Návrh

Legislatívny zámer zákona o informačnej bezpečnosti

Úvod

Informačná bezpečnosť je podľa medzinárodnej normy ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je

- zaistenie kontinuity obchodných procesov,
- minimalizácia strát a
- maximalizácia návratnosti investícií.

V súčasnosti sa informácie v čoraz väčšej miere spracovávajú v elektronickej forme pomocou počítačov a iných informačných a komunikačných technológií. Potenciálna možnosť narušenia týchto informácií, či už priamo alebo prostredníctvom útoku na technické zariadenie alebo prostredie, v ktorom sa informácia spracováva, sa nazýva hrozba. Existuje množstvo činiteľov, ktoré môžu ohroziť alebo spôsobiť znefunkčnenie informačných a komunikačných technológií a znehodnotenie informácií, ktoré sú v nich spracovávané. Sú to napríklad prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus, ktoré by mohli spôsobiť vážne bezpečnostné problémy.

Cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru Slovenskej republiky[1)].

Informačná bezpečnosť musí zohľadňovať záujmy vlastníkov a potreby používateľov informačných a komunikačných technológií, ako aj práva fyzických osôb a právnických osôb, ktorých údaje sa v systémoch spracovávajú. Z hľadiska používateľov sú pri spracovaní informácie najdôležitejšie faktory, a to účel a obsah informácií, presnosť, aktuálnosť, prístupnosť, autenticita, usporiadanie a kvalita informácií. Z hľadiska vlastníkov a prevádzkovateľov je najdôležitejšia dostupnosť informačných zdrojov, podľa možnosti s prístupom on-line, a ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému.

Nezabezpečenie informácií môže mať za následok nenahraditeľné straty a narušenie dôveryhodnosti organizácie a štátu. Vzhľadom na to, že štát je garantom kritických procesov, má úlohu starať sa o celkovú úroveň konkurencieschopnosti spoločnosti, a tým chrániť národné bohatstvo, ktorého súčasťou sú aj znalosti a informácie, a preto si nemôže dovoliť mať nízke kritériá úrovne bezpečnosti. Vzhľadom na možný nepriaznivý dosah je povinnosťou štátu zabezpečiť ochranu informácií pred zneužitím a minimalizovať následky v prípade ich zneužitia.

[1)] Kritickou informačnou infraštruktúrou sú prostriedky a siete informačných a komunikačných technológií, súvisiace hodnoty a elektronické služby, ktorých zničenie alebo znefunkčnenie v dôsledku pôsobenia rizikového faktora spôsobí ohrozenie alebo narušenie politického a hospodárskeho chodu štátu alebo ohrozenie života a zdravia obyvateľstva.

Potrebu informačnej bezpečnosti si uvedomili aj národné vlády, nadnárodné orgány a organizácie vyspelých krajín sveta ako Organizácia pre ekonomickú spoluprácu a rozvoj, Organizácia Spojených národov, Organizácia Severoatlantickej zmluvy, Skupina krajín G8 a medzinárodné a európske normalizačné organizácie, ktoré vytvorili rôzne inštitúcie a inštitucionálne systémy pre zabezpečovanie ochrany informácií, napríklad Európsku agentúru pre bezpečnosť informačných sietí, Skupinu vysokých zástupcov pre otázky správy internetu, Jednotku pre riešenie počítačových incidentov, určili si strategické ciele a prijímajú opatrenia na ich splnenie, z ktorých mnohé už realizujú.

Základný rámec informačnej bezpečnosti verejnej správy je načrtnutý v dokumente „Národná stratégia pre informačnú bezpečnosť v Slovenskej republike“, ktorý bol schválený uznesením vlády Slovenskej republiky (ďalej len „uznesenie vlády“) č. 570 zo dňa 27. augusta 2008. Návrh legislatívneho zámeru zákona o informačnej bezpečnosti je koncipovaný v súlade so stavom a vývojom informačných a komunikačných technológií, reflektuje zmeny v organizácii štátnej správy a územnej samosprávy a zohľadňuje smernice a odporúčania Európskej únie, ako aj ďalšie materiály schválené uzneseniami vlády, napríklad uznesenia vlády č. 283/2009, č. 391/2009 a č. 479/2009.

Informačná bezpečnosť v oblasti utajovaných skutočností je upravená osobitným zákonom a nie je predmetom tohto materiálu.

Prvá kapitola
Zhodnotenie platnej právnej úpravy a dôvody vypracovania zákona o informačnej bezpečnosti

I. Vývoj právnej úpravy

Informačná bezpečnosť je pojem, ktorý zatiaľ nie je v Slovenskej republike v primeranej miere premietnutý do legislatívy. Napriek tomu má informačná bezpečnosť oporu v legislatíve, ako aj v strategických a koncepčných dokumentoch schválených vládou Slovenskej republiky.

Informatizácia spoločnosti a s ňou súvisiaca informačná bezpečnosť verejnej správy je vymedzená zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Ochrana utajovaných skutočností[2)] predstavuje klasifikovanú informáciu a systémy pracujúce s klasifikovanou informáciou. Utajované skutočnosti sú klasifikované z hľadiska dôvernosti, pričom bezpečnostné požiadavky na ich ochranu sú komplexné a zohľadňujú najmä potrebu zaistenia integrity a dostupnosti údajov.

Ochrana osobných údajov a používanie elektronického podpisu sú upravené osobitnými predpismi[3)] a príslušné inštitúcie zabezpečujú dohľad nad ich dodržiavaním.

[2)] *Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a s ním súvisiace predpisy.*

[3)] *Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,*
Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
Zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

Elektronický obchod upravuje zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Počítačovú kriminalitu upravuje § 247 zákona č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov, do ktorého sú premietnuté princípy Dohovoru o kybernetickom zločine CETS č. 185/2001, vydanom Radou Európy.

Autorské právo je upravené autorským zákonom[4)].

