SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

V PRAZE DNE 11. BŘEZNA 2020

Stanovisko Svazu průmyslu a dopravy České republiky k návrhu zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství (dále jen „návrh zákona“)

Kontext:

Ministerstvo Obrany dne 17.6.2019 zpřístupnilo relevantním subjektům od roku 2015 již třetí přepracovanou verzi novely zákona o Vojenském zpravodajství a požádalo relevantní subjekty o komentáře k tomuto textu ve lhůtě do 21.6.2019. Ministerstvo Obrany následně zpracovalo tyto připomínky a dne 7.1.2020 předložilo návrh zákona Legislativní radě vlády. V současné době se zákon nachází po úpravách v Legislativní radě vlády ČR a je zařazen na projednání vládou dne 16. 3. 2020.

Stanovisko Svazu průmyslu a dopravy České republiky (dále jen SP ČR):

SP ČR považuje za důležité bránit bezpečnost České republiky i v oblasti kyberprostoru, který se, vzhledem k rostoucímu využití digitálních technologií, stává stále významnějším. Bezpečnosti klíčových infrastrukturních prvků a systémů České republiky je nutné věnovat adekvátní pozornost, aby bylo možné včas zasáhnout proti kybernetickým nebo teroristickým útokům. Zajišťování bezpečnosti ČR však musí probíhat v co nejvíce možném souladu se zabezpečením dat a soukromí občanů ČR.

I přes dlouho trvající diskuze k návrhu zákona, nejsme stále přesvědčeni o tom, že došlo k adekvátnímu vypořádání připomínek, které byly průběžně k návrhům zákona uplatňovány ze strany našich členských firem, a to ani na základě semináře, který se uskutečnil dne 13. května 2019, kde byly připomínky soukromého sektoru prezentovány. Jsme proto nuceni konstatovat, že ani aktuální text novely zákona o Vojenském zpravodajství nevypořádává nejzásadnější připomínky, které byly k návrhu zákona uplatněny:

- Návrh zákona stále nereflektuje výhrady ke koncepčnímu pojetí, které ve stávající podobě představuje plošné a nepřetržité sledování veškeré komunikace na uzlech veřejných komunikačních sítí a u provozovatelů služeb veřejných elektronických komunikací (dále jen jako „provozovatel SEK“), aniž by k tomu byl předem dán souhlas soudem nebo státním zástupcem. Návrh zákona dle našeho názoru celou věc zjednodušuje přejmenováním dříve v textu používaného termínu „sonda“ na „nástroj detekce“ a pro sbíraná data o provozu pak používá neurčitý termín „metadata“. Metadata jsou však v tomto kontextu data popisující kdo s kým a kdy komunikoval, což bez pochyby představuje informace, které narušují oprávněné soukromí všech uživatelů veřejných komunikačních sítí a veřejných služeb elektronických komunikací, což v důsledku znamená i narušení oprávněného soukromí uživatelů služeb informační společnosti. Vojenské zpravodajství by tato metadata sbíralo v režimu 24/7, bez potřeby souhlasu soudu nebo státního zástupce a uchovávalo po prakticky neomezenou dobu.

TELEFON (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

- Návrh zákona popírá dosavadní zákonné postupy např. policejních orgánů dle zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen „trestní řád“), ve znění pozdějších přepisů, a dalších příslušných právních předpisů, kdy takový policejní orgán má k metadatům či provozně lokalizačním údajům přístup pouze na základě zákonné a odůvodněné písemné žádosti, a v případech, kdy je zasahováno do základních lidských práv a svobod, lze takový zásah ve smyslu § 158d odst. 3 trestního řádu uskutečnit pouze s předchozím povolením soudce. Novela zákona o Vojenském zpravodajství tak opravňuje Vojenské zpravodajství k tomu, aby si údaje prostřednictvím nástroje detekce opatřilo bez jakýchkoli překážek, neomezeně, kdykoli, a bez předchozího povolení soudu sledovalo průběh komunikace ve veřejných sítích elektronických komunikací.
- Návrh zákona je vnitřně rozporným v textu nového § 98a a textu stávajícího § 98 zákona č. 127/2005 Sb., o elektronických komunikacích, a to z důvodu, že jakékoliv cizí a neznámé zařízení v podobě nástroje detekce je při umístění k provozovateli SEK z principu kybernetickou hrozbou. Deklarovaná funkcionalita takového zařízení nemusí odpovídat jeho reálnému fungování. Stejně tak nebude v moci provozovatelů SEK zajistit, že nástroj detekce neobsahuje bezpečnostní zranitelnosti, které neumožní narušiteli získat skrze takové zařízení přístup do citlivé části SEK, aniž by tomu mohl provozovatel SEK zabránit. Návrh zákona ani po četných debatách neobsahuje bližší popis fungování „nástroje detekce“, jež by provozovateli SEK alespoň osvětlil základní principy, důležité pro zabezpečení jím provozovaných sítí nebo služeb.
- Návrh zákona explicitně nevylučuje, že nástroj detekce umísťovaný k provozovateli SEK nemůže být využit k aktivnímu zásahu Vojenským zpravodajstvím podle § 16e návrhu zákona.
- Zavedení institutu inspektora pro kybernetickou obranu v § 16j návrhu zákona, které by mělo představovat vyšší úroveň kontroly činnosti Vojenského zpravodajství v oblasti kybernetické obrany, považujeme za zcela nešťastné. Dle návrhu zákona je tento Inspektor pro kybernetickou obranu zároveň příslušníkem Vojenského zpravodajství. Takové nastavení negarantuje dostatečnou nestrannost. Přestože návrh zákona stanovuje, že výkon funkce musí inspektor provádět nestranně, lze od něj nestrannost za takových okolností, jakožto příslušníka Vojenského zpravodajství, jen těžko očekávat.
- Návrh znění § 16m odst. 4 návrhu zákona dává rozhodovací pravomoc v otázce přiznání náhrady škody nebo nemajetkové újmy v souvislosti s činností Vojenského zpravodajství výlučně do rukou Ministerstva obrany, kterému je Vojenské zpravodajství podřízeno – nikoliv do rukou nezávislého soudu, který by o její oprávněnosti a výši nestranně rozhodoval.
- Problematický zůstává v § 16k návrhu zákona navržený systém přezkoumávání podnětů fyzických a právnických osob v souvislostech se zajištěním jejich práv při výkonu činnosti Vojenského zpravodajství. Jednak Inspektor pro kybernetickou obranu nemá v zákoně uvedenou žádnou možnost ověřit skutkové okolnosti uvedené v podnětu fyzické nebo právnické osoby a jednak budou fyzické a právnické osoby obracející se na Inspektora vždy ve značné důkazní nouzi, neboť o chování umístěných „detekčních zařízení“ nebudou mít žádné informace, aby se mohli svých práv řádně domáhat.
- V návrhu zákona v novém § 98a odst. 2 zákona č. 127/2005, o elektronických komunikacích, se uvádí, že rozhraní pro připojení nástroje detekce nesmí umožnit předávat obsah detekovaných jevů provozu v SEK v opačném směru. Ani při čtení důvodové zprávy k této části návrhu zákona není zřejmé, co je zamýšleno touto formulací.

