Úřad vlády České republiky
Nábřeží Edvarda Beneše 4
118 01 Praha 1

K rukám Mgr. Bohuslava Sobotky
Předsedy vlády České republiky

V Praze 30. ledna 2017

Vládní novela zákona o Vojenském zpravodajství a dalších zákonů (včetně novely zákona o elektronických komunikacích – Sněmovní tisk 931) – zajištění kybernetické bezpečnosti a kybernetické obrany ČR

Vážený pane premiére,

jménem níže podepsaných sdružení, profesních, zájmových a expertních organizací, které jsou součástí kybernetické infrastruktury ČR a které podporují snahy České republiky a jejích představitelů o zajištění bezpečného kyberprostoru, si Vás dovolujeme upozornit na některé skutečnosti, které dle našeho názoru vyplývají z navrhované novely zákona o Vojenském zpravodajství a souvisejících zákonů.

V Poslanecké sněmovně je v současné době projednávána novela zákona o Vojenském zpravodajství, ve které je navrhováno, aby Vojenské zpravodajství (VOZ) dostalo novou pravomoc a subjekty zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací novou povinnost. Pravomoc VOZ je založena na oprávnění umisťovat pasivní i aktivní prostředky kybernetické obrany do sítí provozovatelů sítí elektronických komunikací.

Při přípravě návrhu zákona nebyly vzaty do úvahy skutečnosti, které činí toto potenciální oprávnění VOZ velmi problematickým. Přestože je deklarovaným záměrem zákona zvyšovat kybernetickou bezpečnost a zajišťovat kybernetickou obranu země, může jeho implementací naopak dojít k ohrožení kybernetického prostoru České republiky a řady soukromých i veřejných institucí a organizací. Pokud se do sítí významných operátorů zapojí prvky pod správou VOZ, vznikne tzv. „single point of failure“, tedy jedno místo, kvůli jehož chybě bude možné napadnout všechny dotčené sítě najednou. Pokud tedy bude v zabezpečení či nastavení systému VOZ jediná chyba (což stoprocentně nelze vyloučit u žádné organizace) může toho útočník využít a lehce zaútočit na celou Českou republiku. Z indicií daných VOZ prostřednictvím médií o tom, jak bude celá činnost Národního centra kybernetických sil zajištěna, vyplývá, že vedení VOZ počítá s tím, že roky nebude umět činnost zabezpečit a na pozice expertů bude najímat absolventy VŠ.

Je nesporné, že se zapojením nových prvků do sítě operátora se pojí celá řada provozních rizik. Je prakticky nemožné garantovat bezpečnost a integritu sítě, jak vyplývá z povinnosti ze zákona o elektronických komunikacích. Pokud vlivem zařízení instalovaného VOZ vznikne jakákoliv mimořádná událost, je operátor nucen o této skutečnosti pomlčet – pokud tuto událost vůbec zaznamená, ale to jej nezbavuje odpovědnosti vůči uživatelům jeho sítě, což byl jeden z požadavků na úpravu zákona ze strany povinných subjektů. Může reálně nastat situace, kdy bude operátor sankcionován zákazníky anebo regulátorem za nedodržení kvality služby, ačkoliv tato skutečnost nastane kvůli zařízení VOZ.

Novela zákona také předpokládá aktivní využití prostředků kybernetické obrany, což znamená, že by VOZ mohlo v sítích operátorů provádět i kybernetické útoky a protiútoky. To naráží na dva zásadní problémy:

a) Vzhledem k tomu, že ČR je vnitrozemský stát EU, vede drtivá většina našich zahraničních propojů do sítí našich spojenců v EU a NATO. Generování útoků do těchto sítí by přirozeně bylo vnímáno velmi negativně.

b) Sítě operátorů jsou již dávno stavěny tak, aby detekovaly a eliminovaly případné kybernetické útoky (na základě zákona o kybernetické bezpečnosti, ale zejména z důvodů zajištění své vlastní ochrany). To tedy znamená, že by aktivity – útoky a protiútoky - ze zařízení VOZ byly oslabovány aktivními prvky sítě operátora a zároveň paradoxně detekovány a oznamovány operátorem ve smyslu povinností dle zákona o kybernetické bezpečnosti.