II. Súčasná právna úprava

A. Legislatívny rámec informačnej bezpečnosti tvoria v súčasnosti najmä

- zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov,
- zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov,
- zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,
- zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom v znení neskorších predpisov,
- zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov,
- ústavný zákon č. 254/2006 Z. z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu,
- zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- nariadenie vlády Slovenskej republiky č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností,

---

[4)] Zákon č. 618/2003 Z. z. o autorskom práve a o právach súvisiacich s autorským právom v znení neskorších predpisov.

- metodické usmernenie Úseku bankového dohľadu Národnej banky Slovenska č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky,
- výnos Ministerstva financií Slovenskej republiky z 8. septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy, ktorý obsahuje aj bezpečnostné štandardy.

Vyhlášky Národného bezpečnostného úradu upravujúce ochranu utajovaných skutočností sú

- vyhláška Národného bezpečnostného úradu č. 325/2004 Z. z. o priemyselnej bezpečnosti,
- vyhláška Národného bezpečnostného úradu č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca,
- vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky Národného bezpečnostného úradu č. 315/2006 Z. z.,
- vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní v znení vyhlášky Národného bezpečnostného úradu č. 314/2006 Z. z.,
- vyhláška Národného bezpečnostného úradu č. 339/2004 Z. z. o bezpečnosti technických prostriedkov,
- vyhláška Národného bezpečnostného úradu č. 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií,
- vyhláška Národného bezpečnostného úradu č. 314/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní,
- vyhláška Národného bezpečnostného úradu č. 315/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti,
- vyhláška Národného bezpečnostného úradu č. 453/2007 Z. z. o administratívnej bezpečnosti.

B. Ďalšie právne akty, záväzné pre Slovenskú republiku z dôvodu členstva v Európskej únii, Organizácii pre ekonomickú spoluprácu a rozvoj, Organizácii Spojených národov a Organizácii Severoatlantickej zmluvy sú

- Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 15), transponovaná do zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,
- Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (Mimoriadne vydanie Ú. v. EÚ,

kap.13/zv. 24), transponovaná do zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,

- Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 25), transponovaná do zákona č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Dohovor Rady Európy o počítačovej kriminalite z 23. novembra 2001, transponovaný do zákona č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov; podpísali ho členské štáty Rady Európy a ďalšie účastnícke štáty a Slovenská republika ho podpísala a ratifikovala vo februári 2005,
- Nariadenie Komisie (ES) č. 831/2002 zo 17. mája 2002, ktorým sa vykonáva nariadenie Rady (ES) č. 322/97 o štatistike spoločenstva so zreteľom na prístup k dôverným údajom na výskumné účely (Mimoriadne vydanie Ú. v. EÚ, kap.1/zv. 4),
- Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (Smernica o súkromí a elektronických komunikáciách) (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 29), transponovaná do zákona č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- Dodatkový protokol k Dohovoru o počítačovej kriminalite o kriminalizácii činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov z 28. januára 2003; Slovenská republika ho zatiaľ neratifikovala,
- Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23. 12. 2008),
- Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa (Ú. v. EÚ L 337, 18. 12. 2009); smernica bude v roku 2011 transponovaná do novely zákona č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- Nariadenie Európskeho parlamentu a Rady (ES) č. 223/2009 z 11. marca 2009 o európskej štatistike a o zrušení nariadenia (ES, Euratom) č. 1101/2008 o prenose dôverných štatistických údajov Štatistickému úradu Európskych spoločenstiev, nariadenia Rady (ES) č. 322/97 o štatistike Spoločenstva a rozhodnutia Rady 89/382/EHS, Euratom o založení Výboru pre štatistické programy Európskych spoločenstiev (Ú. v. EÚ L 87, 31. 3. 2009).

Aj v ďalších zákonoch sú ustanovenia, ktoré majú informačno-bezpečnostný vplyv. Z informačno-bezpečnostného hľadiska sú príslušné nielen všetky zákonné normy, ktoré

upravujú podmienky používania informačných a komunikačných technológií, ale aj tie, ktoré umožňujú spracovanie informácií v elektronickej podobe.

III. Hlavné dôvody na vypracovanie zákona o informačnej bezpečnosti

Prakticky všetky dôležité oblasti života spoločnosti v súčasnosti podstatne závisia od spoľahlivého fungovania systémov jej digitálneho priestoru[5)], a preto zaistenie primeranej ochrany digitálneho priestoru je prioritným záujmom Slovenskej republiky. Keďže narušenie alebo zlyhanie jednej časti digitálneho priestoru môže ohroziť inú jeho podstatnú časť, alebo aj celý digitálny priestor, zaistenie informačnej bezpečnosti digitálneho priestoru musí byť trvalé a komplexné, a to si vyžaduje systematický, koordinovaný a legislatívne podporený prístup všetkých zainteresovaných subjektov. Štát môže bezprostredne zaisťovať ochranu informačných systémov verejnej správy, z ktorých sú mnohé pre riadenia a chod štátu kľúčové. Množstvo dôležitých informačných a komunikačných technológií digitálneho priestoru Slovenskej republiky je však v súkromnom vlastníctve a štát nemá iné ako právne nástroje na presadenie potrebných bezpečnostných opatrení na ochranu týchto systémov.

Súčasný právny poriadok Slovenskej republiky síce obsahuje viacero právnych noriem, ktoré riešia čiastkové problémy, a tak pokrývajú špecifické oblasti informačnej bezpečnosti, ale jednotný, všeobecný právny predpis pre informačnú bezpečnosť digitálneho priestoru v slovenskej legislatíve chýba. Absencia takého zákona sa prejavuje napríklad v nekonzistentnosti terminológie, nedostatočnom používaní bezpečnostných štandardov, v prekrývajúcich sa kompetenciách štátnych orgánov a v neúplnosti pokrytia informačnej bezpečnosti právnymi predpismi a kompetenciami.

