|  |  |
| --- | --- |
| **Název materiálu:** | **Novela zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti** (návrh zveřejněný HK 19. 7. 2016) |
| **Jméno:** | František Fejgl, Jana Osadská |
| **Telefon :** | 602 108 487, 220225459 |
| **e-mail:** | frantisek.fejgl@rwe.cz, Jana.Osadska@net4gas.cz |

1. **SHRNUTÍ HLAVNÍCH DOPADŮ PŘEDLOŽENÉHO MATERIÁLU**
2. **ZÁSADNÍ OBECNÉ PŘIPOMÍNKY**

1. Návrh novely zákona má zabezpečit transpozici Směrnice Evropského parlamentu a Rady 2016/1148/EU ze dne 6. července 2016 o opatřeních k zajištění vysoké úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen Směrnice NIS), která musí být implementována do právních předpisů členských států až k datu 9. května 2018. Není nám zřejmý důvod takto překotné implementace zvláště, když české znění této směrnice bylo vydáno až 19. 7. 2016 a dotčené subjekty tak neměli dostatečný časový prostor na seznámení se s touto směrnicí a provedení analýz možných dopadů na jejich podnikatelské aktivity.

2. Nesouhlasíme se způsobem zpracování RIA. Postup při provádění RIA je dán Obecnými zásadami pro hodnocení dopadů regulace (RIA) schváleným usnesením vlády ze dne 14. prosince 2011 a změněnými usnesením vlády ze dne 8. ledna 2014 č. 26 a usnesením vlády ze dne 3. února 2016 (dále jen „Zásady RIA“), k níž máme následující výhrady:

• Podle bodu 9.2 Zásad RIA jsou povinnou součástí RIA konzultace s dotčenými subjekty. Vyhodnocení konzultačního procesu je pak povinnou součástí Závěrečné zprávy hodnocení dopadů RIA. Přestože předložený návrh byl projednáván ve dvou pracovních skupinách, nebyly v nich dostatečně zastoupeny dotčené subjekty, zejména z oblasti energetiky, kde zcela absentovali zástupci plynárenských společností, kterých se předložený návrh dotýká ve značném rozsahu, s dopadem do hospodaření daných subjektů a mající finanční dopady na trhy, kterých se daný předpis bude týkat.

• V důvodové zprávě zcela absentuje kvantifikace dopadů návrhu na soukromý sektor. Vyčíslení dosavadních nákladů na zavádění bezpečnostních opatření v informačních a komunikačních systémech kritické informační infrastruktury a významných informačních systémech podle stávajícího zákona o kybernetické bezpečnosti, které je uvedeno v RIA, je zavádějící.

3. Předložený návrh zákona předpokládá, že v oblasti základních služeb budou dotčené subjekty určeny NBÚ na základě kritérií, které budou uvedeny v prováděcím předpise k tomuto zákonu. Jelikož kritéria pro určení dotčených subjektů a následný dopad právní úpravy na dotčené subjekty je stěžejní součástí uvedeného návrhu zákona, je nutno, aby samotný zákon stanovil uvedená kritéria, neboť by se pak v případě určení těchto kritérií prováděcím právním předpisem mohlo jednat o doplnění zákona, a ne o jeho provedení, což je dle ustálené soudní judikatury nepřípustné. Předložený návrh zákona svou stručností a neurčitostí nedává nutný základní rámec pro podzákonný právní předpis, který by konkretizovat problematiku upravenou v základních rysech již samotným zákonem.

Negativum spatřujeme i v absenci návrhů navazujících prováděcích právních předpisu, čímž vzniká právní nejistota, jak bude konkrétní situace u daného dotčeného subjektu posuzována, jaký rozsah ICT systémů bude do legislativy spadat, jaká část dodavatelského řetězce bude muset být zapojena a jaké povinnosti vyplynou danému subjektu (správcům) a navazujícímu ICT dodavatelskému řetězci (provozovatelům). Připomínáme, že v případě energetických společností podléhajících regulaci představuje realizace opatření, které pro tyto společnosti budou vyplývat z novelizace zákona, navrhnout, rozpočtovat, projednat s Energetickým regulačním úřadem a následně implementovat finančně, organizačně i personálně náročná bezpečnostní opatření v mimořádně komplexním firemním ICT prostředí s řadou implementačních rizik. Nezbytnost komplexní konzultace s Energetickým regulačním úřadem je z pohledu regulovaných činností v rámci odvětví energetiky (distribuce a přenos elektrické energie, distribuce a přeprava plynu) zcela zásadní zejména z pohledu případné možnosti uplatnění investičních výdajů na úpravu či pořízení navazujících ICT systémů.

