Úřad vlády České republiky
Legislativní rada vlády České republiky
Pracovní komise pro hodnocení dopadů regulace (RIA)

V Praze 23. 10. 2020
Čj.: OVA 1184/20

Stanovisko

k návrhu zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

I. Úvod

Cílem novely zákona dle předkladatele je:

a) provedení nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). Podle tohoto nařízení musí každý členský stát určit jeden nebo více vnitrostátních orgánů certifikace kybernetické bezpečnosti na svém území a stanovit pravidla pro sankce za porušení nařízení;

b) jasnější vymezení pravomocí Vládního a Národního CERT umožňující vytvoření národního systému vyhledávání a hodnocení zranitelností, což by mělo přispět ke zvýšení efektivity zajišťování kybernetické bezpečnosti v České republice.

II. Připomínky a návrhy změn

Definice problému (1.2)

Pokud jde o část věnovanou adaptaci aktu o kybernetické bezpečnosti, lze konstatovat, že problém je definován jasně. Předkladateli lze pouze doporučit vypuštění posledních dvou odstavců týkající se procesu přijímání aktu o kybernetické bezpečnosti, protože z hlediska hodnocení dopadů regulace navrhované novely zákona nemají význam.

Část věnovaná vyhledávání a hodnocení zranitelnosti lze považovat za příliš obecnou, k definici problému se vztahuje toliko obsah prvních dvou odstavců, zbylé dva už předjímají řešení problému („*Četnost a rizikovost základních zranitelností lze … snižovat … zapojením systémů, které u sledovaných systémů automatizovaně monitorují verze*“) a hodnotí jej („s *vynaložením poměrně nízkých nákladů*“, celý poslední odstavec). Z této části tedy vyplývá, že počet útoků v kyberprostoru roste a že úroveň zabezpečení informačních a komunikačních systémů je nedostatečná. Bohužel tato tvrzení předkladatel nedokládá žádnými údaji (např. počty útoků v čase, objem napáchaných škod), ani informací, z čeho např. vycházel při hodnocení úrovně zabezpečení (o jaké studie či analýzy se opíral). Uvedení jednoho příkladu (Psychiatrická nemocnice v Kosmonosech) je sice ilustrativní, pokud jde o dopad kybernetického útoku, ale o rozsahu problému a nutnosti přijetí regulace na úrovni zákona nevypovídá vůbec nic.

Dále zcela chybí zhodnocení nezbytnosti státní regulace, tedy zjednodušeně řečeno, proč nepostačuje (dosavadní?) soukromoprávní aktivita subjektů, které tyto sítě a systémy provozují, resp. povinných osob podle zákona o kybernetické bezpečnosti (částečně se o tom předkladatel zmiňuje v části věnovaných variantám řešení – např. otázce přístupu do mezinárodních databází;

tyto části ovšem patří sem). Zejména v případě orgánů státu, nebo státem zakládaných či zřizovaných subjektů by bylo vhodné uvést, zda byla přijata opatření (řídící akty, politiky apod.) k omezení či eliminace uvedených hrozeb a zda se osvědčila či nikoliv.

V podstatě se zde (v rozporu se zásadami hodnocení dopadů regulace) předjímá řešení problémů – zjednodušeně řečeno, předkladatel rovnou navrhuje, že by se měly problémy definované v prvních dvou odstavcích řešit tím, že Vládní a Národní CERT mají poskytovat služby vyhledáváním a hodnocením zranitelností. Je ovšem možné (a jeví se to tak i z jiných částí závěrečné zprávy), že problémem, který má návrh zákona řešit, je ve skutečnosti vyřešení otázky, zda může či nemůže Vládní či Národní CERT provádět některé činnosti a v jakém rozsahu (či pro koho). Právě v jiných částech závěrečné zprávy se hovoří o nejednoznačnostech vymezení pravomocí Vládního či Národního CERT a o možných rizicích s tím spojených (např. „*omezení dostupnosti služeb vyhledávání zranitelností pro ty orgány a osoby, které nemají dostatečné personální, technické či jiné kapacity k tomu, aby vyhledávání zranitelností ve svých systémech samy prováděly"*). Přitom tyto pasáže patří právě do části věnované definici problému. Předkladatel by měl tedy uvést, jaké služby jsou v této oblasti nyní poskytovány (ať už Vládním či Národním CERT nebo soukromými subjekty) a jaké to vyvolává či nevyvolává problémy.

V kapitole věnované návrhům řešení se pak navrhují varianty, které se liší okruhem subjektů, jimž mají být služby poskytovány, ale opět chybí vazba na definici problému (protože definice problému se o otázce okruhu subjektů vůbec nezmiňuje).

Popis existujícího právního stavu v dané oblasti (1.3)

Pokud jde o část věnovanou vyhledávání a hodnocení zranitelností, i zde se bohužel promítají nedostatky zmíněné v souvislosti s kapitolou 1.2. Pokud tam předkladatel rovnou předjímá způsob řešení (Vládní a Národní CERT mají poskytovat služby vyhledávání a hodnocení zranitelností), je skutečně nevyhnutelné se zde zabývat tím, zda takovou pravomoc v zákoně mají či nikoliv.

Předkladatel by se (po provedení změn v kapitole 1.2) měl zabývat i tím, proč např. nepostačuje soukromoprávní regulace v této oblasti, nebo jaké jsou nedostatky současné právní úpravy v případě veřejnoprávních subjektů, pokud jde o možnost zřizovatele, zakladatele či nadřízeného orgánu uložení jim přijetí opatření za účelem odstranění zranitelností.

