Kybernetická bezpečnosť a štát

Ján Hochmann
Národný bezpečnostný úrad

Obsah

- História a analógia procesov
- Akčný plán ku Koncepcii kybernetickej bezpečnosti na roky 2015 – 2020 a jeho oblasti/priority
- Inštitucionálny rámec – kompetenčné rozloženie právomocí
- Návrh zákona o KB a jeho oblasti

História a analógia procesov

- Štátny rozpočet
- Projekty „PHARE“ (ÚV SR)
- Koncepcie, Stratégie, Akčné plány, úlohy/projekty (2004 - ...)
- Štrukturálne fondy: 2005 - 2006 (MVRR SR)
- Štrukturálne fondy/operačné programy: 2007 – 2013 (MF SR a ÚV SR)
- Operačné programy: 2014 – 2020 (.....)

História a analógia

- **Národná stratégia** pre informačnú bezpečnosť v Slovenskej republike (ďalej len „NSIB“), schválená uznesením vlády Slovenskej republiky č. 570/2008,
- Návrh **Akčného plánu** na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, schválený uznes. vlády SR č. 46/2010,
- **Legislatívny zámer zákona o IB**, schválený uznes. vlády SR č. 136/2010,
- Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii,
- **Koncepcia kybernetickej bezpečnosti** Slovenskej republiky na roky 2015-2020, (uznes. vlády SR č. 328/2015).
- **Akčný plán ku Koncepcii kybernetickej bezpečnosti** SR na roky 2015 až 2020, (uznes. vlády SR č. 95/2016)

Akčný plán ku Koncepcii KB na roky 2015 - 2020

Sedem vecných oblastí/priorít a ich rozpracovanie

1. Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.
2. Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.
3. Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru.
4. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti.
5. Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami.
6. Aktívna medzinárodná spolupráca.
7. Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti.

Inštitucionálny rámec – kompetenčné rozloženie právomocí

Ústredný orgán pre kybernetickú bezpečnosť

- NBÚ (od 1. 1. 2016 - kompetenčný zákon)

Koordinácia a riadenie

- MV SR (zákon č. 45/2011 Z. z. o kritickej infraštruktúre)
- MF SR (zákon č. 275/2006 Z. z. o ISVS)

Výkon v oblasti kritickej infraštruktúry - sektory

- MF SR, MDVRR SR, MH SR, MZ SR, MŽP SR

Špecifická oblasť

- MO SR (zákon o obrane SR, vojenská oblasť - NATO)

- **Stratégia pre informačnú bezpečnosť v Slovenskej republike**
  - Uznesenie vlády SR č. 270/2008 (pripraviť legislatívny zámer zákona o IB)
- **Legislatívny zámer zákona o informačnej bezpečnosti**
  - Uznesenie vlády SR č. 136/2010 - predložiť návrh zákona o IB (rok 2012)
- **Návrh zákona o informačnej bezpečnosti (MF SR)**
  - Návrh zákona o IB vypracovaný v októbri 2014 (legislatívny proces zastavený)
  - Nový termín predloženia návrhu do vlády - 30. 12. 2016
- **Návrh zákona o kybernetickej bezpečnosti (NBÚ)**
  - Uznesenie vlády SR č. 328/2015 ku Koncepcii kybernetickej bezpečnosti
  - Plánovaný termín predloženia návrhu do vlády - 28. 2. 2016
- Zrušenie uznesení vlády SR č. 136/2010 a č. 328/2015 uznesením vlády SR **č. 93/2016** a stanovenie novej úlohy pre NBÚ + MF SR na **september 2016**

Predmet zákona o kybernetickej bezpečnosti

Úprava oblastí

a) pôsobnosť orgánov štátnej správy na úseku kybernetickej bezpečnosti,

b) práva a povinnosti fyzických a právnických osôb v oblasti kybernetickej bezpečnosti,

c) pôsobnosť a požiadavky na útvary pre riešenie bezpečnostných incidentov v kybernetickom priestore,

d) rámec notifikácie a riešenia bezpečnostných incidentov v kybernetickom priestore,

e) klasifikácia informácií a kategorizácia IS,

f) ustanovenie minimálnych požiadaviek na bezpečnosť jednotlivých kategórií IS počas ich životného cyklu,

g) zavedenie procesu riadenia informačnej bezpečnosti,

h) kontrolu bezpečnosti a audit bezpečnosti,

i) spôsobilosti a vzdelávanie v kybernetickej bezpečnosti,

j) zodpovednosť za porušenie povinností.