4. Směrnice NIS požaduje jednotné uplatňování definice základních služeb v členských státech (viz. bod 19 preambule směrnice) a k zajištění konzistentního přístupu pak v článku 11 odst. 3 to uvádí jako jeden z úkolů „skupiny pro spolupráci“. Podle článku 24 má být ale tato skupina ustavena nejpozději k 9. únoru 2017, přičemž je na tento proces stanoveno období od 9. 2. 2016 do 9. 11. 2018, takže nevidíme důvod pro horlivý způsob implementace směrnice, který byl v ČR zvolen.

5. **Nesystematické zapracování „Základních služeb“ a „Informačními systémy Základní služby“, neřešené překryvy s plynárenskými KI a KII/KKI**

V současnosti účinné znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti (zákon o kybernetické bezpečnosti) představuje existující komplexní právní úpravu specificky zaměřenou na bezpečnost informací a elektronických komunikací s úzkou vazbou na zákon o krizovém řízení. Transpozicí Směrnice NIS se pod režim zákona o kybernetické bezpečnosti vztáhnou další subjekty poskytující „Základní služby“ podporované „Informačními systémy Základních služeb“.

Stávající legislativa již NIS problematiku základních služeb v energetice pokrývá v Kybernetickém zákoně a v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ČR již v současné době patří mezi evropské lídry v oblasti kybernetické bezpečnosti a oproti ostatním členským státům i EU jako takové je již značně napřed. Legislativa je oproti Směrnici NIS vyspělejší celkovou koncepcí, úrovní zpracování i úrovní detailu. Předložená novelizace zavádí nové NIS termíny „Základní služba“ a „Informačním systém Základní služby“ a definuje povinnosti jejich správcům a provozovatelům a přitom nedostatečně řeší překryvy a duplicity s již zavedenými termíny a v hlubší úrovni detailu má zjevné koncepční a logické mezery.

**Závěr:**

**Z výše uvedených důvodů požadujeme přerušení projednávání předloženého návrhu, také s ohledem na to, že ČR již základní legislativu pro tuto oblast má a na transpozici je stanoveno období 21 měsíců. Neměli bychom tedy Směrnici NIS Direktivu překotně „přilepovat“ k existujícímu zákonu a znepřehlednit a znehodnotit existující právní rámec. Naopak navrhujeme časový prostor využít k vyladění a vyjasnění případných duplicit a překryvů (například v termínech, postupech, numerických kritériích a koncepci).** Jako příklad uvádíme: Současná legislativa předpokládá elektronickou komunikaci jako typickou součást procesů zpracování informací a definuje kromě informačního systému též komunikační systém, NIS komunikaci Informačních systémů Základních služeb exaktně neřeší.

**Z pohledu energetických společností požadujeme přistoupit k nové verzi transpozice Směrnice NIS tak, aby dotčené subjekty byly zatíženy jen skutečně nezbytně nutnými náklady.**

1. **ZÁSADNÍ KONKRÉTNÍ PŘIPOMÍNKY**

**K § 4 odst. 5 - Mlčenlivost subjektů a jejich zaměstnanců jako doplnění nad rámec transpozice**

Nesouhlasíme s navrženým ustanovením odstavce 5, kterým by orgány a osoby uvedené v § 3 písm. c) až f) a jejich zaměstnanci byly povinni zachovávat mlčenlivost o připravovaných a přijatých bezpečnostních opatřeních.

**Odůvodnění:**

Povinnost mlčenlivosti představuje v návrhu novely zákona o kybernetické bezpečnosti jako doplněk nad rámec transpozice Směrnice NIS.

Z důvodové zprávy je patrno, že důvodem pro legislativní zakotvení mlčenlivosti je údajné „značné bezpečnostní riziko úniku citlivých informací“. Je zmíněna snaha zabránit vyzrazení „citlivých údajů“ týkajících se zabezpečení sítí a informačních systémů a obava, že únik „citlivých informací“ by ohrozil provádění bezpečnostních opatření. V odůvodnění novelizace však zcela chybí kvalitativní i kvantitativní data k tomuto „bezpečnostnímu riziku“, v kolika případech skutečně došlo k úmyslnému či neúmyslnému vyzrazení těchto údajů právě zaměstnanci dané společnosti, jaké množství, jakého typu a v jaké úrovni detailu uniklá data byla, zda to reálně ohrozilo realizaci bezpečnostních opatření a jaká je velikost tohoto rizika v porovnání s ostatními kanály úniku dat (dodavatelé, státní správa, externí útočníci) a ostatními riziky obecně. Lze se tedy domnívat, že se jedná o navození tíživé situace bez řádné analýzy tohoto úzce specifického rizika a nyní jsme v tzv. FUD stavu (Fear-Uncertainty-Doubt).

