Problémy Návrhu zákona o kybernetickej bezpečnosti

Daniel Olejár[1]

Prečo je potrebný Zákon o informačnej/kybernetickej bezpečnosti

- digitálne informačné a komunikačné technológie predstavujú v súčasnosti kritickú infraštruktúru každej vyspelej spoločnosti, Slovensko nevynímajúc
- spoľahlivé fungovanie IKT je nutným predpokladom toho, aby štát mohol plniť svoje základné funkcie vo vnútri i navonok
- IKT sa stali cieľom intenzívnych a sofistikovaných útokov (počítačová kriminalita, vojna v kybernetickom priestore), okrem toho ich ohrozujú prírodné vplyvy, technické poruchy, ľudské chyby a omyly, nedostatky sw a hw[2]
- ochrana IKT musí byť preto systematická a komplexná, nestačí chrániť vybrané systémy, ale celú národnú informačnú a komunikačnú infraštruktúru
- to si o.i. vyžaduje aj primeraný legislatívny základ

Ako vznikol

- Vláda SR schválila v roku 2010 legislatívny zámer zákona o informačnej bezpečnosti; zákon bol síce vypracovaný (2014), ale MF SR ho nepredložilo do legislatívneho procesu
- na rokovanie NR SR bol predložený vládny Návrh zákona o kybernetickej bezpečnosti, ktorý mal vychádzať z Legislatívneho zámeru zákona a mal spojiť
    - zákon o informačnej bezpečnosti a
    - Direktívu EÚ NIS[3]
- Návrh zákona mali podľa uznesenia vlády[4] vypracovať MF SR a NBÚ, ale zákon nakoniec pripravil NBÚ bez **účasti MF SR a odbornej verejnosti** (hoci sa v Dôvodovej správe tvrdí opak)

Prečo nie je dobrý

- pripravovala ho uzavretá skupina, bez komunikácie so širšou odbornou verejnosťou,
- už k návrhu zákona v MPK bolo vznesených 706 pripomienok, z toho 236 zásadných

[1] mim. profesor, prorektor pre IT Univerzity Komenského v Bratislave
[2] aktuálne Spektrum a Meltdown
[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[4] Uznesenie Vlády SR 93/2016

- predkladateľ uvádza, že pripomienky boli vysporiadané, ale hoci návrh prešiel úpravami, ktoré vylepšili jeho formálnu stránku, zásadné problémy návrhu zákona ostali nevyriešené

1. navrhovaný **zákon nespĺňa uznesenie Vlády**; implementuje len Direktívu NIS a nerieši ochranu IKT v rozsahu, ktorý bol definovaný Legislatívnym návrhom zákona o informačnej bezpečnosti (a ktorý je pre fungovanie štátu nevyhnutný);

2. aj **implementácia Direktívy NIS** navrhovaným zákonom je sporná, pretože samotná Direktíva sa vzťahuje len na vybrané prvky kritickej (informačnej) infraštruktúry a explicitne uprednostňuje, aby ich ochranu riešili špeciálne zákony. (Okrem toho od členských štátov vyžaduje vytvorenie kontaktných komunikačných bodov, výmenu informácií a účasť v pracovných grémiách.) Navrhovaný zákon ide nad rámec požiadaviek Direktívy NIS.

3. **povinnosti NBÚ** – zákon ukladá NBÚ povinnosti, na ktoré nemá personálne kapacity (štandardizačná, metodická[5] a kontrolná činnosť), ktoré predtým vôbec nerobil (akreditácia jednotiek CSIRT, tvorba znalostných štandardov, koordinácia výskumu a vývoja, audit). Tieto úlohy mal Úrad plniť podľa Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti, porovnanie Návrhu zákona a Akčného plánu a výsledky za dva roky sú uvedené v prílohe.

4. zákon dáva Úradu **možnosť presunúť plnenie** bližšie nešpecifikovaných **úloh na externý subjekt** (fyzickú osobu), §5 ods. 2, čím by výkon verejnej moci mohol prejsť na súkromný subjekt

5. **konflikt záujmu** – Úrad je zároveň kontrolným aj výkonným orgánom pre kybernetickú bezpečnosť; najvypuklejšie sa to prejavuje v akreditácii CSIRT-ov, ktorú robí Úrad, ktorý má zároveň postavenie Národnej jednotky CSIRT. Tá má postavenie akreditovanej jednotky bez akreditácie.