Ďalším dôsledkom neúplného a nekonzistentného právneho rámca informačnej bezpečnosti je to, že sa ochrana informačných a komunikačných systémov v Slovenskej republike riadi rôznymi právnymi predpismi alebo je celkom ponechaná na uváženie ich vlastníkov a správcov. Výsledkom toho je rôznorodá, nekompatibilná a často nedostatočná úroveň ochrany informačných a komunikačných technológií, čo okrem vlastného ohrozenia a ohrozenia digitálneho priestoru znižuje možnosť ich bezpečnej kooperácie a efektívnejšieho využívania existujúcich informačných zdrojov a výpočtových kapacít. Na druhej strane absencia alebo nejednoznačnosť právnych predpisov môže viesť k uplatňovaniu ekonomicky náročných ale pritom neadekvátnych bezpečnostných riešení. Preto je potrebné vytvoriť klasifikačnú schému informačných a komunikačných technológií a ustanoviť minimálne požiadavky na ochranu ich jednotlivých kategórií.

Digitálny priestor Slovenskej republiky je súčasťou globálneho, celosvetového digitálneho priestoru. Vďaka vzájomnej previazanosti informačných a komunikačných technológií je nevyhnutná aj medzinárodná koordinácia ochrany globálneho digitálneho priestoru. Na riešenie bezpečnostných problémov digitálneho priestoru bola zriadená uznesením vlády č. 479/2009 jednotka pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike. Aby si táto jednotka pre riešenie počítačových incidentov mohla plniť stanovené úlohy v domácom aj medzinárodnom meradle, je potrebné legislatívne vymedziť jej kompetencie a vzťahy k ostatným štátnym orgánom Slovenskej republiky.

S postupujúcou informatizáciou spoločnosti narastá počet informačných a komunikačných technológií a používateľov služieb informačnej spoločnosti. Potrebnú úroveň ochrany digitálneho priestoru nie je možné dosiahnuť bez dostatočného bezpečnostného povedomia používateľov a udržiavania primeraných znalostí tých, ktorí informačné a

[5)] *Digitálny priestor tvoria informačné a komunikačné systémy a informácie, ktoré sa v nich spracovávajú.*

komunikačné technológie spravujú a rovnako aj tých, ktorí zodpovedajú za ich ochranu. Je potrebné stanoviť minimálne kvalifikačné požiadavky z informačnej bezpečnosti na informatikov a bezpečnostných špecialistov.

Rozvoj a nasadzovanie informačných a komunikačných technológií otvára neustále nové bezpečnostné otázky, ktoré je potrebné analyzovať a prijímať primerané riešenia ešte pred tým, ako nedostatky týchto technológií spôsobia bezpečnostné problémy pri ich používaní. Zákon by mal ustanoviť, kto bude zbierať a spracovávať informácie o nedostatkoch informačných a komunikačných technológií, komu, v akom rozsahu a akým spôsobom sa tieto informácie budú poskytovať.

Úlohy spojené s ochranou digitálneho priestoru Slovenskej republiky plnia rôzne štátne aj neštátne inštitúcie a s prehlbujúcou sa informatizáciou spoločnosti budú pribúdať ďalšie úlohy. Súčinnosť inštitúcií podieľajúcich sa na ochrane digitálneho priestoru bude potrebné koordinovať. Zo zodpovednosti za informatizáciu spoločnosti vyplýva pre Ministerstvo financií Slovenskej republiky (ďalej len „ministerstvo financií“) aj úloha koordinátora informačnej bezpečnosti. Zákon ustanoví formu tejto koordinácie.

Druhá kapitola
Ciele a obsah navrhovaného zákona

I. Ciele

Zákon o informačnej bezpečnosti bude riešiť dva okruhy problémov, a to zaistenie ochrany pre informačné systémy verejnej správy a vytvorenie všeobecného právneho rámca pre ochranu celého digitálneho priestoru Slovenskej republiky.

Vychádzajúc zo skutočností uvedených v predchádzajúcej časti, zákon sleduje najmä nasledujúce ciele

- vytvoriť jednotný legislatívny rámec pre oblasť informačnej bezpečnosti v Slovenskej republike,
- definovať kompetencie orgánov štátnej správy v oblasti informačnej bezpečnosti a spôsob koordinácie orgánov štátnej správy pri riešení spoločných úloh v oblasti informačnej bezpečnosti,
- zaviesť jednotnú terminológiu základných pojmov z oblasti informačnej bezpečnosti,
- vytvoriť štandardizačný rámec informačnej bezpečnosti,
- zaviesť proces riadenia informačnej bezpečnosti vo verejnej správe,
- zaviesť klasifikáciu informačných systémov verejnej správy z hľadiska požiadaviek na informačnú bezpečnosť a definovať minimálne bezpečnostné požiadavky pre jednotlivé kategórie informačných systémov verejnej správy,
- vymedziť postavenie jednotky pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike a úlohy ďalších takýchto útvarov pri ochrane digitálneho priestoru Slovenskej republiky,
- definovať minimálne znalostné štandardy v oblasti informačnej bezpečnosti pre pracovníkov spravujúcich informačné systémy verejnej správy a zaisťujúcich ich ochranu,

- ustanoviť minimálne požiadavky na bezpečnosť elektronickej verejnej správy,
- ustanoviť minimálne požiadavky na bezpečnosť internetu,
- zvýšiť celkové povedomie pracovníkov verejnej správy v oblasti informačnej bezpečnosti.

Zdôvodnenie. Štát je povinný zaisťovať primeranú ochranu informačných a komunikačných technológií, ktoré sú v pôsobnosti štátnych orgánov a orgánov samosprávy. Cieľom zákona o informačnej bezpečnosti je vytvoriť ucelený, koordinovaný a efektívny systém ochrany informačných systémov verejnej správy Slovenskej republiky. Keďže informačné systémy verejnej správy sú súčasťou širšieho digitálneho priestoru, ktorého značná časť je v súkromných rukách, zákon vytvára podmienky na zvyšovanie úrovne informačnej bezpečnosti v celom digitálnom priestore Slovenskej republiky prostredníctvom štandardizácie informačnej bezpečnosti.