Legislativa se z celé problematiky „Insider Threat“ zaměřuje toliko na subjekty uvedené v návrhu § 3 písm. c) až f) a jejich kmenové zaměstnance a diktuje velmi kontroverzní a archaické řešení – sjednat a dodržet blíže neurčený závazek mlčenlivosti, a to pod správní pokutou jak pro podnik, tak pro desítky jeho zaměstnanců.

Typově návrh spadá do Security through obscurity“, a je ve značném rozporu se současným trendem globální spolupráce států a dotčených subjektů k potlačení kybernetické kriminality. Nesystémovost, nedostatek argumentace a nezvážení alternativ je zarážející, účinnost a vymahatelnost bude velmi omezená.

Argumentace se opírá o obdobné ustanovení zákona č. 127/2005 Sb., o elektronických komunikacích, který však vymezuje rozsah mlčenlivosti u citlivých údajů zřejmě (odposlechy, záznamy zpráv, lokalizace účastníků, výpisy realizovaných hovorů), kde se jedná o snadno ohraničitelnou interní provozní situaci, o letitou a zavedenou praxi, o relativně malý počet interních zaměstnanců a o pochopitelnou a prakticky realizovatelnou záležitost. Situace v kybernetické bezpečnosti v energetice je však naprosto odlišná a s telekomunikacemi nesouměřitelná.

Souhlasíme, že bezpečnostní detaily ICT technologií by neměly být volně dostupné a snadno dohledatelné ve veřejných informačních zdrojích, většina úspěšných podniků si daná rizika uvědomuje a řeší je. Většina subjektů v ČR se nachází v raných fázích ISO PDCA cyklu a musí se soustředit na řadu výzev. Navrhujeme problematiku znovu projednat v širším okruhu dotčených subjektů, zpřesnit a vymezit rozsah předmětu utajení a zvážit alternativní koncepce a formulace.

Stávající zákon o kybernetické bezpečnosti představuje relativně novou a komplexní právní úpravu. Její zavedení v energetice představuje mnohaletý proces se zapojením významného procenta útvarů dotčených subjektů i samotných zaměstnanců. Mimo jiné to představuje opakovaně navrhovat, rozpočtovat, projednat s Energetickým regulačním úřadem a následně implementovat finančně, organizačně i personálně náročná bezpečnostní opatření v mimořádně komplexním firemním ICT prostředí s řadou implementačních rizik. Připomínáme, že opatření vyžadují vysokou míru expertízy a specializace, kde kompetenční a kapacitní nároky na dané experty převyšují možnosti interních zdrojů, ty běžně doplňujeme externími konzultanty z oboru kybernetické bezpečnosti. Připomínáme, že v energetice obecně sílí tlak na snižování nákladů a tlak na modernizaci ICT, které vedou k situaci, kdy ICT prostředí zahrnuje vysoký podíl outsourcingu a komplexní dodavatelské řetězce. Navíc lze výhledově v ČR očekávat komoditizaci ICT ve formě cloudových služeb a intenzívní zapojení globálních cloud poskytovatelů.

Zapojení dodavatelů (včetně ICT) je i v energetice regulováno zákonem č. 134/2016 Sb., o zadávání veřejných zakázek se značnou mírou zveřejnění a transparence.

Do kybernetických bezpečnostních opatření v energetice jsou tedy v různých fázích životního cyklu zapojeny desítky interních zaměstnanců, desítky externích konzultantů, desítky státních zaměstnanců na straně regulace a desítky až stovky zaměstnanců dodavatelských firem.

Silným trendem v energetice i kybernetické bezpečnosti je intenzívní spolupráce v rámci odborných komunit, expertních skupin a specializovaných konferencí na regionální i EU úrovni, za plynárenství zmiňujeme ČPS a GIE, za ICT sdružení AFCEA. Od spolupráce očekáváme oborově specifickou Threat Intelligence a sdílení nejlepších zkušeností, osvědčených technologií, dodavatelů a expertů. Očekáváme komunitní sdílení a následnou oponenturu zvažovaných bezpečnostních opatření.

Stávající znění zákona o kybernetické bezpečnosti se aktivně odkazuje a intenzívně čerpá z ISO norem rodiny ISO 27000, jedním z nosných konceptů ISO norem je nastavení PDCA cyklu a nastavení procesu postupného zlepšování.

**Povinnost mlčenlivosti existuje v návrhu jako doplnění nad rámec NIS transpozice a žádný časový tlak či závazný konečný termín na řešení této tématiky nám není známý.**

**Vedle toho je třeba zdůraznit, že ve vazbě na nařízení EU o ochranně osobních údajů č. 2016/679/EU, existuje riziko dalších komplikací a vícenákladů pro dotčené soukromé subjekty, protože podle jejího článku 90 mohou členské státy přijmout zvláštní pravidla, aby stanovily pravomoci dozorových úřadů ve vztahu ke správcům nebo zpracovatelům osobních údajů.**

**Alternativní návrh** – Většina dotčených subjektů má interně definovaný systém klasifikace informací. Na řadu energetických subjektů navíc dopadá zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákon o krizovém řízení, které nakládání s klasifikovanými informacemi řeší (např. informace na stupni “vyhrazeno“, „zvláštní skutečnosti“) a dále také zákon č. 224/2015 Sb., o prevenci závažných havárií.

