Stanovisko Univerzity Komenského k návrhu Zákona o kybernetickej bezpečnosti

Obsah

1 Kontext

- informačná bezpečnosť sa na Slovensku začala rozvíjať v 90-tych rokoch minulého storočia
- čiastkové ustanovenia o IB sa objavili v špecifických zákonoch (Ochrana osobných údajov, Utajované skutočnosti, Elektronický podpis, ISVS, Kritická infraštruktúra, Zákon o bankách a i.)
- zákony boli z hľadiska IB nekonzistentné a nepokrývali všetky problémy, ktoré pre zabezpečenie IB na Slovensku bolo treba riešiť (a ktoré sa v praxi prejavovali)
- potreba zjednocujúceho zákona o IB (schválený legislatívny zámer zákona, MF SR síce zákon v roku 2014 pripravilo, ale nepredložilo do medzirezortného pripomienkového konania)
- Koncepcia kybernetickej bezpečnosti a úloha napísať zákon o kybernetickej bezpečnosti, ktorý by nahradil aj zákon o informačnej bezpečnosti
- potreba implementovať (ale nielen v zákone o KB) Smernicu 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

2 Plánovaný/povinný obsah zákona

- pôvodný legislatívny zámer definoval nasledujúce ciele
  a) vytvoriť jednotný legislatívny rámec pre oblasť informačnej bezpečnosti v Slovenskej republike,

b) definovať kompetencie orgánov štátnej správy v oblasti informačnej bezpečnosti a spôsob koordinácie orgánov štátnej správy pri riešení spoločných úloh v oblasti informačnej bezpečnosti,

c) zaviesť jednotnú terminológiu základných pojmov z oblasti informačnej bezpečnosti,

d) vytvoriť štandardizačný rámec informačnej bezpečnosti,

e) zaviesť proces riadenia informačnej bezpečnosti vo verejnej správe,

f) zaviesť klasifikáciu informačných systémov verejnej správy z hľadiska požiadaviek na informačnú bezpečnosť a definovať minimálne bezpečnostné požiadavky pre jednotlivé kategórie informačných systémov verejnej správy,

g) vymedziť postavenie jednotky pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike a úlohy ďalších takýchto útvarov pri ochrane digitálneho priestoru Slovenskej republiky,

h) definovať minimálne znalostné štandardy v oblasti informačnej bezpečnosti pre pracovníkov spravujúcich informačné systémy verejnej správy a zaisťujúcich ich ochranu,

i) ustanoviť minimálne požiadavky na bezpečnosť elektronickej verejnej správy,

j) ustanoviť minimálne požiadavky na bezpečnosť internetu,

k) zvýšiť celkové povedomie pracovníkov verejnej správy v oblasti informačnej bezpečnosti.

- tieto ciele sú aktuálne aj v súčasnosti, resp. možno ich použiť ako základ, na ktorom sa dá ďalej pracovať
- Smernica 2016/1148 z roku 2016 stanovila nasledujúce požiadavky

l) prijať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov

m) definovať (aspoň jeden) orgán zodpovedný za bezpečnosť sietí a informačných systémov

n) vytvoriť jedno (single) kontaktné miesto

o) vytvoriť aspoň jeden CSIRT, pokrývajúci sektory kritickej infraštruktúry

p) identifikovať poskytovateľov/prevádzkovateľov základných a digitálnych služieb

q) nahlasovať bezpečnostné incidenty

r) členstvo v komisii pre spoluprácu a sieti CSIRTov

- požiadavky Smernice nie sú v rozpore s cieľmi zákona o informačnej bezpečnosti

3 Obsah návrhu zákona o kybernetickej bezpečnosti

- Terminologická poznámka. V návrhu zákona sa používa pojem kybernetická bezpečnosť, po obsahovej stránke je kybernetická bezpečnosť podmnožinou informačnej bezpečnosti, ale vzhľadom na to, že je v záujme Slovenska chrániť celý virtuálny priestor, chápeme informačnú a kybernetickú bezpečnosť ako synonymá.
- návrh zákona o KB vychádza predovšetkým zo Smernice. Jednotlivé ciele z legislatívneho zámeru a povinnosti vyplývajúce zo Smernice sú v návrhu riešené takto