II. Obsah

Rozsah zákona

Zákon o informačnej bezpečnosti sa bude vzťahovať na informačné systémy verejnej správy a ustanovovať povinné bezpečnostné požiadavky na ostatné informačné a komunikačné technológie digitálneho priestoru Slovenskej republiky, ktoré komunikujú s informačnými systémami verejnej správy v rozsahu potrebnom na zaistenie bezpečného fungovania informačných systémov verejnej správy. Zákon o informačnej bezpečnosti nebude meniť kompetencie subjektov zodpovedných za špecifické oblasti informačnej bezpečnosti definované existujúcimi zákonmi, ktoré plnia osobitné úlohy podľa osobitných predpisov.

Zdôvodnenie. Zákon o informačnej bezpečnosti bude všeobecným právnym predpisom pre informačnú bezpečnosť v Slovenskej republike. Z tejto pozície bude definovať základné ciele a procesy riadenia informačnej bezpečnosti vo verejnej správe a zjednocovať riadenie informačnej bezpečnosti u povinných osôb a týmto vytvorí ucelený systém riadenia informačnej bezpečnosti. Osobitné zákony čiastkovo upravujúce požiadavky informačnej bezpečnosti budú ustanovovať parametre a určovať špecifické opatrenia informačnej bezpečnosti pre spracovávané údaje v oblasti svojej pôsobnosti v nadväznosti na zákon o informačnej bezpečnosti.

Nový zákon o informačnej bezpečnosti navrhujeme členiť na tieto časti:

1. časť – Základné ustanovenia

Táto časť zákona upraví predmet a účel zákona, t. j. okruh spoločenských vzťahov v rámci informačnej bezpečnosti. Zároveň bude obsahovať definície základných pojmov informačnej bezpečnosti a určenie povinných osôb.

Zákon bude definovať základné pojmy informačnej bezpečnosti, a tým položí základy jednotnej slovenskej terminológie v tejto oblasti. Zákon o informačnej bezpečnosti ustanoví povinnosť ministerstvu financií priebežne aktualizovať terminológiu informačnej bezpečnosti a sprístupňovať ju používateľom.

Zdôvodnenie. Ministerstvo financií je v súčasnosti poverené uznesením vlády č. 570/2008 zosúladiť v spolupráci s Ministerstvom kultúry Slovenskej republiky legislatívnu terminológiu pre oblasť informatizácie spoločnosti, do ktorej spadá aj terminológia informačnej bezpečnosti. V záujme zosúladenia a doplnenia v súčasnosti nejednoznačnej a neúplnej terminológie informačnej bezpečnosti je potrebné zjednotiť definície pojmov v tejto oblasti, ktoré sú rôznym spôsobom definované v osobitných zákonoch. Zjednocovanie terminológie v oblasti informačnej bezpečnosti sa bude primárne týkať návrhov nových právnych predpisov. V existujúcich právnych predpisov sa bude aplikovať postup zmien právnych predpisov podľa dokumentu schváleného uznesením vlády č. 595/2009 „Analýza legislatívneho prostredia a zoznam právnych predpisov, určených pre implementáciu elektronického spracovania agend". Keďže terminológia informačnej bezpečnosti je rozsiahla a neustále sa vyvíja, zákon ustanoví ministerstvu financií povinnosť aktualizovať ju a zverejňovať, napríklad vo forme terminologického slovníka, vydávaného v papierovej forme alebo na webovom sídle.

2. časť - Postavenie orgánov štátnej správy, kompetencie a koordinácia riadenia informačnej bezpečnosti

Zákon v tejto časti ustanoví kompetencie orgánov štátnej správy v oblasti riadenia a koordinácie informačnej bezpečnosti vyplývajúce z cieľov navrhovaného zákona, pričom súčasné rozdelenie kompetencií, ktoré sa vyvinuli historicky, zostanú zachované.

Zákon ustanoví

a) minimálne prvky systému riadenia informačnej bezpečnosti v oblasti
   - koordinácie riadenia informačnej bezpečnosti,
   - štandardizácie informačnej bezpečnosti,
   - posudzovania rizík a ustanovenia kritickosti informácie alebo systému,
   - definovania opatrení a minimálnych bezpečnostných požiadaviek,
   - mechanizmov kontroly zavedenia opatrení,
   - rozširovania postupov a spôsobov riadenia,

b) formu a kompetencie medzirezortného zoskupenia zloženého z vedúcich predstaviteľov dotknutých subjektov, ktoré sú gestormi osobitných predpisov, tvoriacich prienik právnej úpravy informačnej bezpečnosti vo verejnej správe, pričom pôsobnosť a členstvo v medzirezortnom zoskupení ustanoví štatút.

Vzhľadom na globálny charakter informačných a komunikačných technológií, na zaistenie bezpečnosti vybraných systémov v tejto oblasti sa nestačí obmedziť na prijatie opatrení vzťahujúcich sa len na tieto technológie, ale je potrebné primerane chrániť aj prostredie, v ktorom pôsobia, t. j. ostatné informačné a komunikačné technológie. V konečnom dôsledku je potrebné zaistiť aspoň minimálnu úroveň ochrany všetkých informačných a komunikačných technológií a informácií, ktoré sa v nich spracovávajú na území Slovenskej republiky. Tieto systémy a informácie v nich spracovávané tvoria digitálny priestor. Niektoré časti digitálneho priestoru prešli samostatným vývojom a ich riadenie a ochrana je upravená osobitnými zákonmi.

V prvom rade ide o systémy určené na spracovávanie utajovaných skutočností. Utajované skutočnosti sa môžu vyskytovať aj v systémoch patriacich súkromným spoločnostiam, ktoré poskytujú služby štátu, a tak kybernetický priestor, ktorý je súčasťou digitálneho priestoru Slovenskej republiky, obsahuje popri štátnych systémoch aj súkromné informačné a komunikačné technológie. Ustanovenia zákona o informačnej bezpečnosti budú použiteľné aj pre tieto systémy. Vzhľadom na prienik právnej úpravy digitálneho a kybernetického priestoru budú v zákone o informačnej bezpečnosti zohľadnené aj niektoré spoločné ciele vyplývajúce z Koncepcie ochrany utajovaných skutočností v Slovenskej republike, schválenej uznesením vlády č. 475/2007 zo dňa 30. mája 2007. Tieto ciele budú zohľadnené najmä pri zavádzaní jednotnej terminológie základných pojmov z oblasti informačnej bezpečnosti, napríklad vymedzenie digitálneho a kybernetického priestoru, ďalej pri zavádzaní spoločnej kategorizácie informačných systémov verejnej správy v závislosti od klasifikácie spracúvaných informácií a pri zabezpečovaní súčinnosti a spolupráce medzi špecializovanými jednotkami na riešenie počítačových incidentov.

