Výbor Nezávislého ICT průmyslu

Jakub Rejzek
prezident

Zásadní stanovisko dotčených subjektů, expertů a průmyslu
k vládnímu návrhu novely zákona o Vojenském zpravodajství
a zákona o elektronických komunikacích

Ochrana kybernetického prostoru České republiky je klíčový veřejný a státní zájem dotýkající se národní bezpečnosti. Všechny zúčastněné subjekty, jejichž veřejné, obchodní i soukromé aktivity se odehrávají v kyberprostoru, usilují o minimalizaci rizik, které souvisí s kybernetickým světem - i v rámci dopadů online aktivit do světa reálného.

Navrhovaná novela zákona o Vojenském zpravodajství, ani úprava zákona o elektronických komunikacích snahy o zajištění bezpečného kyberprostoru zásadním způsobem neposiluje; naopak – může výrazně ohrozit zajištění kybernetické bezpečnosti sítí poskytovatelů internetového připojení, a tím přináší potenciálně nové hrozby a případná rizika, kterým bude potřeba čelit. Řešení představované novelou může mít ve většině případů zásadní negativní dopady na zajištění ochrany osobních údajů, komunikaci a soukromí uživatelů internetu.

ZÁSADNÍ VÝHRADY:

I. NESOULAD S LEGISLATIVOU EU – podle rozhodnutí Soudního dvora EU o zrušení směrnice ohledně Data Retention je plošný sběr provozních a lokalizačních údajů zakázaným zásahem do základních práv občanů EU;

II. NESOULAD S ÚSTAVNÍM POŘÁDKEM – návrh také porušuje práva na ochranu soukromí a listovního tajemství v ČR, existuje reálné riziko jejich prolomení (není totiž technicky možné provádět monitorování provozu bez nahlédnutí dovnitř takového provozu); návrh říká, že činností Vojenského zpravodajství nesmí být narušena důvěrnost obsahu zprávy - to neznamená záruky, že zpráva nemůže být pověřenou osobou přečtena;

III. NESOULAD S VNITROSTÁTNÍM PRÁVEM – návrh je v rozporu s povinnostmi vyplývajícími ze zákona o elektronických komunikacích (povinnost zajištění bezpečnosti a integrity sítí, § 98), zákona o kybernetické bezpečnosti a krizového zákona;

IV. VYLOUČENÍ KLÍČOVÝCH ORGÁNŮ Z JEDNOTLIVÝCH PROCESŮ – např. NÚKIB, který má za povinnost dotčené povinné subjekty a/nebo subjekty KII o kyberbezpečnostním incidentu informovat, může být novelou vyloučen z informačního řetězce a obranného procesu (stejně tak nadřízený subjekt – premiér); k zajištění ochrany osobních údajů příslušný orgán (ÚOOÚ) je vyloučen z legislativního procesu (připomínkového řízení);

V. ROZPOR V KOMPETENCÍCH – návrh zákona směřuje na zajištění pasivní kybernetické obrany a aktivní kybernetické obrany – zpravodajská činnost (monitoring datového provozu) není pasivní kybernetická obrana, plánovaná aktivní obrana musí být jasně v kompetenci Armády ČR;

VI. TECHNICKÁ NEKOMPABILITA – návrh zákona nedefinuje technické parametry tzv. sondy, která má být umístěna do sítí operátorů; nelze zaručit, že takový prvek bude možné bezpečně zapojit, zajistit a řídit, je velmi pravděpodobné, že předpokládané výpadky budou ohrožovat poskytované služby;

VII. NARUŠENÍ BEZPEČNOSTI A INTEGRITY SÍTÍ – jakýkoliv „cizí“ prvek implementovaný do komunikační sítě představuje potencionální bezpečnostní riziko, které může ohrozit nastavené služby, zejména povinnost zejména přenášet zprávy a data bez zásahu;

VIII. VÝZNAMNÉ ZVÝŠENÍ RIZIKA NAPADENÍ – s novými implementovanými prvky zpravodajských služeb, sondami, se sítě poskytovatelů internetového připojení stanou častějším a usilovnějším cílem akcí kybernetických útočníků zejména zvenčí, obrana proti těmto útokům s ohledem na nové, neznámé a dle zákona pro povinný subjekt nedotknutelné prvky v síti bude výrazně komplikovaná až nemožná.

Jakub Rejzek
prezident

IX. O NÁS A NAŠICH ZÁKAZNÍCÍCH BEZ NÁS – došlo k úplnému vyloučení odborné veřejnosti, zástupců a expertů malých, středních a velkých poskytovatelů veřejných sítí elektronických komunikací z diskuse, přípravy a připomínek v rámci novely zajištění ochrany kybernetického prostoru ČR;

X. **RESUMÉ: ŘEŠENÍ = MODEL 4 SIL**

Drtivá většina právních a technologických expertů ze soukromého sektoru, na základě svých hlubokých znalostí a zkušeností z ČR i zahraničí, je dlouhodobě přesvědčena, že ochrana kybernetického prostoru ČR by měla být budována na principu modelu funkčně oddělených kompetencí a pravomocí jednotlivých státních organizačních složek, v systému důsledné koordinace na nejvyšší národní a nadnárodní úrovni, za zajištění dostatečné nezávislé kontroly a minimalizace rizika zneužití pravomocí zejména s ohledem na jistý zásah do soukromí občanů a firem v prostředí online světa.

Za naprosto nepřípustný pokládáme argument, který je předkládán nejméně poslední 3 roky – tedy že Armáda ČR (AČR) nemá v tento okamžik kapacity vybudovat a provozovat jednotky kybernetické obrany a boje a že jediným subjektem, který je schopen tuto činnost zastat, může být Vojenské zpravodajství (VZ).

VZ má v tuto chvíli dostatečné nástroje a oprávnění k výkonu a plnění úkolu, ke kterému je primárně ze zákona určeno a jehož základ spočívá ve zpravodajské činnosti, a legislativa dle našeho názoru nesmí překročit tento rámec, a umožnit zpravodajské organizaci nekontrolovaně monitorovat internet či v něm dokonce provádět aktivní činnosti, narušovat soukromí občanů a firem a případně pozměňovat či modifikovat jejich komunikaci a osobní data.

Jsme plně přesvědčeni, že AČR je schopna vybudovat a provozovat jednotky kybernetické obrany, má k tomu jednoznačné předpoklady a je k tomu z hlediska obrany ČR jediným ze zákona určeným subjektem. Za soukromý sektor a průmysl jsme připraveni tyto aktivity podpořit a plně spolupracovat.

MODEL 4 SIL – je nezbytné ve spolupráci všech zainteresovaných subjektů zavést princip systémového zajištění prevence a represe v oblasti: kybernetické kriminality, kybernetické bezpečnosti, zpravodajských činností a kybernetické války; oddělení jednotlivých aktivit, jejich národní i nadnárodní koordinace, přísná a nezávislá kontrola, koordinace napříč sily na nejvyšší úrovni bezpečnostní a politické odpovědnosti – **tato novela takový princip nereflektuje a nepředstavuje!**