Odborné stanovisko IT Asociácie Slovenska k vládnemu návrhu zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony

Predložená novela zákona o kybernetickej bezpečnosti, ktorá má byť prerokovaná v Národnej rade SR v prvom čítaní ... marca 2021, má viacero rizík a ide nad rámec európskej legislatívy. V prípade novely zákona o kybernetickej bezpečnosti platí, že aj správna vec sa dá zneužiť.

Súhlasíme, že zmeny sú potrebné, nie však za cenu nadmerných obmedzení a ohrození pre používateľov. **Považujeme preto za mimoriadne dôležité upozorniť na možné riziká pripravovanej novely.** Ak by mal byť zákon schválený v súčasnom znení, **navrhujeme, aby sa radšej stiahol z rokovania Národnej rady SR na prepracovanie a aby sa pokračovalo v odbornej diskusii.**

Novela zákona prekračuje to, čo sa považuje za štandard v Európskej únii a obsahuje ustanovenia s viacerými rizikami. **Poslanci Národnej rady SR by sa preto mali hlboko zamyslieť nad tým, ako v prípade jej schválenia poslúžia občanom a podnikateľom.**

Považujeme za nelogické a aj neprípustné, že NBÚ pripravil novelu zákona o kybernetickej bezpečnosti **ešte pred predložením Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025**, ktorá by mala tvoriť rámec novely. Stratégia je sformulovaná ako východiskový strategický dokument, ktorý určuje prístup Slovenska k zvyšovaniu úrovne kybernetickej bezpečnosti. Novela zákona mala asi východiská iné – **v skutočnosti sa do znenia novely nepremietli princípy tohto dôležitého strategického dokumentu.**

„Národná stratégia kybernetickej bezpečnosti reflektuje strategické smerovanie štátu v oblasti kybernetickej bezpečnosti, zohľadňuje princípy Bezpečnostnej stratégie SR a vychádza aj zo strategických dokumentov NATO, EÚ, OECD a OSN,“ komentuje NBÚ. Súhlasíme s tým, čo sa uvádza v samotnej stratégii: *„Štát musí pri budovaní dôveryhodnosti a bezpečnosti vykonávať všetky aktivity v súlade s Ústavou Slovenskej republiky a **vstupovať do základných ľudských práv a slobôd len v nevyhnutnej miere.“*** Kľúčovou otázkou teda je, **prečo tieto isté princípy nerešpektuje aj novela zákona**. O to viac nás zaráža, že predkladateľom stratégie a aj zákona je ten istý Národný bezpečnostný úrad (NBÚ).

V Národnej stratégii kybernetickej bezpečnosti na roky 2021 až 2025 je okrem iného uvedené:
„Slovenská republika sa hlási k rešpektovaniu základných ľudských práv tak, ako sú zadefinované v Charte ľudských práv a presadzuje názor, že ľudské práva sú vykonateľné ako v „offline“, tak aj v „online“ priestore. ...

Kybernetický priestor musíme začať považovať za ekvivalent fyzického sveta, spolu s aplikáciou jednoznačných pravidiel, ktoré budú rešpektovať ústavou garantované základné ľudské práva a slobody, vrátane práva na súkromie tak, aby bol nielen bezpečný, ale aj otvorený, slobodný a prístupný pre všetkých, ktorí doň vstupujú. Bezpečnosť kybernetického priestoru musí byť prepojená s jeho slobodou a základné ľudské práva a slobody v digitálnom priestore je možné garantovať iba za predpokladu zachovania digitálnej suverenity krajín Európskej únie ako celku, čo zaručuje nezávislosť a suverenitu aj v kybernetickom priestore. ...

Národná stratégia kybernetickej bezpečnosti má právny základ v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a premieta povinný obsah, ktorý

je zakotvený v smernici Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii a bol transponovaný do predmetného zákona. ...

Zároveň štát musí pri budovaní dôveryhodnosti vykonávať vyššie uvedené aktivity v súlade s Ústavou Slovenskej republiky a ostatnými zákonmi a vstupovať do základných ľudských práv a slobôd len v nevyhnutnej miere."

Budovanie 5G sietí a ich bezpečnosť je v centre pozornosti Európskej únie, ktorá prijala tzv. Toolbox – strategické a technické opatrenia na zmiernenie rizík, ktoré majú posilniť integritu a bezpečnosť nových sietí. **Naša verzia ich implementácie však značne prekračuje rámec tohto Odporúčania EÚ**.

Návrh novely ide nad rámec aktuálne platnej Smernice NIS (Smernica Európskeho parlamentu a Rady EÚ 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Prekračovanie smerníc a odporúčaní Európskej únie (tzv. gold-plating) je známou slovenskou chorobou. Je jedným z hlavných dôvodov nezvládnutého čerpania eurofondov alebo nekonečných verejných obstarávaní.