Špeciálnou kategóriou údajov, ktorých ochrana je nevyhnutná z dôvodu zaistenia súkromia, sú osobné údaje. Narábanie s nimi upravuje zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov. Podobne ako v prípade utajovaných skutočností sa aj osobné údaje vyskytujú v štátnych aj súkromných systémoch.

Kritickú infraštruktúru vo všeobecnosti tvoria systémy, a to nielen informačné, ktorých poškodenie alebo vyradenie z činnosti by mohlo vážne ohroziť, napríklad fungovanie štátu, zdravie a majetok osôb. Informačné a komunikačné technológie predstavujú špecifickú kategóriu aktív kritickej informačnej infraštruktúry, pretože mnoho systémov kritickej infraštruktúry vo všeobecnosti bezprostredne od nich závisí, napríklad banky, komunikačné systémy, riadenie výrobných systémov, doprava, štátna administratíva, výroba a zásobovanie. A práve tu je nevyhnutné zabezpečiť spoluprácu medzi subjektmi zodpovedajúcimi za jednotlivé sektory kritickej infraštruktúry pri špecifikácii požiadaviek na bezpečnosť informačných a komunikačných technológií podporujúcich systémy kritickej infraštruktúry.

Zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov zaraďuje internet a počítačové siete medzi elektronické komunikačné siete. Podľa tohto zákona majú príslušné kompetentné orgány rozsiahle regulačné a kontrolné právomoci. Z hľadiska informačnej bezpečnosti ide o aspekty, ako sú fyzická bezpečnosť sietí, dodržiavanie technických noriem, prevádzková bezpečnosť, elektromagnetické vyžarovanie, úprava podmienok odpočúvania komunikácie, šírenie reklamných správ, ochrana osobných údajov a údajov spojených s prevádzkou komunikačných sietí.

Elektronický podpis je tiež upravený osobitným zákonom, ale z hľadiska informačnej bezpečnosti predstavuje len jednu, aj keď dôležitú, bezpečnostnú funkciu, a nie je potrebné ho v zákone o informačnej bezpečnosti explicitne spomínať.

Medzi osobitné predpisy, ktoré pokrývajú špecifické oblasti informačnej bezpečnosti patria najmä

- zákon č. 179/1998 Z. z. o obchodovaní s vojenským materiálom a o doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení neskorších predpisov,
- zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov,

- zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,
- zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov,
- zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- návrh zákona o kritickej infraštruktúre (v legislatívnom procese),
- legislatívna úprava eHealth (v príprave).

Zdôvodnenie: Na zabezpečovaní ochrany digitálneho priestoru sa podieľa viacero štátnych inštitúcií, ktorých činnosť je potrebné koordinovať. Informačná bezpečnosť je širokospektrálna a previazaná s prevádzkou informačných a komunikačných technológií, a preto sa nedá zaistiť bez spolupráce správcov a prevádzkovateľov týchto systémov.

3. časť - Kategorizácia informačných systémov verejnej správy

V tejto časti zákona sa zavedie klasifikačná schéma pre informačné systémy verejnej správy a ustanovia sa procesy klasifikácie informačných systémov verejnej správy založených na kritickosti spracúvaných dát podľa aspektov dôvernosti, integrity, dostupnosti, a špecifickosti obsahu a ich potenciálneho negatívneho vplyvu na občanov, právnické osoby a štát. Ustanoví sa povinnosť povinných osôb podľa zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov kategorizovať údaje vo svojich informačných systémoch podľa tejto schémy s ohľadom na základné aspekty informačnej bezpečnosti a ustanoví sa minimálna povinná úroveň ich ochrany. Zároveň sa ustanovia minimálne bezpečnostné požiadavky a ciele riadenia informačnej bezpečnosti pre jednotlivé klasifikačné stupne

- podľa hodnoty a kritickosti informačných aktív, pričom informačnými aktívami sú spracovávané údaje,
- podľa vymedzenia pojmu „kritický informačný systém verejnej správy" a kritérií na určenie „kritickosti" informačného systému verejnej správy,
- podľa kompetencií a kritérií pre kontrolu bezpečnosti informačných systémov verejnej správy,
- v súlade s ostatnými právnymi predpismi, týkajúcimi sa narábania s údajmi.

Zdôvodnenie. Súčasná právna úprava neobsahuje klasifikáciu informačných systémov a klasifikáciu limitovaných informácií z bezpečnostných dôvodov s výnimkou klasifikácie osobných údajov a utajovaných skutočností. Sú to informačné systémy obsahujúce informáciu s nižšou mierou ochrany pred jej nedovoleným rozširovaním v porovnaní s utajovanými informáciami. Okruh osôb oprávnených oboznamovať sa s nimi bude určený jej pôvodcom bez potreby osobitného bezpečnostného preverovania pre vznik oprávnenia. Nakladanie s nimi bude podliehať ochranným opatreniam, o ktorých rozhodne subjekt, ktorý s informáciou nakladá na základe uváženia vhodnosti a dostatočnosti pre zaistenie ich ochrany bez nutnosti dodržiavania striktného režimu vzťahujúceho sa na utajované skutočnosti. Nevyhnutnosť vymedzenia tejto kategórie v právnom poriadku je daná napríklad aj potrebami vyplývajúcimi z aplikácie zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

4. časť - Jednotka pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike

V tejto časti zákon ustanoví postavenie a úlohy útvarov pre riešenie počítačových incidentov vo všeobecnosti, a špecificky pre vzniknutú jednotku pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike

- pri prevencii a pri riešení bezpečnostných incidentov v informačných systémoch verejnej správy, prípadne v celom slovenskom digitálnom priestore,
- vo vzťahu k špecializovaným útvarom pre riešenie počítačových incidentov a iným štátnym inštitúciám[6)], ktoré sa podieľajú na ochrane slovenského digitálneho priestoru,
- vo vzťahu k medzinárodným organizáciám podobného zamerania.

