Ministerstvo financií
Slovenskej republiky

EFQM

Koncepcia vytvárania legislatívnych pravidiel pre zabezpečenie ISVS

ITAPA - 26. október 2011

Jan Hochmann
Ministerstvo financií SR
Štefanovičova č. 5, 817 82 Bratislava 15

Ministerstvo financií
Slovenskej republiky

EFQM

Obsah

1. Globálne prostredie a rámec

- Ľudské činnosti a nové aktivity
- Hranice, hrozby, ohrozenia
- Nové technológie

2. Strategické materiály a legislatíva

- Strategické materiály a nové výzvy
- Smernice a nariadenia EÚ / EK
- Legislatíva na národnej úrovni
- Princípy členenia digitálneho priestoru na sektory a kritická infraštruktúra
- Kategorizácia ISVS a stanovenie minimálnych požiadaviek na IKT
- Minimálne požiadavky na bezpečnosť elektronickej verejnej správy / Internet

Globálne prostredie a rámec - ľudské činnosti, nové aktivity

- Nové povolania (web obchody, výmena informácií, vyhľadávanie informácií, lotérie)
- Videokonferencie (pracovné stretnutia a porady na diaľku),
- Voľná komunikácia (poradenstvo, štatistiky, analýzy, cenníky),
- Certifikácie (nové štandardy / normy, školenia, eLearning),
- Autorské právo, obchodné právo v priestore IKT,
- Sociálne siete (masovokomunikačné médiá, Facebook a pod.),
- Elektronická verejná správa (VS)
  - elektronické služby a registre verejnej správy, základné prístupové komponenty eVS,
  - komunikácia medzi orgánmi VS,
  - identifikácia a autentifikácia spojená s poskytovaním a využívaním služieb eVS,
  - využívanie elektronického podpisu pri komunikácii,
  - elektronické cezhraničné a medzisektorové interakcie medzi európskymi inštitúciami VS.

Hranice / hrozby / ohrozenia

Prínos internetu:

- Neohraničený priestor,
- Voľné pravidlá prevádzky internetu,
- Elektronická pošta,
- Voľný pohyb produktov,
- Konkurenčné prostredie (eObchod - nie sú fyzické sklady tovarov),

Nové technológie

- Bezkontaktné identifikačné zariadenia a spracovanie údajov na báze rádiofrekvenčného prenosu (RFID),
- Biometrická identifikácia,
- Čiarové kódy,

Použitie:

Bankomatové karty, osobné karty, čipové karty (eHealth, diaľničná kontrola, ochrana objektov a tovaru, priemyselné účely, kamerové systémy spracovania informácií, hromadná archivácia a spracovanie dát v telekomunikačnej oblasti, eVouting, el. sčítanie ľudí a pod.)

Hranice: je veľmi ťažké určiť kde? (možnosť zneužitia - sledovanie osôb, spam ?)

- **Ohrozenie / zneužitie**
  - Krádeže identity,
  - Poškodenia majetku a dobrého mena,
  - Zámena identity (úmyselná / neúmyselná / ohrozenie detí),
  - Sledovanie osôb,
  - Spamy (nevyžiadaná pošta).
- **Ochranné prostriedky**
  - Legislatívne,
  - Technologické,
  - Technické,
  - Organizačné (vzdelávanie / povedomie)
- **Úloha štátu**
  - Tvorba legislatívy,
  - Vytváranie podmienok,
  - Regulácia trhu,
  - Dohľad,
  - Sankcie za porušovanie

Ministerstvo financií
Slovenskej republiky

EFQM

Strategické materiály a legislatíva

Východiská: NSIB - legislatíva a súvisiace dokumenty

- Smernica Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu
- Smernica Rady 2008/114/ES o identifikácii a označení kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu
- Digitálna agenda 2010 - 2015 (15. mája 2010)
- Európska bezpečnostná stratégia a Plán rozvoja spôsobilostí z roku 2008 novelizovaná v roku 2011
- Nová štúdia kybernetickej obrany v rámci EÚ – (spoločná jednotná terminológia - rok 2011), kto je za čo zodpovedný, vytvorenie pracovného tímu
- Návrh akčného plánu k NSIB na roky 2009 až 2013 k NSIB (január 2010)
- Legislatívna analýza a návrh právnych predpisov (august 2009)
- ratifikácia vzájomnej Dohody o boji proti kybernetickému zločinu ČŠ (vypracuje COM)
- Dohoda o min. požiadavkách a štandardoch v doméne kybernetickej bezpečnosti

Ministerstvo financií
Slovenskej republiky

EFQM

Legislatíva na národnej úrovni - (vybraná)

- **Zákon č. 45/2011 o ochrane kritickej infraštruktúry**
- **Zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,**
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy,
- Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností,
- Zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov,
- Zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom v znení neskorších predpisov,
- **Návrh zákona o elektronizácii administratívnych procesov (zákon o eGov)**
- **Návrh zákona o informačnej bezpečnosti,**

Výzvy v sieťovej a informačnej bezpečnosti

- **Ciele útokov:**
  - Cloud computing
  - Internetové služby
  - Platobné operácie (kreditné a platobné karty)
  - RFID (rádiofrekvenčná bezkontaktná identifikácia, tovary, služby, transakcie)
- **Hlavné smery vývoja technológií**
  - Mobilná revolúcia (manažment digitálneho prostredia cez mobily) predstavuje problém ohrozenia súkromia prístupnosti údajov
  - Cloud computing (outsorce IKT predstavuje problém s infraštruktúrou)
  - Explózia informácií a enormný nárast dát (dnes cca 380 bil. DVD)
  - Virtualizácia (prepojenie medzi prvkami)
  - Sociálne siete (zneužitie dát a politická moc)
  - Ochrana ľudských práv a duševného vlastníctva (trvalý problém)
  - Nárast hrozby kybernetických útokov