6. **Jednotný informačný systém kybernetickej bezpečnosti, JISKB.** Bližšie nešpecifikovaný „magický“ systém s funkcionalitou webovej stránky, jednoduchej databázy a komunikačného rozhrania, ktorý má plniť kľúčové úlohy (povinný komunikačný kanál, informačný zdroj, analytický nástroj). Jednotlivé funkcie takého systému sa dajú realizovať pomocou štandardných systémov/aplikácií (web, databáza, SIEM[6]); takýto systém bežne používajú organizácie CSIRT (pozri napr. CSIRT.SK). JISKB je potenciálny *single point of failure* riadenia kybernetickej bezpečnosti v SR, lebo sa (zbytočne) predpisuje jeho povinné používanie pri hlásení bezpečnostných incidentov. Vývoj takého systému môže byť drahý a dlhý a sám o sebe žiadne problémy nevyrieši.

7. **Terminológia.** Zákon umelo oddelil informačnú a kybernetickú bezpečnosť a zavádza nové pojmy pripájaním prívlastku kybernetický. Odvoláva sa na Direktívu NIS, ale tá pojednáva o informačnej bezpečnosti a slovo kybernetický sa v nej spomína raz. Vo svete

[5] http://www.dsl.sk/article.php?article=20669

[6] security information and event management (SIEM), https://en.wikipedia.org/wiki/Security_information_and_event_management

je zaužívaná terminológia informačnej bezpečnosti a kybernetická bezpečnosť sa chápe ako informačná bezpečnosť kybernetického priestoru/alebo technickej informačnej a komunikačnej infraštruktúry[7]. Z vecného hľadiska je kybernetická bezpečnosť podmnožinou informačnej bezpečnosti, čo sa nakoniec prejavuje aj v zákone a návrhu vykonávacích predpisov, ktoré explicitne vychádzajú zo štandardov informačnej bezpečnosti. Umelo zavedené „kybernetické" pojmy sú nejasné, majú sporné definície, čo spôsobí problém s implementáciou zákona (v slovenskej legislatíve sa používa terminológia informačnej bezpečnosti) a medzinárodnou kompatibilitou (svet našim pojmom nebude rozumieť) Navyše existuje len jediný ISO štandard pre kybernetickú bezpečnosť, čo sa prejavuje aj v samotnom zákone a Tézach vykonávacích predpisov, ktoré sa opierajú o normy informačnej bezpečnosti (premenovanej na kybernetickú).

8. protirečivosť zákona.

a) Podľa § 2, ods. 2 sa zákon o KB sa nevzťahuje na utajované skutočnosti, (ako aj na ďalšie ustanovenia iných osobitných právnych prepisov uvedených v poznámkach pod čiarou) pričom v prílohe č. 1 základných služieb sa im vymedzuje nový osobitný sektor/podsektor (viď. „Sektor 10 Verejná správa" aj s príslušnými podsektormi),

b) zákon o KB sa nevzťahuje na najdôležitejšie systémy štátu, vrátane všetkých systémov kritickej infraštruktúry (podľa zák. č. 45/2011 Z.z.), vrátane ďalších osobitných právnych predpisov uvedených v poznámke pod čiarou), pričom tieto subjekty sú duplicitne uvedené v tabuľke základných služieb[8] v prílohe č.1, čo znamená, že tu opäť ide o zásadný rozpor,

c) špecifický prípad – návrh zákona najprv zmenou zákona 45/2011 zo sektora kritickej infraštruktúry *Informačné a komunikačné technológie*, obsahujúci podsektory Informačné systémy a siete a Internet (spadajúci pod MF SR) vytvoril sektor *Verejná správa* s jedným podsektorom *Informačné systémy verejnej správy* a priradil ho Úradu podpredsedu vlády, pričom z neho vyňal správu domén a kľúčových prvkov Internetu a tú priradil NBÚ[9] (Príloha 1). V zákone o kritickej infraštruktúre aj Návrhu zákona ostáva sektor *Elektronické komunikácie* (kam by správa Internetu a domén prirodzene patrila) pod Ministerstvo dopravy. Systémy, ktoré nie sú ISVS ostali bezprizorné.

d) tieto rozpory sa prejavujú najmä v prípadoch ak pôjde o prvky kritickej infraštruktúry; otázne je napr. podľa akých kritérií sa budú prvky zaraďovať, vyraďovať, kontrolovať, kto je ich správcom, prevádzkovateľom[10], kto ponesie zodpovednosť za sektory, ktoré sú podľa Návrhu zákona definované tak, že zodpovednosti sú duplicitné, dokonca aj triplicitné.

e) Do tabuľky základných služieb sú „duplicitne" začlenené sektory kritickej infraštruktúry podľa zákona č. 45/2011 Z.z. Ide o ich plnú kópiu. Opäť ide o duplicitu a zásadný rozpor, pretože podľa „§ 2 odseku 2 písm. f)" návrhu sa na tieto prvky zákon o KB nevzťahuje, pričom tabuľka v prílohe č. 1 je základom tohto návrhu zákona, kde si zároveň úrad