Jednotka pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike bude plniť úlohu tímu pre riešenie bezpečnostných incidentov v prostredí národnej informačnej a komunikačnej infraštruktúry, t. j. predovšetkým poskytovanie kontaktného miesta pre pomoc pri riešení bezpečnostných incidentov, ktoré zasahujú do národnej informačnej a komunikačnej infraštruktúry alebo majú v nej pôvod a sú zamerané na ciele mimo nej.

Medzi úlohy jednotky pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike patrí

- monitorovanie hrozieb,
- vytvorenie systému včasného varovania ako informovanie cieľových skupín o existujúcich hrozbách, varovanie potenciálnych cieľových skupín, vyhlásenie poplachu,
- pomoc pri riešení bezpečnostných incidentov,
- identifikácia, zaznamenávanie a vyhodnocovanie bezpečnostných incidentov,
- monitorovanie efektívnosti navrhovaných opatrení na riešenie bezpečnostných incidentov,

---

[6)] *Policajný zbor (počítačová kriminalita), Prokuratúra (podnety na trestné stíhania pri zistení počítačových zločinov), Ministerstvo obrany Slovenskej republiky (licenčné konanie), CSIRTy v špeciálnych zložkách, Školstvo – vzdelávanie, Spravodlivosť a súdy – legislatívna a expertná činnosť.*

- vzdelávanie a zvyšovanie všeobecného povedomia v oblasti informačnej bezpečnosti v Slovenskej republike,
- podpora rozvoja všeobecnej informačnej bezpečnosti v Slovenskej republike.
- spolupráca pri koordinácii národných úsilí pri ochrane digitálneho priestoru Slovenskej republiky a pri efektívnom zapojení sa do medzinárodnej spolupráce na základe analýzy potrieb a možností Slovenskej republiky v oblasti informačnej bezpečnosti.

Zákon ustanoví povinnosť jednotky pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike priebežne monitorovať stav informačnej bezpečnosti v informačných systémoch verejnej správy a predkladať súbornú správu o stave informačnej bezpečnosti vláde Slovenskej republiky.

Rovnako sa bude podieľať aj na vytváraní potrebnej legislatívy a na príprave a presadzovaní bezpečnostných štandardov.

Zdôvodnenie. Jednotka pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike nemá zatiaľ oporu v zákone na to, aby mohla vykonávať v plnej miere svoje úlohy. Na to, aby táto jednotka mohla plniť úlohu zásahového strediska pri ohrození alebo narušení informačnej bezpečnosti, a to najmä vo vzťahu k internetu vo všeobecnosti, a tej časti národnej informačnej a komunikačnej infraštruktúry[7)], ktorá je v jeho neformálnej pôsobnosti, je potrebné zákonne ustanoviť jej potrebné kompetencie.

5. časť - Štandardizácia

Zákon vytvorí štandardizačný rámec informačnej bezpečnosti, pričom bude nadväzovať na štandardizáciu podľa zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a na medzinárodné štandardy informačnej bezpečnosti. Súčasťou bude aj zavedenie minimálnych bezpečnostných požiadaviek na dodávku informačných systémov pre verejnú správu, a to ako pre prevádzkovateľov, tak aj dodávateľov týchto systémov. Zároveň zákon prostredníctvom štandardov ustanoví minimálne bezpečnostné požiadavky, ktoré bude musieť splniť nielen prevádzkovateľ informačného systému, ale aj jeho dodávateľ, nezávisle od zmluvy s povinnou osobou, ktorou je inštitúcia verejnej správy tak, aby bola zaručená minimálna úroveň informačnej bezpečnosti daného informačného systému. Štandardy sa budú okrem technických požiadaviek týkať aj procesnej oblasti riadenia informačnej bezpečnosti.

V nadväznosti na kategorizáciu informačných systémov verejnej správy podľa kritickosti spracúvaných údajov alebo kritickosti systému sa ustanovia požiadavky a postupy pre povinnú certifikáciu vybraných kategórií systémov. Certifikácia konkrétnej verzie informačného systému bude dokladom splnenia požiadaviek na bezpečnosť dodávaného informačného systému bez ohľadu na počet inštalácií systému.

Zdôvodnenie: Takto vytvorený systém organizačných a procesných štandardov umožní efektívne využívať zdroje vo verejnej správe neopakovaním rovnakej činnosti tvorby postupov a smerníc a zároveň umožní menším inštitúciám efektívnejšie riadenie informačnej bezpečnosti, pretože ich finančné aj interné ľudské zdroje pre oblasť informačnej bezpečnosti sú značne obmedzené. Povinným osobám bude umožnené si vytvoriť vlastný systém riadenia

7) Národnou informačnou a komunikačnou infraštruktúrou sú všetky systémy a komponenty informačných a komunikačných technológií na území štátu.

informačnej bezpečnosti, spĺňajúci požiadavky podľa zákona o informačnej bezpečnosti alebo prijať systém procesných a technických štandardov, vytvorených podľa tohto zákona.

6. časť - Vzdelávanie a certifikácia osôb v informačnej bezpečnosti

V zmysle vládnej stratégie vzdelávania v informačnej bezpečnosti zákon ustanoví minimálne znalostné štandardy vo verejnej správe pre osoby s kompetenciami v oblasti riadenia informačnej bezpečnosti a vytvorenie vzdelávacieho a certifikačného rámca. Pre tento účel budú ustanovené minimálne požiadavky na vzdelanie a certifikáciu podľa jednotlivých stupňov kategorizácie.