úloha	hodnotenie	Poznámka
a) vytvoriť jednotný legislatívny rámec pre oblasť informačnej bezpečnosti v Slovenskej republike,	nie	návrh sa zaoberá len vybranými problémami IB/KB a dokonca sa obmedzuje len na poskytovateľov/prevádzkovateľov vybraných služieb
b) definovať kompetencie	čiastočne	podrobne len kompetencie NBÚ, ale nie v plnom

orgánov štátnej správy v oblasti informačnej bezpečnosti a spôsob koordinácie orgánov štátnej správy pri riešení spoločných úloh v oblasti informačnej bezpečnosti,		rozsahu, zamerané na úlohy vyplávajúce zo Smernice vzťahy s ostatnými štátnymi orgánmi sú popísané len všeobecne
c) zaviesť jednotnú terminológiu základných pojmov z oblasti informačnej bezpečnosti,	nie	návrh neobsahuje ani len korektné definície použitých pojmov, preberá laické definície odborných pojmov zo Smernice
d) vytvoriť štandardizačný rámec informačnej bezpečnosti,	nie	ani v zúženom rozsahu, spomenuté bez náväznosti v §29
e) zaviesť proces riadenia informačnej bezpečnosti vo verejnej správe,	nie	zákon sa tým vôbec nezaoberá
f) zaviesť klasifikáciu informačných systémov verejnej správy z hľadiska požiadaviek na informačnú bezpečnosť a definovať minimálne bezpečnostné požiadavky pre jednotlivé kategórie informačných systémov verejnej správy,	nie	zákon sa tým vôbec nezaoberá, spomenuté bez náväznosti v §29
g) vymedziť postavenie jednotky pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike a úlohy ďalších takýchto útvarov pri ochrane digitálneho priestoru Slovenskej republiky,	čiastočne	ale v rozpore s úlohami CSIRT definovanými napr. agentúrou ENISA
h) definovať minimálne znalostné štandardy v oblasti informačnej bezpečnosti pre pracovníkov spravujúcich informačné systémy verejnej správy a zaisťujúcich ich ochranu,	nie	návrh zákona sa tým vôbec nezaoberá
i) ustanoviť minimálne požiadavky na bezpečnosť elektronickej verejnej správy,	nie	návrh zákona sa tým vôbec nezaoberá
j) ustanoviť minimálne požiadavky na bezpečnosť internetu,	nie	návrh zákona sa tým vôbec nezaoberá
k) zvýšiť celkové povedomie pracovníkov verejnej správy v oblasti informačnej bezpečnosti.	nie	návrh zákona sa tým vôbec nezaoberá

- pre úplnosť prejdeme ešte úlohy vyplývajúce zo Smernice:

l) prijať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov	čiastočne	existuje veľmi všeobecná Koncepcia kybernetickej bezpečnosti a rok platný Akčný plán, ale realizácia ??? návrh zákona spomína prípravu Národnej stratégie
m) definovať (aspoň jeden) orgán zodpovedný za bezpečnosť sietí a informačných systémov	áno	Kompetenčný zákon, čiastočne návrh zákona, ale samotný Úrad to neutiahne, treba sa dohodnúť s ostatnými štátnymi orgánmi na rozdelení úloh a spôsobe spolupráce
n) vytvoriť jedno (single) kontaktné miesto	áno	organizačné opatrenie NBÚ, ale bude potrebovať informácie
o) vytvoriť aspoň jeden CSIRT, pokrývajúci sektory kritickej infraštruktúry	čiastočne	existujú dva fungujúce a použiteľné, predstava o rýchlom vytvorení vládneho v NASES je nereálna
p) identifikovať poskytovateľov/prevádzkovateľov základných a digitálnych služieb	áno	návrh zákona rieši
q) nahlasovať bezpečnostné incidenty	áno	návrh zákona rieši, záleží od realizácie
r) členstvo v komisii pre spoluprácu a sieti CSIRTov	áno	návrh zákona ráta s podporou členstva a činnosti