Teraz sme v priamom prenose svedkami gold-platingu v oblasti kybernetickej bezpečnosti. Môže to viesť k tomu, že **podnikanie na Slovensku bude menej predvídateľné, nákladnejšie a občania si začnú zvykať na pocit, že môžu byť nepretržite sledovaní.**

O gold-platingu v tomto prípade hovoríme hneď v niekoľkých oblastiach:

a) Návrh novely ide nad rámec aktuálne platnej Smernice NIS.
b) Sektor elektronických komunikácií je už roky regulovaný v tejto oblasti európskym regulačným rámcom pre elektronické komunikácie (Kódex) a zákonom o elektronických komunikáciách, a preto nemá byť regulovaný v tej istej veci aj zákonom o kybernetickej bezpečnosti.
c) Už pri pripomienkovaní novely sa požadovalo, aby došlo k vypusteniu celého sektora elektronických komunikácií z regulačného rámca zákona o kybernetickej bezpečnosti, a to z dôvodu, že telekomunikačný sektor nie je predmetom Smernice NIS a je regulovaný vlastným regulačným rámcom. Jednoducho povedané, bezpečnostné požiadavky podľa zákona o kybernetickej bezpečnosti nie sú aplikovateľné na sektor elektronických komunikácií. Keby sa totiž v absolútnej miere uplatnili v praxi, išlo by o celoplošné nepretržité sledovanie.
d) Novela navyše rozširuje základné služby o ďalšie oblasti v sektore Digitálnej infraštruktúry, ako napríklad *„prevádzkovateľa obchodu na internete s možnosťou vyhľadávania, objednávania a nákupu tovarov a služieb",* čo je v rozpore so Smernicou NIS. Toto rozšírenie tvorca novely interpretuje ako spresnenie terminológie, čo už nie je regulácia, ale gold-plating.

Automatizované poskytovanie informácii je nielen technicky náročné a drahé opatrenie, ale vyvoláva aj množstvo otázok: **napríklad či je v poriadku, keď citlivé dáta občanov a firiem zhromažďuje štát, ktorý má za sebou bohatú históriu únikov informácií a ich zneužitia, na rozdiel od firiem, ktoré majú v oblasti ochrany dát oveľa lepšiu povesť.**

Nepretržité sledovanie systémových informácii zo sietí a informačných systémov vybraných prevádzkovateľov základných služieb na základe určenia NBÚ **môže priniesť výrazný zásah aj do súkromia občanov.** Toto opatrenie je možno vhodné pre internú komunikáciu v niektorých štátnych inštitúciách, ale určite nie vo firmách a verejných komunikačných sieťach a službách. **Navyše to prináša vysoké riziko úniku citlivých informácií vzhľadom na skutočnosť, že úroveň zabezpečenia**

v bankovom či telekomunikačnom sektore je vyššia ako na strane vládnych organizácií (napr. nedávny únik dát z NCZI).

Zákaz používania produktu, procesu alebo služby môže viesť **k poškodeniu záujmov podnikateľských subjektov a to bez účasti dotknutých firiem a mimo procesov správneho konania**. Ak zároveň firmám nebude známa analýza rizík, proces nákupu zariadení sa stane vysoko rizikovým. Opäť je to nad rámec odporúčaní EÚ. Oprávnenie má byť použiteľné na všetkých prevádzkovateľov základných služieb nielen do budúcna, ale aj spätne, pričom zámerom EÚ je regulácia len pre oblasť budovania 5G sietí. **Spätne predstavuje určitý zásah do vlastníckeho práva, k čomu má dôjsť bez kompenzácie a mimo správneho konania.** Ide o široké oprávnenie NBÚ zakázať alebo obmedziť ktorémukoľvek prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu pod pomerne vágne koncipovanou podmienkou *„ak používanie neumožňuje alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb alebo ak ohrozuje bezpečnostné záujmy Slovenskej republiky“.*

Aj keď sa vopred stanovujú presnejšie kritéria a riziká, ktoré musí NBÚ bližšie vyhodnocovať, a požaduje sa vyjadrenie Bezpečnostnej rady ako ďalšieho subjektu vstupujúceho do procesu rozhodovania, pôjde o rozhodovanie mimo správneho konania **bez procesnej účasti dotknutých prevádzkovateľov. Vnáša to nepredvídateľnosť do podnikateľského prostredia a tiež možné odklonenie od princípov voľného trhu presadzovaného Európskou úniou aj v Odporúčaní Tooboxu.**

Opätovne žiadame úpravu týchto ustanovení, minimálne jasnejšie pravidlá, pokiaľ ide o určenie primeranej doby potrebnej na výmenu už obstaraných zariadení (napr. 7 rokov od zverejnenia rozhodnutia) a právo na kompenzáciu nákladov vynaložených na zariadenia pred vydaním rozhodnutia. Zároveň žiadame prístup k Analýze rizík, aby mohli firmy prijať primerané opatrenia na ich mitigáciu.

Ide o citlivú tému z pohľadu nastavenia právneho rámca tak, aby sa rešpektovali princípy ochrany základných práv a slobôd, či princípy sieťovej neutrality. Blokovanie takzvaného škodlivého obsahu alebo škodlivých aktivít, ktoré môžu zapríčiniť bezpečnostný incident sa má naviac diať **bez predchádzajúceho súhlasu súdu a len na základe rozhodnutia NBÚ.** Nevieme však, kto bude mať systémový dozor nad činnosťou NBÚ (rozhodnutie bude aspoň preskúmateľné súdom), ani akým spôsobom sa štát postaví k prípadným hospodárskym škodám, ktoré takto môžu vzniknúť.

Je nevyhnutné, aby sa v zákone výslovne deklarovala aj **transparentná garancia zodpovednosti za škodu**. Za prípadnú škodu spôsobenú vykonaním blokovania musí zodpovedať NBÚ. Taktiež musí byť jasne definovaný dohľad a kontrola nad činnosťami NBÚ v tejto oblasti.