Jako naprosto nesystémové a nedomyšlené ze strany tvůrců zákona je, že novela míří pouze na provozovatele sítí elektronických komunikací. Tím jsou vyloučeny z obrany subjekty, které služeb operátorů nevyužívají, ale z hlediska kybernetického provozu jsou velmi významné. Může jít o významné poskytovatele obsahu (např. Seznam.cz, Google) nebo o mnohé nadnárodní subjekty, které mají vlastní spoje do peeringových center a do zahraničí, mj. i banky. Například nedávný krátký výpadek služeb společnosti Google jasně ukázal, jak je česká společnost na službách těchto poskytovatelů obsahu závislá. Z tohoto pohledu se jeví vymezení povinných subjektů jako účelové, nejasné, nelogické a nesystémové.

Je také alarmující, že ačkoliv je deklarováno, že zařízení VOZ nebudou provádět plošný odposlech, ze své podstaty přes ně bude nekontrolovaně procházet téměř veškerý internetový provoz. Ačkoliv to zákon vylučuje, bude technicky možné odposlechnout jakýkoliv provoz v síti (libovolného uživatele) pouze na základě rozhodnutí administrátora systému. To generuje vysoká bezpečnostní rizika v případě selhání konkrétního jedince nebo například v situaci, kdy nějaký hacker prolomí systém VOZ a využije tuto infrastrukturu ke svým cílům.

Jsme současně přesvědčeni o neefektivnosti navrhovaného řešení. V případě jiných (výrazně méně demokratických) zemí, které se snaží kontrolovat uživatele internetu a jejich infrastruktura je k tomu plně uzpůsobena, nelze hovořit o tom, že by zajištění kybernetické bezpečnosti a kybernetické obrany byla vyšší, a i průměrně technicky vzdělaní uživatelé mají celou řadu možností, jak případné státem vybudované překážky obejít. Z tohoto pohledu je tedy nesmyslné hromadit v rukou několika málo jednotlivců tak velké a tak zneužitelné oprávnění.

V neposlední řadě musíme zmínit rozhodnutí Evropského soudního dvora z prosince 2016, které konstatuje, že zákony umožňující plošný sběr a uchovávání lokalizačních a provozních údajů jsou v rozporu s právem EU.

Ve svém rozhodnutí Evropský soudní dvůr napsal, že plošné ukládání těchto dat, které zahrnuje například odesílatele a příjemce zprávy SMS a historii volání, umožňuje velmi přesně vyvodit závěry týkající se soukromého života osob, jejichž data byla takto uchovávána, a takováto právní úprava překračuje meze toho, co je nezbytné a nutné, a nemůže být považována v demokratické společnosti za odůvodněnou. Jakékoliv oprávnění, které má za cíl bojovat proti závažné trestné činnosti, musí podléhat předchozímu přezkoumání soudu anebo nezávislého orgánu. Vzhledem ke skutečnosti, že toto rozhodnutí bylo zveřejněno na konci minulého roku, nemohla ho Vláda ČR zohlednit při přípravě návrhu zákona.

Vážený pane premiére, s ohledem na výše uvedené Vás žádáme o pečlivé zvážení všech argumentů, pozastavení legislativního procesu, znovuotevření diskuze o podobě předkládaného návrhu zákona a jeho úpravu ve spolupráci s odborníky a zástupci průmyslu tak, aby byl co nejlépe naplněn veřejný zájem budování kyberneticky bezpečné a prosperující České republiky.

S pozdravem,

Ondřej Filip
Výkonný ředitel sdružení CZ.NIC

Zdeněk Zajíček,
Prezident ICT Unie

Martin Semrád
Ředitel sdružení NIX.CZ