S ohledem na výše uvedené lze konstatovat, že pro účinnou ochranu klasifikovaných skutečností lze využít existující legislativu. Případně lze do zákona o kybernetické bezpečnosti zavést povinnost dotčených subjektů informace a informační aktiva analyzovat, klasifikovat a náležitě chránit a dále povinnost interně klasifikovat informace o opatřeních na nejvyšší stupeň. Informace by pak byly chráněny během transferu, během uložení i během použití a daná problematika by byla podchycena koncepčně a odborně.

**K § 2 písm. k) – on line tržiště**

Požadujeme jednoznačně specifikovat, na jaké subjekty se vztahuje termín „on-line tržiště“.

**Odůvodnění:**

Z obecného výkladového stanoviska lze pod pojem „on-line tržiště“ podřadit všechny společnosti nabízející jakoukoliv službu na internetu. Dále jsou v návrhu zákona definované ještě kategorie „internetové vyhledávače“ a „služby cloud computingu“. Definice všech těchto skupin jsou však dost vágní a tak se zatím přesně neví, na koho se povinnosti z návrhu zákona budou vztahovat. Pro provozovatele digitálních služeb bude situace o to těžší, že se budou muset v zákoně sami identifikovat, anebo vyčkat na prováděcí předpis ze strany NBÚ, který bude definovat jednotlivé požadavky na konkrétní začlenění pod citovanou novelu zákona. Z pohledu energetických společností nevnímáme začlenění do kategorie „on-line tržiště“ jako adekvátní krok z hlediska kybernetické bezpečnosti, neboť v porovnání s ostatními poskytovateli těchto služeb se nám jeví zařazení do kategorie jako nadbytečné. Ve všech společnostech je to jenom další kanál pro uzavření smluvního vztahu se zákazníkem, nicméně nejsou provozovány platební brány (v celém procesu se nejedná o on-line předávání informací z platebních karet).

**K § 12 odst. 3 – zveřejňování informací o kybernetickém bezpečnostním incidentu**

Nesouhlasíme s navrženým ustanovením § 12 odst. 3, které opravňuje NBÚ z důvodu veřejného zájmu a po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, informovat veřejnost o tomto incidentu nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám.

**Odůvodnění:**

Předně bychom chtěli upozornit, že navrhované ustanovení není transpozičním ustanovením, jelikož jde nad rámec Směrnice NIS. Z důvodové zprávy není patrno, jak by zveřejnění kybernetického bezpečnostního incidentu mohlo vést k jeho předcházení nebo zvládnutí. V navrženém ustanovení navíc zcela absentují měřítka a kritéria, kterými by se měl NBÚ při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu řídit.

Za držitele licencí na přepravu a distribuci plynu si dovolujeme upozornit na nebezpečí zveřejňování kybernetických bezpečnostních incidentů. Z logiky věci máme za to, že široká medializace kybernetického bezpečnostního incidentu neprospěje, spíše uškodí. Upozorňujeme, že veřejnost (i odborná) má velmi povrchní znalosti detailů řízení přepravy a distribuce plynu, včetně průmyslových řídicích systémů a provázání tzv. provozních technologií s IT technologiemi. Zveřejnění kybernetických bezpečnostních incidentů ve smyslu katastrofických scénářů kybernetických útoků a senzacechtivost médií tudíž vyvolává přehnané reakce veřejnosti na sebemenší podnět. Jako negativní aspekt vidíme i možné poškození pověsti či obchodních zájmů provozovatelů základních služeb a poskytovatelů digitálních služeb, kteří incidenty ohlašují, nelze opomenout ani následný mediální tlak na dotčený subjekt. Jako konkrétní příklad uvádíme nedávnou negativní zkušenost provozovatele přepravní soustavy, a dále také kauzu malware v nukleární elektrárně patřící skupině RWE v Bavorsku.

Jako účelnější a bezpečnější postup navrhujeme zakotvení povinnosti informování odborné komunity o kybernetickém incidentu, konkrétně členy oborových organizací v plynárenství a členy oborových organizací v ICT bezpečnosti a uplatnit klasifikaci informací (např. „semafory“ používané při sdílení informací mezi CERT teamy). Pouze část informací (např. s klasifikací „bílého semaforu“) by byla následně poskytnuta odborné veřejnosti.

Praha 9. 8. 2016