- z uvedeného vyplýva, že návrh zákona o KB je implementáciou Smernice, ale nerieši problémy kybernetickej/informačnej bezpečnosti Slovenska
- tri otázky:
- treba tieto problémy riešiť?
- ak áno, kto za ich riešenie bude zodpovedný (Úrad pre kybernetickú a informačnú bezpečnosť?) a v akom zákone sa vytvorí na ich riešenie potrebný legislatívny rámec?
- a napokon ako budú rozdelené kompetencie medzi NBÚ a Úradom pre kybernetickú a informačnú bezpečnosť?

4 Pripomienky

Pripomienok je veľa, rôzneho charakteru a závažnosti. V tejto časti uvádzame len zhrnutie podložené ukážkami.

4.1 terminologické

- terminológia uvedená v zákone nie je úplná, jednoznačná, správna pojmy sa nepoužívajú konzistentne, definície v ktorých sa používajú iné pojmy sú niekedy protirečivé alebo cyklické (pozri časť 4.2.), namiesto presných definícií sa naširoko vymenúvajú podobné pojmy a spájajú rôzne aspekty do jedného pojmu, čo vedie k neprehľadným a protirečivým definíciám
- v návrhu nie sú definované základné pojmy (hrozba, aktívum, riziko, analýza rizík, akceptovateľné riziko, bezpečnostné opatrenie, bezpečnostný projekt, dôvernosť, dostupnosť, integrita, autentickosť, služba, bezpečnostný incident,...)
- pojmom sa pripisuje iný význam ako je ich prirodzený
    - reaktívne opatrenie, §23

- definícia CSIRT nezodpovedá medzinárodnej definícii: jednotkou CSIRT útvar orgánu verejnej moci zapísaný do zoznamu jednotiek CSIRT, - takáto jednotka nebude ako CSIRT uznaná medzinárodne

- zmiešavajú sa dva významy pojmu kybernetická bezpečnosť – stav nejakého systému a činnosť na dosiahnutie tohto stavu.
- (§ 17) (1) Bezpečnostné opatrenia predstavujú súhrn úloh, procesov, rolí a technológií, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas celej doby životnosti informačného a komunikačného systému prevádzkovateľa základnej služby. Ale §3
- kybernetickou bezpečnosťou stav, kedy je kybernetický priestor dostatočne zabezpečený a odolný proti kybernetickým bezpečnostným incidentom a systém opatrení na zaistenie odolnosti kybernetického priestoru proti kybernetickým bezpečnostným incidentom, ako aj činností a prostriedkov zameraných na dosiahnutie požadovanej úrovne bezpečnosti kybernetického priestoru,
- to znamená, že
  - Bezpečnostné opatrenia predstavujú súhrn úloh, procesov, rolí a technológií, ktorých cieľom je zabezpečenie stavu, kedy je kybernetický priestor dostatočne zabezpečený a odolný proti kybernetickým bezpečnostným incidentom,
  - Bezpečnostné opatrenia predstavujú súhrn úloh, procesov, rolí a technológií, ktorých cieľom je zabezpečenie systému opatrení na zaistenie odolnosti kybernetického priestoru proti kybernetickým bezpečnostným incidentom, ako aj činností a prostriedkov zameraných na dosiahnutie požadovanej úrovne bezpečnosti kybernetického priestoru,

- podobne (§24) Stav kybernetického ohrozenia nastáva v prípade závažného zníženia úrovne kybernetickej bezpečnosti alebo bezprostrednej hrozby ohrozenia kybernetickej bezpečnosti, ak by v jeho dôsledku mohlo dôjsť k narušeniu bezpečnosti
- mechanicky sa kopírujú definície pojmov zo slovenského prekladu smernice NIS, ktoré sú po odbornej stránke zlé
- zavádza sa viacero pojmov, medzi ktorými nie je definovaný vzťah: štátna politika, Koncepcia KB, Národná stratégia, politika správania sa v kybernetickom priestore, niektoré sa pritom definujú, iné nie