Zdôvodnenie: Cieľom zákona je aj zvýšenie celkového povedomia v oblasti informačnej bezpečnosti.

7. časť – Bezpečnosť elektronickej verejnej správy

Zákon bude riešiť

- bezpečnú komunikáciu medzi elektronickými službami a registrami verejnej správy,
- minimálne bezpečnostné opatrenia pre základné prístupové komponenty elektronickej verejnej správy,
- bezpečnostné požiadavky na rozhrania aplikácií typu „komunikácia medzi orgánmi verejnej správy“,
- identifikáciu a autentifikáciu spojenú s poskytovaním a využívaním služieb elektronickej verejnej správy,
- požiadavky na využívanie elektronického podpisu pri komunikácii medzi orgánmi verejnej správy,
- audit a kontrola bezpečnosti služieb elektronickej verejnej správy,
- bezpečné elektronické cezhraničné a medzisektorové interakcie medzi európskymi inštitúciami verejnej správy.

Zdôvodnenie: Informačné a komunikačné technológie prenikli aj do práce vládnych orgánov a verejnej správy, a to vzhľadom na prechádzanie na služby elektronickej verejnej správy na všetkých úrovniach, ako aj vzhľadom na ich nové uplatnenia, napríklad v inovatívnych riešeniach súvisiacich so zdravotníctvom, energetikou, obchodom a politickou angažovanosťou, kde sa verejný sektor stáva silne závislým na informačných a komunikačných technológiách.

8. časť – Bezpečnosť internetu

Zákon vymedzí

- priority štátu pre kritické zložky internetu, týkajúce sa napríklad správy domén, internetových adries a protokolov a záležitosti týkajúce sa internetu, kde ministerstvo financií zohráva úlohu gestora,
- vypracovanie zásad a usmernení pre odolnosť a stabilitu internetu k dokumentom „Národná koncepcia pre informatizáciu verejnej správy“ a „Národná stratégia pre informačnú bezpečnosť“; pôjde o štátnu úroveň, kde rezortné organizácie vypracujú zásady a usmernenia pre odolnosť a stabilitu internetu, pričom sa treba zamerať na regionálne nápravné opatrenia, dohody o vzájomnej pomoci, stratégie koordinovanej

obnovy a kontinuity, zemepisné rozmiestnenie kritických internetových zdrojov, technologické bezpečnostné záruky v internetovej architektúre a protokoloch, replikáciu a rozmanitosť služieb a údajov a na ďalšie súvisiace aktivity,

- kompetencie, zodpovednosti a koordináciu pri rozsiahlom narušení slovenského internetového priestoru, napríklad pri vyradení časti serverov poskytujúcich kľúčové služby elektronickej verejnej správy,
- bezpečnostné požiadavky na kritické informačné systémy verejnej správy závislé od služieb internetu, bezpečnostné požiadavky na poskytovateľov internetu pre kritické informačné systémy verejnej správy,
- bezpečné a vierohodné rozpoznávanie doménových mien.

Zdôvodnenie: Zákon venuje osobitnú pozornosť internetu ako súčasti kritickej infraštruktúry vo všeobecnosti tak, aby sa zabezpečila jeho odolnosť a stabilita na základe opatrení. Ide o dosiahnutie spoločného konsenzu o prioritách pre odolnosť a stabilitu internetu, pokiaľ ide o verejnú správu a jeho uvádzanie do prevádzky a zahrnutie organizácií do procesu vypracúvania súboru zásad. V zásadách by sa odzrkadľovali základné hodnoty, a to pre odolnosť a stabilitu internetu v rámci nášho štátu.

9. časť – Bezpečnosť špecifických technológií

V tejto časti zákon vytvorí všeobecný bezpečnostný rámec a podmienky možnosti používania bezkontaktných identifikačných zariadení a spracovania údajov založených na báze rádiofrekvenčného prenosu. Sú to najmä rádiofrekvenčné identifikačné technológie (RFID) ohrozujúce súkromie občanov. Ide predovšetkým o skupinu automatickej identifikácie zberu dát, ktorá zahŕňa čiarové kódy, biometrické snímanie údajov, magnetické pásky a magnetické prúžky, optické znakové rozpoznávanie, čipové karty, hlasové rozpoznávanie a podobné technológie postavené na tomto princípe.

Táto časť zároveň určí rámec pre koordinované riešenie oblasti nevyžiadanej elektronickej pošty.

Zdôvodnenie: Aplikácie založené na rádiofrekvenčných identifikačných technológiách (RFID) sú dlhodobo používané pri preprave a ochrane tovarov, v prístupových kontrolných a identifikačných systémoch, napríklad pri vstupoch do budov, chránených objektov a obchodov, pri diaľničných kontrolách, pri vstupoch na rôzne športové a kultúrne podujatia a v poslednom čase aj v identifikačných osobných kartách, bankových kartách a pasoch osôb, pri výrobe a logistike distribúcie tovaru, automobilovom priemysle a zdravotníctve.

10. časť – Požiadavky na proces riadenia informačnej bezpečnosti

Táto časť zákona upraví minimálne požiadavky na proces riadenia informačnej bezpečnosti a jeho náležitosti u povinných osôb, čím umožní definovať minimálne procesné a organizačné aspekty, ktorými sú najmä

- definovanie cieľov, rozsahu a organizačných prostriedkov riadenia informačnej bezpečnosti, napríklad bezpečnostná politika, mechanizmy riadenia a koordinácie informačnej bezpečnosti u povinnej osoby,

- aktivity identifikovania a hodnotenia rizík informačnej bezpečnosti ako hodnotenie vplyvov, zraniteľností a hrozieb a z nich vyplývajúcich rizík, a to aj v nadväznosti na kritickosť údajov a systémov,
- aktivity rozhodnutia o spôsobe riadenia rizika podľa miery identifikovaného rizika,
- identifikácia záväzných bezpečnostných opatrení vyplývajúcich z príslušnej legislatívy a iných štandardizačných zdrojov aj v nadväznosti na štandardizáciu podľa tohto zákona,
- definovanie bezpečnostných mechanizmov, a to procesných, organizačných aj technických, v zmysle identifikovaných záväzných opatrení a rozhodnutí o spôsobe riadenia rizika,
- definovanie prostriedkov pre zabezpečenie implementácie a prevádzky bezpečnostných opatrení,
- definovanie prostriedkov kontroly uplatňovania definovaných bezpečnostných mechanizmov,
- definovanie postupov riešenia bezpečnostných incidentov v prípade narušenia definovaných cieľov informačnej bezpečnosti u povinnej osoby aj v nadväznosti na mechanizmy riešenia incidentov podľa tohto zákona.