Pojmy a vymedzenie priestoru

1. Digitálny priestor je súhrn

a) **informačných a komunikačných technológií,** vrátane ich programového vybavenia a informačných systémov a sietí,

b) **informácií, vrátane údajov**, ktoré sa prenášajú, spracovávajú alebo uchovávajú prostredníctvom informačných a komunikačných technológií alebo opisujú štruktúru, konfiguráciu a činnosť informačných a komunikačných technológií,

c) **procesov,** ktoré prebiehajú v rámci informačných a komunikačných technológií,

d) **podpornej infraštruktúry** zabezpečujúcej činnosť informačných a komunikačných technológií, vrátane elektronických komunikačných sietí, a

e) **vzťahov medzi údajmi a informáciami** podľa bodu b) a pravidiel upravujúcich tieto vzťahy,

2. Digitálny priestor

- **štátu** alebo organizácie je časť digitálneho priestoru v ich pôsobnosti, pričom táto organizácia alebo štát majú právo určovať pravidlá a spôsob fungovania príslušnej časti digitálneho priestoru a majú prostriedky na presadzovanie týchto pravidiel,
- **Slovenskej republiky** je časť digitálneho priestoru v pôsobnosti Slovenskej republiky, na ktorý sa vzťahujú všeobecné právne predpisy Slovenskej republiky

3. Kybernetický priestor

je časť digitálneho priestoru pozostávajúca zo všetkých informačných systémov prepojených na globálnej dátovej úrovni, pričom jej základom je Internet; informačný systém alebo prvok v izolovanom priestore nie je súčasťou kybernetického priestoru.

Správa na úseku kybernetickej bezpečnosti

Subjekty

a) Vláda Slovenskej republiky (ďalej len **„vláda“)**

b) Národný bezpečnostný úrad (ďalej len **„úrad“)**

c) Ústredný orgán štátnej správy podľa osobitného predpisu, ktorý je vecne príslušnou autoritou (ďalej len **„vecne príslušná autorita“**)

d) Jednotky a útvary pre riešenie počítačových bezpečnostných incidentov (ďalej len **„CSIRT“)**

Povinné osoby

a) osoby, ktoré sú správcami informačného systému verejnej správy podľa osobitného predpisu,

b) prevádzkovatelia informačných systémov, ktoré sú významnými informačnými systémami,

c) prevádzkovatelia prvkov kritickej infraštruktúry, pričom súčasťou týchto prvkov je časť digitálneho priestoru Slovenskej republiky podľa osobitného predpisu,

d) poskytovatelia elektronických komunikačných sietí a poskytovatelia elektronických komunikačných služieb podľa osobitného predpisu,

e) osoby, na ktoré sa vzťahujú všeobecné právne predpisy Slovenskej republiky, najmä poskytovatelia služieb informačnej spoločnosti podľa osobitného predpisu, prevádzkovatelia hazardných hier podľa osobitného predpisu a poskytovatelia služieb podľa osobitného predpisu.

Informácie a systémy, bezpečnostné požiadavky, úrovne

- **Základnými bezpečnostnými požiadavkami** na klasifikáciu informácií systémov sú: „autentickosť“, „dostupnosť“, „dôvernosť“ a „integrita“
- **Bezpečnostné úrovne** informácie na základe vážnosti dopadu alebo ujmy sú
  a) nepodstatná,
  b) nízka,
  c) stredná,
  d) vysoká.
- **Súbory min. bezpečnostných opatrení** a metóda klasifikácie - vyhláška.