4.2 logické

- cyklické definície (§3): kybernetickou bezpečnosťou stav, kedy je kybernetický priestor dostatočne zabezpečený a odolný proti kybernetickým bezpečnostným incidentom a kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má alebo môže mať negatívny vplyv na kybernetickú bezpečnosť; t.j. kybernetickou bezpečnosťou stav, kedy je kybernetický priestor dostatočne zabezpečený a odolný proti udalostiam ktoré majú alebo môže mať negatívny vplyv na kybernetickú bezpečnosť
- jednotný informačný systém kybernetickej bezpečnosti (§8) je raz verejný, druhý krát je k nemu prístup regulovaný; obsahuje údaje, bez ktorých sa kybernetická bezpečnosť nedá zabezpečiť, ale tie nemajú byť dostupné pre každého:
- V jednotnom informačnom systéme kybernetickej bezpečnosti úrad vedie a zverejňuje
- informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu prostredníctvom centrálneho systému včasného varovania.

- Informácie v jednotnom informačnom systéme kybernetickej bezpečnosti nie sú verejne prístupné
- Reaktívne služby sa zameriavajú na riešenie kybernetických bezpečnostných incidentov ako a) výstrahy a varovania. To znamená, že kybernetickým bezpečnostným incidentom sú výstrahy a varovania?
- riešenie bezpečnostného incidentu podľa návrhu zákona nevyžaduje, aby sa niečo robilo v priebehu samotného incidentu; znamená to, že napríklad v prípade útoku má CSIRT zaregistrovať útok, počkať, kým skončí, analyzovať ho a podať o ňom správu?! „riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s odhaľovaním, analýzou a riešením následkov kybernetického bezpečnostného incidentu“(§ 3),
- (§16) Prevádzkovateľ základnej služby je povinný prijať a dodržiavať bezpečnostné opatrenia – bezpečnostné opatrenie na zaistenie fyzickej ochrany prístupu je plot. Ako sa prijíma a dodržiava plot?

4.3 odborné

- zamieňa sa pojem hrozba a riziko
- nesprávnym chápaním a používaním pojmov sa kladú nerealistické požiadavky na komunikáciu
- CSIRT má riešiť bezpečnostné incidenty a nie plniť úlohy manažéra informačnej bezpečnosti a správcu systému
- bezpečnostných incidentov je tak veľa, že nie je možné vypracovať postup pre každý scenár, ktorý potenciálne môže nastať, keby sa táto povinnosť mala dodržiavať, CSIRTy by zahltili Úrad operačnými postupmi;
- a čo ak by došlo k incidentu, ktorý by bolo treba riešiť a CSIRT by ešte nemal schválený operačný postup, lebo to NBÚ nestihol zúradovať?
- bezpečnostné hrozby sa vyvíjajú rýchlejšie ako v dvojročných intervaloch a tak môžu byť mnohé operačné postupy po dvoch rokoch už neaktuálne
- zoznam tzv. bezpečnostných opatrení v § 17 je dôkazom nepochopenia základných pojmov informačnej bezpečnosti. Ide o zoznam oblastí, podoblastí a konkrétnych opatrení uvedených v norme ISO/IEC 27002. Navyše sú niektoré pojmy zle preložené
- Bezpečnostné opatrenia pre bezpečnosť systémov a zariadení
- uplatňovanie systému bezpečnosti,
- riadenie dostupnosti sietí
- nástroje na detekciu, zber a vyhodnocovanie kybernetických bezpečnostných incidentov.

bezpečnostné opatrenia nie je vhodné popisovať v zákone (ISO 27002 má vyše 100 strán), pretože tu nie je priestor na ich vysvetlenie a nutne dochádza k zjednodušeniam a nesprávnej interpretácii. Opatrenia je potrebné uviesť na úrovni oblastí (ak vôbec) a ponechať ich upresnenie na vyhlášku. Ale ak majú byť opatrenia primerané, buď je potrebné zaviesť klasifikáciu systémov a informácií alebo požadovať bezpečnostný projekt vychádzajúci z analýzy rizík