Ako je uvedené v časti o štandardizácii, tieto aspekty by povinná osoba napĺňala buď tvorbou vlastných postupov, alebo prijatím štandardov vytvorených podľa tohto zákona.

Zdôvodnenie: Vzhľadom na to, že v súčasnosti neexistuje rámec procesu riadenia informačnej bezpečnosti, je potrebné ustanoviť požiadavky na tento proces riadenia tak, aby tieto požiadavky slúžili aj ako dobrovoľný referenčný rámec pre ostatné subjekty pri úprave ich zmluvných vzťahov.

11. časť – Spôsob a výkon kontrolnej činnosti

V tejto časti zákon ustanoví štandardné požiadavky na výkon, spôsob výkonu a oprávnenie vykonávať kontrolu dodržiavania povinností v oblasti informačnej bezpečnosti, najmä toho, či sú systémy a informácie povinných osôb chránené v súlade s definovanými požiadavkami. Pokiaľ osobitný zákon neustanoví inak, orgán, v ktorého kompetenciách je definovanie požiadaviek na informačnú bezpečnosť, má právomoc vykonávať kontrolu dodržiavania ním definovaných požiadaviek u povinnej osoby. Zákon zároveň ustanoví všeobecné sankčné mechanizmy pre nedostatky zistené pri výkone týchto kontrolných činností.

V nadväznosti na príslušné ustanovenia, ktoré sa nachádzajú v osobitných zákonoch platných v Slovenskej republike, napríklad overenie bezpečnosti informačného systému banky podľa zákona č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, výkon auditu treťou stranou podľa zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, audit bezpečnosti informačného systému podľa zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov, zákon ustanoví kompetenciu príslušnému regulačnému orgánu vyžiadať si od dotknutej osoby v špecifických prípadoch nezávislý audit a rovnako aj požiadavky na osoby oprávnené vykonávať takýto audit.

Zákon ďalej ustanoví povinnosť príslušných regulačných orgánov koordinovať vzájomne svoj výkon v medziach platnej legislatívy pri výkone kontrolných činností. Ak

regulačný orgán pri výkone svojej kontrolnej činnosti zistí skutočnosti, ktoré poukazujú na možnosť porušenia povinností povinnej osoby v oblasti informačnej bezpečnosti definovaných iným osobitným zákonom alebo iným regulačným orgánom, má povinnosť informovať o tejto skutočnosti príslušný regulačný orgán.

Zdôvodnenie: Súčasný právny poriadok Slovenskej republiky obsahuje viacero právnych noriem, v ktorých je čiastkovo upravený spôsob a výkon kontrolnej činnosti, týkajúcej sa informačnej bezpečnosti, tieto však nie sú navzájom zosúladené. Cieľom zákona je napraviť tento stav harmonizáciou kompetencií príslušných subjektov v oblasti kontrolnej činnosti a v oblasti ukladania sankčných opatrení. Pri samotnej tvorbe zákona o informačnej bezpečnosti bude upriamená pozornosť na osobitné predpisy, v ktorých je čiastkovo upravený spôsob a výkon kontrolnej činnosti. Zákon ustanoví kontrolné právomoci príslušných orgánov tak, aby boli jednoznačne definované a tým bolo možné jednoznačne vyvodiť zodpovednosť príslušného subjektu.

12. časť - Riešenie bezpečnostných incidentov

Zákon ustanoví jednotný a systematický rámec notifikácie o významných bezpečnostných incidentoch v regulovaných oblastiach.

Zdôvodnenie:

Predmetom jednotného systematického riešenia incidentov bude nahlásenie incidentu na príslušný regulačný orgán a koordinácia riešenia incidentu v spolupráci so systémom útvarov pre riešenie počítačových incidentov vytvorených podľa zákona o informačnej bezpečnosti.

Vzhľadom na to, že táto problematika sa týka aj spracovania osobných údajov v sektore elektronických komunikácií, pri tvorbe zákona o informačnej bezpečnosti sa prihliadne aj na zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov, do ktorého bude v roku 2011 transponovaná smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa. Podľa tejto smernice je členským štátom ustanovená povinnosť do 25. mája 2011 prijať a uverejniť zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou, t.j. okrem iného, aby v prípade porušenia ochrany osobných údajov poskytovateľ verejne dostupných elektronických komunikačných služieb oznámil bez zbytočného meškania porušenie ochrany osobných údajov príslušnému národnému orgánu.

13. časť - Dohľad a správne konanie

Zákon o informačnej bezpečnosti ustanoví dohliadajúci orgán pre oblasť riadenia informačnej bezpečnosti vo verejnej správe a upraví správne konanie a právne postihy za porušenie tohto zákona. Orgánom dohľadu bude ministerstvo financií.

Zdôvodnenie: Ustanoviť dohliadajúci orgánu je potrebné z dôvodu zabezpečenia implementácie právnej úpravy a pre prípad porušenia právnej úpravy respektíve nesúladu so zákonom o informačnej bezpečnosti.

14. časť – Splnomocňovacie ustanovenie

Táto časť bude obsahovať splnomocňovacie ustanovenie na vydanie vykonávacích predpisov podľa tohto zákona

Zdôvodnenie: Vykonávacie predpisy budú podrobne upravovať najmä oblasť

- vzdelávania a certifikácie osôb v informačnej bezpečnosti a
- bezpečnosti elektronickej verejnej správy, internetu a špecifických technológií.