelného podezření, na omezenou dobu a za soudem stanovených podmínek. I tak jsou množství odposlechů i časté skandály s jejich úniky předmětem kritiky. Oproti tomu novela zákona o Vojenském zpravodajství je ohromně vágní a dává vojákům pravomoci téměř neomezené.

„Jako taková nepřinese žádný posun k aktuálním otázkám kybernetické ochrany, pouze rozvolní ústavou zaručenou ochranu veřejnými sítěmi přenášených informací a vytvoří nástroj jejich možného zneužití bez efektivní kontroly ze strany nezávislého orgánu,“ uvedla v nedávném prohlášení [2] Česká advokátní komora. „Operátoři tak již nebudou schopni zaručit plnou důvěrnost komunikace zákazníků. Ústavně garantovaná ochrana listovního tajemství tak bude jednoznačně porušena,“ doplňuje komora.

Zastánci zákona tvrdí, že sledování konkrétního člověka by musel coby „zpravodajský prostředek“ povolovat soud. Problém je v tom, že pokud budou „černé skříňky“ nainstalovány na linky, nikdo nezjistí, co všechno sledují. „Technicky budou schopny sledovat plošně všechen provoz,“ varuje Pavel Růžička. Zastánci novely si podle něj často protiřečí: „Na jedné straně říkají, že nebudou plošně odposlouchávat všechny, současně ale mluví o tom, že budou v komunikaci hledat konkrétní klíčová slova. Takové vyhledávání rozhodně nelze provádět jinak, než vstupem do komunikace samotné. Celá idea zákonem vynucováného pronikání státu, prostřednictvím jím provozovaných síťových zařízení, do sítí soukromých subjektů je naprosto zcestná a je zásadním ohrožením demokracie a ústavou zaručených svobod,“ upozorňuje Růžička.

Velká část naší internetové komunikace je šifrovaná – přístup k emailu, komunikace s bankami, firemní VPN přenášející obchodní tajemství, či přenos zdravotnické dokumentace. Právě šifrování může vytvářet falešný pocit bezpečí. Ve skutečnosti jsou k dispozici i technologie a postupy, které umožňují šifrování prolamovat. Pokud se nepodaří prolomit přímo použitou šifru samotnou, je možné použít útok typu Man-in-the-Middle (MitM), pro nějž jsou právě černé skříňky – umožní-li zákon jejich „aktivní“ podobu – ideální platformou. Vojenské zpravodajství by tedy tímto získalo legální možnost vstupovat a např. i pozměňovat obsah šifrované komunikace.

Nedostatečná kontrola

Závažný problém je, že nikdo efektivně nezkontroluje, co budou sondy vojenského zpravodajství skutečně dělat. „Návrh zákona tedy představuje obrovský prostor pro

zneužití, u něhož je jen obtížně představitelné, že by ze strany Vojenského zpravodajství, mimochodem držitele anticeny pro Úředního slídila za rok 2013 za své angažmá v kauze Nagyová, nebyl využit k obcházení soudních povolení pro nasazování zpravodajské techniky či zjišťování informací o elektronických komunikacích," uvádí [3] Jan Vobořil z nevládní organizace Iuridicum Remedium, která se k iniciativě Přichází rozvědka připojila.

Nejhlasitější zastánce a zpravodaj novely, Bohuslav Chalupa (ANO), se snaží uklidňovat veřejnost „pětistupňovou kontrolou". Jmenuje interní kontrolu VZ, ministra obrany pod kontrolou premiéra a parlamentní komisi pro kontrolu Vojenského zpravodajství, které však sám předsedá. Těžko předpokládat, že rozvědka bude efektivně sama bránit svému zneužití. Ministr obrany, pod nějž vojenské zpravodajtsví spadá, je politik, aktuálně Martin Stropnický (ANO). A parlamentní komise nemůže vstupovat do živých kauz a pracuje pouze s informacemi, které jim zpravodajci sami předají.

Jistou nadějí by mohl být „druhý stupeň kontroly", jak jej navrhuje novela zákona o zpravodajských službách, která však stále neprošla parlamentem. „Nový expertní kontrolní orgán, složený z důvěryhodných, bezpečnostně prověřených a veřejností respektovaných občanů, by měl mít pravomoc provádět hlubší kontrolu všech tří tajných služeb. Zásadním problémem může být, že tento ‚důvěryhodnější' orgán bude konat pouze na základě podnětu orgánů parlamentních, které se, z důvodů svých omezených pravomocí, o potřebě provést hlubší kontroly nemusí dozvědět a tedy v mnoha případech pravděpodobně ani nebude potřebnou kontrolu iniciovat. Případné schválení novelizace fungování kontrolních orgánů tajných služeb je jistě zlepšením oproti současnému stavu, i přesto se ale lze oprávněně domnívat, že taková kontrola bude v mnoha případech nedostatečná," říká Pavel Růžička z platformy DBaS.