- §18, súlad informačného a komunikačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti – a to sú ktoré?
- §22 je zbytočný, časť z neho sa dá zaradiť do povinností poskytovateľa/prevádzkovateľa a časť do § 23

4.4 koncepčné

- pôsobnosť zákona §2 nie je explicitne definovaná; je vymedzená len vo vzťahu k iným zákonom
- sústredenie sa na vybrané systémy (uvedené v Smernici) a ignorovanie ostatných systémov nevyrieši problémy IB/KB Slovenska
- zákon by mal byť lex generalis pre informačnú a kybernetickú bezpečnosť, vzhľadom na charakter IKT nie je kybernetický priestor možné rozdeliť na kompartmenty. Ak má byť chránený celý, musia byť definované aspoň základné bezpečnostné požiadavky jednotne.
- NBÚ nemá odborné kapacity na vykonávanie úloh, ktoré mu zákon ukladá
    - výskum a vývoj v oblasti kybernetickej bezpečnosti,
    - vzdelávanie
    - kontrolná činnosť
    - príprava štandardov a metodických materiálov
    - zabezpečenie odbornej prípravy jednotiek CSIR
- formulácie postavenia NBÚ voči zahraničiu sú všeobecné, treba ich upresniť, aby NBÚ nevstupovalo do kompetencie iných štátnych orgánov
- zákon vo všeobecnosti stavia NBÚ do nedobrej pozície voči ostatným štátnym orgánom ale aj komerčným subjektom – veľké kompetencie, málo konkrétnych úloh, možnosť kontroly a udeľovania sankcií na základe zle definovaných kritérií; čo sa určite prejaví pri pripomienkovaní návrhu a ak by prešiel, tak pri jeho praktickom používaní
- jednotný systém kybernetickej bezpečnosti bude len nástroj, ktorý bude treba naplniť a pracovať s ním. Nedá sa očakávať, že vyrieši to, čo nevieme riešiť aj bez neho. Ak by mal plniť takú kľúčovú úlohu, ako mu stanovuje zákon môže byť slabým článkom kybernetickej bezpečnosti Slovenska (kým sa vysúťaží, vyvinie, odladí, nasadí a začne používať, môže uplynúť niekoľko rokov a bude to štát o dva rády viac, ako keby si taký systém NBÚ postupne vybudovalo samo). Tento systém bude ISVS, zároveň referenčným registrom a bude musieť spĺňať požiadavky zákona o e-Gov.
- Direktíva NIS nevyžaduje, aby mala každá vecne príslušná autorita jednotku CSIRT, Slovensko potrebuje aspoň jeden CSIRT a ľudí, ktorí budú zabezpečovať kritické systémy (to sú v prvom rade technickí správcovia, bezpečnostní manažéri, ale aj operátori špeciálnych zariadení, audítori). Návrh zákona nerozlišuje úroveň „CSIRTov“.
- Akreditácia nejakého útvaru Úradom a jeho prehlásenie za CSIRT nemá z medzinárodného hľadiska žiaden význam,
- vládny CSIRT aj CSIRT-NBÚ by mali byť akreditované a podliehať štandardnej kontrole a nezávislým auditom. Podmienky na akreditáciu by mali byť kompatibilne s požiadavkami FIRST, aby aspoň vrcholné slovenské CSIRTy boli medzinárodne uznávané
- koncepcia kybernetickej bezpečnosti s takto rozdelenými kompetenciami a povinnosťami by možno mohla fungovať v mieri, keď útočníkmi budú jednotlivci. V prípade koordinovaného profesionálne vedeného útoku na vybrané prvky kritickej informačnej infraštruktúry sa však celý systém zrúti