[7] ešte aj v USA, kde pojem kybernetický priestor vznikol, majú ako lex generalis pre túto oblasť Federal information security management act; ISO má cca 200 noriem venovaných informačnej bezpečnosti a jedinú kybernetickej bezpečnosti

[8] opakovane sa uvádza správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené

[9] NBÚ v tejto oblasti v minulosti nič nerobil

[10] zoznam týchto prvkov podľa zák. č. 45/2011 Z.z. je neverejný

uplatňuje právo ukladať opatrenia (pozn.: ukladanie opatrení podľa tohto návrhu zákona (viď. § 20) je všeobecný a široký pojem, takže môže zahŕňať aj zásahy úradu, alebo ním povereného subjektu do kompetencií, organizačnej štruktúry, personálnych opatrení atď., ako aj do správy systémov iných subjektov).

9. **Odborné nedostatky** v informačnej bezpečnosti.

a) kľúčový problém je zlá interpretácia, nepochopenie a nekonzistentné používanie základných pojmov (pozri §20, ods. 1 a 2 – opatrenia, vzťah klasifikácie informácií a kategorizácie systémov), odvolávanie sa na neexistujúce štandardy, mechanické opisovanie z rôznych ISO noriem bez zosúladenia a prispôsobenia kontextu (§20, ods. 2 a 3; §27, ods. 7, protirečivosť pojmov §24, ods. 2, §27, ods. 4 a i.), čo vedie k rozporným/nelogickým/nezrozumiteľným tvrdeniam, nerealizovateľným požiadavkám, resp. nedostatočným riešeniam.

b) Návrh vníma kybernetickú/informačnú bezpečnosť predovšetkým z administratívno-byrokratického hľadiska (tvorba dokumentov, koncepcií, politík, správ, akreditácie, vedenie evidencie), čo spolu s implementáciou štandardných bezpečnostných opatrení nepochybne prispeje k zvýšeniu bezpečnosti jednotlivých systémov, ale nerieši bezpečnosť celého priestoru a nepostačuje na predvídanie a riešenie nových bezpečnostných problémov.

c) ciele kybernetickej bezpečnosti, z ktorých vyplývajú povinnosti pre poskytovateľov služieb (§22, ods. 2), sú formulované vágne/rozporne;

d) nevhodné úpravy štandardných bezpečnostných postupov - požiadavky, aby Úrad ukladal povinnosť riešiť kybernetické bezpečnostné incidenty, schvaľoval bezpečnostné opatrenia, bude spôsobovať časové straty a eskaláciu bezpečnostných incidentov (§27, ods. 1);

e) redukcia[11] cieľov kybernetickej bezpečnosti na kontinuitu (poskytovania služieb);

f) nepochopenie úlohy akreditácie, podmienky akreditácie; Návrh nezohľadňuje medzinárodné uznávanie akreditácie, existujúce medzinárodné organizácie CSIRT-ov.

10. **vykonávacie predpisy.** Podmienky a povinnosti, ktoré sú v zákone formulované len veľmi všeobecne, by mali presne špecifikovať vykonávacie predpisy. Zo 6 vyhlášok je uvedená len jedna a ďalšie sú nahradené tézami. Tézy vykonávacích predpisov sú veľmi nesúrodé (vo väčšine prípadov sú všeobecné, ale obsahujú podrobné časti prevzaté z noriem). Podobne ako zákon, majú množstvo formálnych, terminologických, logických ale najmä odborných nedostatkov (Príloha). Vykonávací predpis podľa § 32 ods. 1 písm. d), ktorým sa ustanovujú bezpečnostné štandardy a znalostné štandardy obsahuje 42 odkazov na ISO normy, z toho 26 odkazov je na **neplatné normy**. Podobne Vykonávací predpis podľa § 32 ods. 1 písm. f), uvádza ako východisko tri ISO/IEC normy, z ktorých sú dve **neplatné**.