- Formulace ustanovení § 16f novely zákona o Vojenském zpravodajství není pro ochranu základních lidských práv a svobod dostatečná, jelikož už ze samotného principu umístění nástroje detekce na určený bod veřejné komunikační sítě dochází k permanentnímu sledování provozu. Nutno dále zdůraznit, že např. pojem tzv. „veřejného zájmu a zajišťování obrany státu“ není dostatečně určitý, a činí potenciálně jakýkoliv zásah Vojenského zpravodajství do základních lidských práv ve smyslu výše uvedeného ustanovený zákonným.

SP ČR pozitivně vnímá tu skutečnost, že se od představení první podoby návrhu zákona z kraje roku 2019 Vojenské zpravodajství alespoň snaží vyslechnout všechna oficiální i neoficiální připomínková místa ohledně možných vylepšení návrhu zákona. Bohužel, tato zpětná vazba není reflektována v návrhu textu, přestože soukromý sektor opakovaně nabízel konstruktivní návrhy řešení tak, aby bylo vhodněji vyhověno požadavkům Ministerstva obrany a Vojenského zpravodajství.

Zástupci Vojenského zpravodajství na pořádaném semináři 13.5.2019 přítomným odborníkům potvrdili obavy provozovatelů SEK, a to jak v případě sledovaného obsahu internetového provozu, možnosti data ukládat až po dobu 10 let a zpětně je tak analyzovat, tak i přes tyto uzly aktivně zasáhnout. Jsme přesvědčeni, že skrze položené otázky a jejich odpovědi se jen utvrdilo podezření odborné veřejnosti, že zvolené pojetí celého návrhu zákona je nutné zásadně zlepšit, a to za podpory technických expertů, důkladné analýzy možných funkčních dopadů do internetového provozu a odborné expertízy nad bezpečností přenášených dat uživatelů v případě, že bude konkrétní „nástroj detekce“ implementován do běžného provozu.

Stávající návrh zákona považuje SP ČR za velmi problematický a vyzývá Vojenské zpravodajství a Ministerstvo obrany, aby s privátním sektorem a odbornou veřejností zahájili skutečnou a seriózní diskusi o potřebách při kybernetické ochraně státu, ve které dnes naprosto zásadní a neoddiskutovatelnou roli hrají právě především zástupci privátního sektoru v České republice. Jsme přesvědčeni, že pokud by k tomu dalo Ministerstvo obrany a Vojenské zpravodajství prostor, tak privátní sektor je schopen v horizontu měsíců navrhnout funkční model splňující potřeby státu v oblasti kybernetické ochrany při zachování zabezpečení dat a soukromí občanů ČR.

Shrnutí – 5 požadavků:

- **Zajištění důvěrnosti komunikací -** „nástroje detekce“ nesmí umožnit sběr obsahu přenášených dat ani jakkoli narušovat jejich kryptografickou ochranu
- **Garance pasivních prvků -** pasivita „nástrojů detekce“ garantuje jak předchozí bod, tak chrání infrastrukturu
- **Zbavení odpovědnosti za škodu třetím stranám** (případně provozovateli v souvislosti s provozem zařízení) - činnost VZ v infrastruktuře operátora a provozovatele SEK může být příčinou výpadků nebo zhoršení kvality poskytované služby zákazníkům
- **Stanovení povinnosti uzavřít smlouvu -** smlouva jednoznačně definuje umístění „nástrojů detekce“, garanci dostupnosti, přístupu k zařízení a datům, technická omezení atd.
- **Provoz a zřízení budou na náklady žadatele** - veškeré náklady na provoz a pořízení zařízení, včetně energií a místa v datovém rozvaděči budou na náklady VZ.