Informácie a systémy

- **Informačné systémy** sa kategorizujú na základe každej základnej bezpečnostnej požiadavky osobitne a to vo vzťahu ku každej základnej bezpečnostnej požiadavke do kategórií podľa úrovne ich ochrany, ktorá je
  a) nízka,
  b) stredná
  c) vysoká
- **významný informačný systém** sa zaraďuje do kategórie strednej úrovne ochrany
- **informačný systém podľa osobitného predpisu** (napr.: zákon č. 45/2011 Z.z., zákon č. 319/2002 Z. z.) sa zaraďuje do vysokej úrovne ochrany.

Ochrana informačných systémov

a) Pre **všetky informačné systémy** sa použije súbor bezpečnostných opatrení nízkej úrovne a pre všetky informačné systémy strednej úrovne sa použije súbor bezpečnostných opatrení strednej úrovne.

b) Pre informačné systémy s vysokou úrovňou ochrany sa vypracuje kvalitatívna analýza rizík.

c) Bezpečnostná politika a bezpečnostný projekt informačného systému (metodické zjednotenie tvorby BP).

Životný cyklus informačného systému

- Povinná osoba zabezpečí **ochranu informačného systému počas** celého jeho **životného cyklu**, ktorý sa skladá z:

a) **prípravnej fázy** vytvárania alebo úpravy informačného systému,

b) **inicializačnej a realizačnej fázy** vytvárania alebo úpravy informačného systému,

c) **dokončovacej fázy** vytvárania alebo úpravy informačného systému,

d) **prevádzkovej fázy** informačného systému a

e) **vyraďovacej fázy** informačného systém

Procesy riadenia

a) Zavedenie systému riadenia IB/KB vo svojej organizácii,

b) zadefinovanie cieľov, rozsahu, podmienok, kompetencií jednotlivcov a organizačných zložiek povinnej osoby a organizačných prostriedkov,

c) ustanovenie organizačných útvarov, funkčných miest a rol, ktoré zabezpečujú riadenie KB,

d) zriadenie a personálne obsadenie **riadiacej**, **výkonnej** a **kontrolnej** zložky systému riadenia kybernetickej bezpečnosti, *(neprípustná ich vzájomná kumulácia!).*

Vzdelávanie v Kybernetickej bezpečnosti

- **Ministerstvo školstva** vypracováva minimálne znalostné požiadavky vo forme štandardov pre oblasť kybernetickej bezpečnosti pre kategórie
  a) laických používateľov informačných systémov,
  b) riadiacich pracovníkov,
  c) informatikov, ktorí nie sú špecialisti na informačnú a kybernetickú bezpečnosť,
  d) informatikov, ktorí sú špecialisti na informačnú bezpečnosť,
  e) audítorov informačnej bezpečnosti.
- Znalostné štandardy (vykonávací predpis: MŠVVŠ SR, NBÚ, ...)
- Zavedenie/zabezpečenie povinného vzdelávania v IB na pracoviskách

Bezpečnostné incidenty

- **Povinné nahlasovanie** počítačových bezpečnostných incidentov na kontaktné miesto
  a) pre významné informačné systémy
  b) pre systémy kritickej informačnej infraštruktúry
- Štandardizácia procesu nahlasovania (formuláre, ...)
- Zavedenie bezpečnostných opatrení na detekciu incidentov/evidencia
- Vedenie evidencie

Internet

- **Gestor štátu** pre kritické zložky internetu: „národná doména .sk," „doména druhej úrovne," „internetové adresy" a „internetové protokoly" a ďalšie prvky týkajúce sa správy internetu na národnej úrovni,
- **vypracovanie zásad** a usmernení pre odolnosť a stabilitu internetu pre štátnu správu (MF SR vydá pravidlá/usmernenia),
- **povinné osoby:** „Prevádzkovateľ DB menného priestoru domén druhej úrovne," „registrátor domén druhej úrovne"

Ďalšie časti a doplnenia návrhu

- **Kontroly a bezpečnostné audity**

- **Zmeny a doplnenia iných právnych predpisov**

ĎAKUJEM ZA POZORNOSŤ
Otázky?