Hlavním prostředkem obrany proti zneužití by podle expertů měly být striktní limity, které vojákům dá sám zákon. V současném znění ale novela nijak nedefinuje, jak se bude se získanými daty nakládat, zda se budou moci ukládat, na jak dlouho a kdo k nim bude mít přístup. Nevylučuje ani například předání třetí straně. „Je třeba se na věc dívat ne z pohledu toho, co vojáci slibují, že budou či nebudou dělat, ale z pohledu toho, co jim zákon umožní," říká Pavel Růžička.

Obavy poskytovatelů internetu

Podle navrhovaného znění zákona tak můžou vojáci přijít za poskytovateli připojení a umístit na všechny odchozí linky do okolních sítí sondy, které budou schopny provoz nejen zachytávat a analyzovat, ale i modifikovat, tedy blokovat přístup k některým službám, či celým webům, v extrémním případě i např. podvrhávat důkazy na nepohodlné osoby. „Nepodezíráme vojáky z toho, že by to plánovali, ale zákon by tuto zneužitelnou pravomoc neměl dávat vůbec nikomu. Z takto vybudované sítě se může stát obdoba ruské státní šmírovací sítě SORM [4]. Pokud by novela prošla, byla by i tato extrémní varianta zcela legální," doplňuje Růžička.

„Tvrdí-li obhájci zákona, že jim půjde pouze o obecné informace o provozu, tzv. metadata, měl by to zákon stanovovat.“ Pro poskytovatele internetového připojení by to znamenalo ohromný rozdíl. Zařízení umístěné na odchozí linku, které bude mít neomezené “pravomoci“, je technicky něco úplně jiného, než pasivní odbočka internetového provozu a něco jiného je svod informací o metadatech (tzv. NetFlow). A právě novelou stanovená „aktivní“ role černých skříněk vzbuzuje v providerech obavy — černé skříňky mohou například nezamýšlenou chybou napáchat v jejich sítích zásadní škody a bezpečnost tuzemského internetu tak paradoxně ohrozí. “Jediná chyba v zabezpečení či nastavení systému tak může umožnit útočníkovi zaútočit na celou zemi. Navíc prvky pod cizí správou v síti operátora mohou narušit funkčnost a stabilitu sítě,“ uvedlo [5] minulý týden Sdružení pro internetový rozvoj (SPIR). Zákon nestanovuje rozvědce za případné chyby žádnou odpovědnost. Poskytovatelé internetu budou navíc vázáni mlčenlivostí a nebudou moci zákazníkům vysvětlit, proč k selhání sítě došlo. „Pro operátory neexistuje žádný opravný prostředek, popřípadě formalizovaná možnost přezkumu využívání těchto prostředků v síti operátora,“ uvedla již dříve [6] ICT Unie. Zákon navíc nevylučuje monitoring hlasových služeb a SMS — i to je vágnost, která je podle operátorů znepokojující.

„Novela si vyžaduje zásadní revizi, zásadní odbornou diskusi a zásadní změnu. Proto si myslíme, že poslanecká sněmovna by měla návrh odmítnout,“ říká Jan Vobořil, z nevládní organizace Iuridicum Remedium. Novela je podle něj i proto jedním z horkých favoritů na anticeny Velkého bratra, jež IuRe každoročně vyhlašuje. „O cenách bude dnes rozhodovat porota a budou vyhlášeny 16. 2.,“ doplňuje Vobořil.

Odkazy v textu:

[1] — Iniciativa Přichází rozvědka, https://prichazi.rozvedka.cz
[2] — Vyjádření České advokátní komory, http://www.cak.cz/scripts/detail.php?id=16787
[3] — Vyjádření IURE, http://www.slidilove.cz/content/poslanci-budou-rozhodovat-o-plosnem-sledovani-internetu-vojenskym-zpravodajstvim-0
[4] — Ruský šmírovací systém SORM, https://freedomhouse.org/sites/default/files/FOTN%202016%20Russia.pdf
[5] — Vyjádření SPIR, http://www.spir.cz/novela-zakona-o-vojenskem-zpravodajstvi-prinasi-do-internetoveho-prostredi-nova-rizika
[6] — Vyjádření ICTU, http://www.ictu.cz/fileadmin/user_upload/documents/Stanoviska___Komentare/2016/2016-05-23-HK-102_16-pripominky_ICTU.pdf

Kontakt pro média:

Pavel Růžička, DBaS, info@dbas.cz
Štefan Šafár, DBaS, +420 739 773 111
petice: https://prichazi.rozvedka.cz
twitter: @dbascz a #orwelluv_zakon