Cílový stav (1.5)

Cílový stav, pokud jde o část věnovanou vyhledávání a hodnocení zranitelností, je opět popsán **velmi obecně** (druhý odstavec). Předkladatel by měl v návaznosti na jasně formulovanou definici problému (zejména pokud jde o rozsah) upřesnit cílový stav. Pokud by byl problém vymezen např. tak, že skupina X subjektů kategorie Y (např. státní nemocnice) nemá v současnosti provedenou analýzu zranitelností, pak cílovým stavem je (například), že všechny státní nemocnice budou mít alespoň jednou ročně provedenu takovou analýzu.

Bez jasné definice problému a cílového stavu nelze posoudit, zda má právní regulace vůbec nějaký smysl a zda má za tím účelem smysl vynakládat prostředky.

Třetí odstavec (s výjimkou první věty) svým obsahem v podstatě náleží do kapitoly 1.2. Ani čtvrtý odstavec systematicky do kapitoly 1.5 nenáleží, neboť spíše popisuje jedno (jediné) navržené řešení problému. Vysloveně matoucí je pak věta „*Nejedná se přitom o faktické rozšíření činností Vládního, resp. Národního CERT, jelikož obě tato pracoviště již v současnosti aktivity spočívající ve vyhledávání zranitelností vykonávají v rámci plnění ostatních zákonných povinností.*" Pokud tedy již tyto aktivity vykonávají v rámci jiných zákonných povinností, proč je třeba měnit zákon?

Návrh variant řešení

U variant řešení lze jen obtížně odhadnout, zda se vztahují k řešení problému či nikoliv, pokud není problém jasně vymezen a zda vedou k dosažení cíle, pokud ani cíl není jasně vymezen. Celkově chybí vazba na definici problému, neboť najednou zde předkladatel představuje varianty, jež se liší

rozsahem subjektů, jimž budou poskytovány služby, či typem infrastruktury, jíž se má tato činnost týkat.

Není zřejmé, proč předkladatel pominul variantu, že by uvedené činnosti vykonával jiný subjekt na komerční bázi (alespoň pro vymezený okruh subjektů).

Vyhodnocení nákladů a přínosů

Pokud jde o vyhledávání zranitelností, nulová varianta velmi obecně popisuje možné náklady (*„náklady nulové varianty tak budou spojeny především s nápravou škod v důsledku kybernetických útoků“*), aniž bychom ovšem věděli, o jaké náklady se jedná a kdo je ponese (viz též absence jakéhokoliv pokusu o kvantifikaci rozsahu problému v kapitole 1.2). Dále zcela chybí vyhodnocení nákladů/úspor v personální oblasti či materiálním zabezpečení (i při jeho obnově), pokud by byla zvolena tato varianta.

U dalších variant chybí zcela vyhodnocení nákladů na personální a materiální zabezpečení (a jeho obnovu), chybí i odhad, jak by mohla vzrůst intenzita vykonávaných činností – předkladatel pouze uvádí nicneříkající „*náklady této varianty se odvíjí od potřeby intenzity provádění činností vyhledávání a hodnocení zranitelností*“.

III. Shrnutí připomínek ke zprávě z hodnocení dopadů regulace (zpráva RIA)

PK RIA uplatňuje následující zásadní připomínky:

1. Je nezbytné, aby byl text zprávy RIA logicky konzistentní, aby jedna část navazovala na druhou ve smyslu připomínek uvedených ve zprávě Pracovní komise RIA výše (zejména definice problému – cílový stav – varianty, které k němu vedou).
2. Je třeba správně formulovat jednotlivé části zprávy RIA v duchu Obecných zásad a jejich smyslu.
3. Ve zprávě RIA je nezbytné dopracovat části týkající vyhledávání a hodnocení zranitelnosti, zejména:
   a. Jasně popsat současný stav, definovat problém a uvést, proč se se stávajícími nástroji nedaří problém odstranit; dále doplnit údaje o rozsahu problému (kvantifikace škod, počty útoků apod.);
   b. Popsat cílový stav jako specifický výsledek uplatnění/implementace navrhovaného zákona a uvést alespoň řádově kvantifikované údaje o minimálním žádoucím cílovém stavu, z nichž bude zřejmé, že popsaný problém bude alespoň částečně (byť i z velmi malé části) vyřešen.
   c. Uvést návrh variant, které budou vycházet z popisu problému a cílového stavu, zohlednit i variantu, že by uvedené činnosti vykonával jiný subjekt;
   d. U variant identifikovat náklady a přínosy (úspory), a provést alespoň odhad změn v intenzitě vykonávané činnosti. Kvantifikace je důležitá i v případě, kdy se bude jednat o odhady s přesností na řád – budou-li odhady smysluplně zdůvodněny, je to přijatelné.
   e. Pro každou variantu zpracovat porovnání nákladů a přínosů a pak porovnat navzájem náklady a přínosy jednotlivých variant, všude, kde to bude možné kvantitativně, a kde to není možné, alespoň kvalitativně.
   f. Výběr zvolené varianty důsledně zdůvodnit na základě nákladů a přínosů, a to tak, že vazba mezi volbou varianty a náklady a přínosy uvedenými dříve bude jasná na první pohled.

IV. Závěr

Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace **na základě posouzení zprávy z hodnocení dopadů regulace doporučuje** Legislativní radě vlády**, aby projednávání návrhu zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů přerušila za účelem přepracování návrhu předkladatelem ve smyslu** výše uvedených **zásadních připomínek.**

Vypracoval: Mgr. Zdeněk Mandík

prof. Ing. Jiřina Jílková, CSc.
v. r.
předsedkyně komise