Úřad vlády České republiky

LEGISLATIVNÍ RADA VLÁDY ČESKÉ REPUBLIKY
PRACOVNÍ KOMISE PRO HODNOCENÍ DOPADŮ REGULACE (RIA)

V Praze 25. 10. 2016
Čj. OVA: 1297/16

Stanovisko

k návrhu zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

I. Úvod

Jak uvádějí předkladatelé, cílem návrhu zákona je transpozice směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Rovněž návrh zákona zapracovává některá ustanovení, která by měla řešit problémy zjištěné na základě aplikační praxe zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „směrnice“) musí být v souladu s právem Evropské unie zapracována do českého právního řádu ve stanovené transpoziční lhůtě.

Předkladatelé analýzy dopadů regulace (RIA), se drželi standardní struktury hodnocení RIA a každý z bodů hodnocení velmi precizně zpracovali včetně hodnocení variantních přístupů a konceptů.

II. Připomínky a návrhy změn

Problém a cíle řešení

Zpracovatelé navrhované právní úpravy se snažili především naplnit minimální požadavky na standardní zabezpečení kritické informační infrastruktury a významných informačních systémů a rozšířit je i na informační systémy provozovatelů základních služeb, respektive správců a provozovatelů informačních systémů základních služeb, a zajistit vládnímu dohledovému pracovišti v reálném čase přehled o kybernetické bezpečnostní situaci v rámci subjektů spadajících pod regulaci zákona o kybernetické bezpečnosti.

Provozovatelům základních služeb, správcům informačních systémů základních služeb a provozovatelům informačních systémů základních služeb zajistí navrhovaná právní úprava nepřetržitý kontakt s vládním dohledovým pracovištěm umožňující kvalitnější identifikaci kybernetických bezpečnostních rizik s původem mimo příslušný systém, službu nebo síť, efektivnější analýzu kybernetických bezpečnostních událostí a účinnější reakci na kybernetické bezpečnostní incidenty.

PK doporučila předkladateli:

- **doplnit v této části informace o IA (Impact Assessment – hodnocení dopadů na úrovni EU) k výše zmiňované směrnici EU 2016/1148,**
- **upřesnit, jaká opatření navrhovaná v novele jdoucí nad požadavky transpozice jsou uvažována a jaké náklady s tím budou spojeny (gold plating).**

Varianty a analýza dopadů

V analýze dopadů jsou rozvedeny i dopady ekonomické, jejichž odhady se provádějí jen obtížně, protože se formy kyber-kriminality rychle rozvíjejí spolu s novými technologickými a softwarovými možnostmi.

Nesmírně obsažná a náročná se jeví etapa vyjednávání s dotčenými subjekty a resorty. Zápis z mezirezortního projednávání činí více jak 200 stran a velká část připomínek rezortů vedla ke zkvalitnění jak textu zákona, tak i ve zkvalitnění hodnocení RIA.

Mnoho diskuzních otázek a připomínek při mezirezortním projednávání i v diskuzích s dotčenými subjekty souviselo s definicí „Provozovatele základní služby“, základní informační infrastruktury.

V hodnocení RIA předkladatelé uvádějí, že se kategorie provozovatelů základních služeb fakticky částečně kryje s již existujícími prvky kritické infrastruktury, resp. kritické informační infrastruktury, které jsou určovány podle zákona o kybernetické bezpečnosti a zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů (krizový zákon), směrnice však zavádí některé nové odvětvové a průřezové parametry pro určovací kritéria.

Analýza ekonomických dopadů se týká zejména institucí, které budou podléhat regulaci jakožto povinné osoby. Bude se jednat o náklady na implementaci bezpečnostních opatření a plnění dalších povinností podle zákona o kybernetické bezpečnosti, dále pak personální náklady a potenciální náklady vzniklé zvýšením sankcí. Je zřejmé, že vzniknou náklady Národnímu bezpečnostnímu úřadu jakožto správním orgánu odpovědnému za oblast kybernetické bezpečnosti. V obou příkladech by bylo dobré uvést upřesněné kvalifikované odhady.

Parametry dopadových kritérií pro určení provozovatelů základních služeb jsou stanoveny ve směrnici, přičemž konkretizovány budou v prováděcím právním předpisu k zákonu o kybernetické bezpečnosti.

Podle směrnice se jedná o tyto parametry:

- počet uživatelů závislých na službě poskytované daným subjektem;
- závislost dalších odvětví na službě poskytované daným subjektem;
- možný dopad incidentů (intenzita a trvání) na ekonomické nebo společenské činnosti nebo na veřejnou bezpečnost;
- podíl daného subjektu na trhu;
- zeměpisný rozsah oblasti, která by mohla být incidentem dotčena;

- důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby;
- s přihlédnutím k dostupnosti alternativních způsobů jejího zajištění;
- případné zvláštní okolnosti podle jednotlivých odvětví.

Zde zaslouží pozornost další, ve směrnici neuvedený parametr související s „Hybridním charakterem nepřátelského působení“ v rámci politické destabilizace země nebo celé EU – dezinformačními weby. Případně globální hrozby nezodpovědným nebo účelovým – destruktivním zneužívání „sémantického webu“. Otázku větší regulační inherence v síťových službách rozvádí a relativizuje např. ČNB.

ČNB k bodu 5 (§ 2, doplnění písm. h), odvětví bankovnictví):

„ *Jedná se zde o bezdůvodnou širší interpretaci přílohy č. II ke směrnici 2016/1148 – směrnice pokrývá pouze instituce podle čl. 4(1) nařízení č. 575/2013, tj. podnik, jehož činnost spočívá v přijímání vkladů nebo jiných splatných peněžních prostředků od veřejnosti a poskytování úvěrů na vlastní účet“, zatím co v novele ZoKB toto omezení není – navrhujeme tedy definici přizpůsobit unijnímu právu.*
Pojem bankovnictví dnes není vymezen, banky mohou kromě přijímání vkladů a poskytování úvěrů provádět různé další činnosti na finančním trhu, včetně různého zprostředkování, obchodování se zlatem aj. Tyto další aktivity zpravidla nejsou spojeny s tak vysokým rizikem kybernetických útoků jako výše zmíněná oblast.“ **Předkladatel ve své reakci odkládá zúžení jednotlivých oblastí do Vyhlášky. Je tedy na místě otázka, kdy bude tato vyhláška k dispozici? Jak bude selektivita uplatnění zákona prakticky naplňována?**

PK RIA dále doporučuje, aby předkladatel v analýze hodnocení dopadů upřesnil zajištění dostatečného sledování dodržování požadavků novely povinnými osobami (track record) a s tím spojené náklady.

Ministerstvo dopravy ve svých připomínkách uvádí skutečnost, která se týká procesních, řídících a zabezpečovacích systémů integrovaných v dopravních procesech. Předkladatel správně reaguje ve smyslu Evropské směrnice. Např. současné zpracování dat o pohybu vozidel (i vozidel bezpečnostních služeb apod.) probíhá v mýtném systému částečně i mimo území ČR a náš stát nemá dohled nad bezpečností nakládání s těmito daty.

Pokud se týká využití zkušeností a analýz dopadů obdobných zákonů v zemích EU, předkladatel uvádí přednosti naší legislativy ve srovnání s průměrem EU. **Bylo by dobré doplnit ukázku „Best practice“ z vybrané členské země EU.**

III. Závěr

PK RIA předložené hodnocení dopadů regulace přijímá s doporučením dopracování dle výše uvedených připomínek.

Vypracoval:

prof. Ing. Petr Moos, CSc.

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