4.5 legislatívno-právne

- návrh nerešpektuje pôvodný Vládou schválený legislatívny zámer zákona o informačnej bezpečnosti
- jeden a ten istý problém sa rozpisuje na viacerých miestach bez toho, aby sa odvolával (postavenie jednotného informačného systému kybernetickej bezpečnosti, povinnosti poskytovateľa/prevádzkovateľa služieb, audit)
- zákon obsahuje články opisného charakteru (§ 7, ods. 1 a 2, §8, §14, §23. ods. 1)
- § 10 nezapadá do zákona, pri riešení bezpečnostných incidentov sa človek môže dostať k informáciám, ktoré si vyžadujú nielen ochranu z hľadiska dôvernosti. Resp. ochranu informácií pri riešení bezpečnostných incidentov by bolo treba najprv analyzovať, čo všetko sa môže stať (napr. človek bez previerky sa dostane ku klasifikovaným informáciám) a až potom stanovovať povinnosti v zákone
- vykonávacími predpismi (§29) nie je možné stanovovať povinnosti, ktoré nie sú uvedené v Zákone
- niektoré kompetencie sa mi vidia problematické:
    - môže Úrad určovať koncepciu štátnej politiky? Nemusí ju schváliť Vláda?
    - vyhlásenie stavu ohrozenia má vážne dôsledky, nemala by ho vyhlasovať Vláda?
    - kybernetický priestor je jedným z frontov, na ktorom môže prebiehať vojnový konflikt (zem, voda, vzduch, kozmický priestor, kybernetický priestor), nemala by v takomto prípade prevziať okamžite zodpovednosť za obranu armáda?
    - nemá byť kontaktným bodom pre NATO MNO SR alebo MZV SR?
- treba spraviť porovnanie návrhu zákona a zákonov o ochrane osobných údajov, utajovaných skutočnostiach, kritickej infraštruktúre, telekomunikačnom zákone, zákone o e-Gov, ISVS a i. aby sa dosiahla kompatibilita požiadaviek
- v prílohe sú sektory definované inak ako v zákone o kritickej infraštruktúre
- takisto treba porovnať návrh zákona s požiadavkami Smernice NIS
- môže jeden štátny orgán platiť inému štátnemu orgánu za služby?

5 Záver

Zákon po obsahovej stránke sa nezaoberá problémami, ktoré je potrebné pre zaistenie potrebnej úrovne bezpečnosti slovenského virtuálneho priestoru riešiť. Na veľmi všeobecnej úrovni implementuje Smernicu, ale konkrétne problémy, ktoré sú spojené s praktickým plnením úloh Smernice ponecháva otvorené (kooperácia štátnych orgánov, povinnosti poskytovateľov/prevádzkovateľov základných a digitálnych služieb). Pre NBÚ stanovuje úlohy, na ktoré NBÚ nemá odborné kapacity (vzdelávanie, výskum a vývoj v kybernetickej bezpečnosti, kontrola bezpečnosti systémov a sietí,...), podceňuje zložitosť realizácie úloh (vytvorenie vládneho CSIRTu v NASES). Povinnosti poskytovateľov a prevádzkovateľov nie sú dostatočne definované, Zákon dáva NBÚ možnosť vykonávacími predpismi ukladať povinnosti, ktoré nie sú stanovené v Zákone a Úrad môže za nedodržiavanie povinností udeľovať vysoké pokuty. V zákone sú vážne odborné chyby (bezpečnostné opatrenia, požiadavky na ochranu (systémov), neznalosť poslania CSIRT, podmienok medzinárodnej akreditácie CSIRT, neznalosť noriem), ktoré ho robia nevykonateľným. Mám pochybnosti aj o právnej korektnosti navrhovaných riešení (čo ako laik neviem posúdiť) môže sa kontrola súkromných firiem riadiť zákonom o kontrole v štátnej správe, môže Úrad požadovať od firmy prijatie opatrení, ktoré ohrozia jej existenciu?

Nedostatky posudzovaného návrhu zákona sú natoľko vážne, že sa nedajú vyriešiť lokálnymi úpravami. Odporúčam návrh zákona stiahnuť a vypracovať nový návrh.

Bratislava 12/02/2017