11. **nepravdivé a problematické tvrdenia** v dôvodovej správe (podrobná analýza v prílohe)

    a. zákon vôbec **nezohľadňuje legislatívny zámer zákona** o informačnej bezpečnosti

    b. **Komisia riaditeľa NBÚ** návrh zákona o kybernetickej bezpečnosti **neprerokovala** (naposledy sa zišla začiatkom septembra 2016)

    c. NBÚ navrhnuté pracovné skupiny Komisie **nezriadilo** (bod 3.2, str. 21)

[11] táto pripomienka bola ošetrená zavedením (nepresných) definícií kontinuity, dôvernosti a integrity v §3 (chýba autentickosť, súkromnosť, prípadne ďalšie bezpečnostné požiadavky), ale tieto sa nezohľadnili v plnom rozsahu v ďalšom texte Návrhu

d. Smernica NIS kybernetickú bezpečnosť **nerieši**, zaoberá sa informačnou bezpečnosťou, t.j. tvrdenie, že návrh zákona rieši požiadavky na kybernetickú bezpečnosť je nepravdivé (alebo je kybernetická bezpečnosť totožná s informačnou bezpečnosťou)

e. kybernetická bezpečnosť sa v slovenskej legislatíve spomína len raz, v kompetenčnom zákone, preto sa nedá hovoriť o nekompatibilite zákonov

f. bod 7, str. 9 (Transpozícia práva EÚ) – *Uveďte, v ktorých ustanoveniach ide národná právna úprava nad rámec minimálnych požiadaviek EÚ spolu s odôvodnením* - predkladatelia návrhu na túto požiadavku odpovedali, že návrh v plnej miere implementuje smernicu NIS, ale to čo presahuje požiadavky NIS neuviedli a nezdôvodnili.

g. bod 3.5. str. 24 – SR má minimum výskumných pracovníkov v oblasti informačnej/kybernetickej bezpečnosti, zákon predpokladá rozvoj výskumu v tejto oblasti a dôvodová správa uvádza, že Návrh zákona nemá vplyv na inovácie.

12. **implementácia zákona.** Predkladateľ mená dostatočnú predstavu, čo bude znamenať implementácia zákona:

    a. viaceré položky v tabuľke vybraných vplyvov nie sú vyplnené alebo zdôvodnené.

    b. Stála pracovná komisia na posudzovanie vybraných vplyvov vyjadrila nesúhlasné stanovisko s materiálom predloženým na predbežné pripomienkové konanie s odporúčaním na jeho dopracovanie podľa pripomienok

    c. Chýba analýza vplyvov na rozpočet verejnej správy

    d. neráta so zvyšovaním počtu zamestnancov, hoci na zaistenie činnosti CSIRT-ov a ochrany systémov povinných osôb na požadovanej úrovni bude potrebné získať kvalifikovaných odborníkov.

    e. neráta s novými pracovnými miestami pre zamestnancov výskumu, hoci sa predpokladá, že sa na výskum budú čerpať prostriedky vyhradené na RIS3, a neráta so žiadnym vplyvom na inovácie, hoci bezpečnosť kritickej informačnej infraštruktúry je základným a nutným predpokladom pre nové informačné služby, IoT a pod.

Čo sa stane ak bude zákon prijatý v tejto podobe?

- SR formálne splní povinnosť implementovať Direktívu NIS
- vynaložíme niekoľko desiatok miliónov eur na budovanie a prevádzku národného a vládneho CSIRT-u, rezortných CSIRT-ov, Jednotného informačného systému kybernetickej bezpečnosti, na akreditácie, koncepcie, stratégie, štandardy, memorandá a pod.

- keďže štát nemá ľudí na plnenie odborných úloh, bude si najímať firmy, aby to robili za neho; (až na to, že firmy tiež nemajú dostatok odborníkov na informačnú/kybernetickú bezpečnosť)
- budeme rozvíjať bezpečnosť po administratívno-byrokratickej stránke (písanie politík, bezpečnostných projektov, posielanie a evidencia hlásení o bezpečnostných incidentoch, vydávanie metodík, štandardov, audity, kontroly, pokuty, cvičenia)
- ale väčšina systémov na Slovensku nebude spadať do pôsobnosti zákona
- keď sa minú peniaze z eurofondov, firmy skončia a štát bude musieť začínať s informačnou bezpečnosťou od začiatku, alebo
- dôjde k veľkému bezpečnostnému incidentu, ktorý ukáže, že koncepcia ochrany slovenského kybernetického priestoru vychádzajúca zo zákona je nedostačujúca
- a potom to bude treba spraviť poriadne (pozri Nemecko, USA).

Čo sa s tým dá spraviť

- na nedostatky zákona sme upozorňovali pred vyše rokom, NBÚ, podpredsedu vlády, premiéra – bez odozvy
- radikálne riešenie – stiahnuť zákon, vymeniť autorský a realizačný kolektív, implementovať Direktívu NIS úpravou iných zákonov a rýchlo pripraviť nový zákon
- konzervatívne riešenie – upraviť zákon ako sa len dá, vymeniť autorský a realizačný kolektív, napísať rozumné vykonávacie predpisy a začať pripravovať najprv novelu a potom nový zákon