2. Legislatíva na národnej úrovni

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre

- **Smernica Rady 2008/114/ES**
  - zo dňa 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení zlepšiť ich ochranu

  Gestor zákona – Ministerstvo vnútra SR

  - účinnosť od 1. marca 2011

- **Štruktúra zákona**

  Predmet zákona
  - Organizácia a pôsobnosť OŠS na úseku kritickej infraštruktúry
  - Postup pri určovaní prvkov KI
  - Povinnosti prevádzkovateľa pri ochrane prvku KI
  - Vrátane obrannej infraštruktúry
  - Prechodné ustanovenia - úlohy

- **Základné pojmy - štruktúra**
  - ➢ **Prvok** kritickej infraštruktúry (časť ktorej zničenie má vážne dôsledky na funkciu štátu)
  - ➢ **Sektor kritickej infraštruktúry** (časť / oblasť do ktorej sú zaradené prvky)
  - – Kritická infraštruktúra (systém členený na sektory a prvky)
  - ➢ **Sektorové kritériá** (súbor tech. a sektorových kritérií s prahovými hodnotami v sektore)
  - – Prierezové kritériá (súbor kritérií s prahovými hodnotami pri určovaní všetkých sektorov)
  - – Prvkom európskej kritickej infraštruktúry (negatívny dosah na štát EÚ)
  - ➢ **Európske sektorové kritériá** (európska KI v sektore)
  - – Európske prierezové kritériá (určovanie prvkov v európskej KI)
  - – Ochrana prvku (zabezpečenie funkcionality, integrity, a kontinuity činnosti prvku s cieľom predísť, odvrátiť alebo zmierniť hrozbu narušenia alebo zničenia)
  - ➢ **Analýza rizík sektora** (dokument obsahujúci posúdenie hrozby narušenia alebo zničenia)
  - – Citlivou informáciou (neverejná informácia, ktorej zverejnenie by mohlo poškodiť ...)
  - – Prevádzkovateľom (právnická, fyzická osoba – podnikateľ alebo fyzická osoba, ktorá je vlastníkom prvku alebo z iného právneho dôvodu prevádzkuje prvok)
  - – Mechanickým zábranným prostriedkom
  - – Technický zabezpečovacím prostriedkom

- **Spoločné, prechodné a záverečné ustanovenia**
  - ÚOŠS predloží návrh sektorových kritérií 31. 3.2011
  - Ministerstvo predloží vláde návrh všetkých kritérií 31. 5.2011
  - ÚOŠS predloží MV SR návrh prvku a jeho zaradenie do sektoru 31. 8.2011
  - ➢ **Ministerstvo predloží vláde - II - 31.10.2011**
  - ÚOŠS predloží ministerstvu analýzu rizík sektora 31.10.2012

- **Prílohy**
  - Postup podľa etáp pri určovaní prvku a prvku európske kritickej infraštruktúry
  - Minimálny postup pri vypracúvaní bezpečnostného plánu
  - Sektory v pôsobnosti ústredných orgánov
  - 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).

Ministerstvo financií
Slovenskej republiky

EFQM

Sektory v pôsobnosti ústredných orgánov:

Sektor	Podsektor	ÚOŠS
1. Doprava	Cestná, letecká, vodná, železničná,	MDVRR SR
2. Elektronické komunikácie	Satelitná komunikácia, Siete a služby pevných a mobilných elektronických komunikácií	MDVRR SR
3. Energetika	Baníctvo, Elektroenergetika, Plynárenstvo, Ropa a ropné produkty,	MH SR
4. Informačné a komunikačné technológia	Informačné systémy a siete, Internet	MF SR
5. Pošta	poštové služby, poštový platobný styk a obstarávateľská činnosť	MDVRR SR
6. Priemysel	Farmaceutický, hutnícky, chemický,	MH SR
7. Voda a atmosféra	Meteorologická služba, vodné stavby, zabezpečenie pitnej vody,	MŽP SR
8. Zdravotníctvo		MZ SR

Ministerstvo financií
Slovenskej republiky

EFQM

Legislatíva na národnej úrovni

- **SMERNICA EURÓPSKEHO PARLAMENTU A RADY 2009/140/ES** z 25. novembra 2009, ktorou sa menia a dopĺňajú smernice 2002/21/ES o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby, 2002/19/ES o prístupe a prepojení elektronických komunikačných sietí a príslušných zariadení a 2002/20/ES o povolení na elektronické komunikačné sieťové systémy a služby.

- **ZÁKON č. 610/2003 Z. z. o elektronických komunikáciách, § 64:**
  - zabezpečenie bezpečnosti, integrity, predchádzanie incidentom
  - poskytovanie informácie podľa odseku 3 regulačným orgánom v členských štátoch a agentúre ENISA,
  - úrad každoročne predkladá Európskej komisii a agentúre ENISA súhrnnú správu o oznámeniach podľa odseku 3 a o opatreniach, ktoré v tejto súvislosti vykonal.

2. Zákon o informačnej bezpečnosti – (IB)

1. Legislatívny zámer zákona

- uznesenie vlády SR č. 136/2010 zo dňa 25. februára 2010

2. Návrh § - ého znenia zákona o IB

- predpokladaná účinnosť rok 2012

Štruktúra návrhu zákona o IB

- **Cieľ zákona**

  Vytvorenie základných podmienok pre zaistenie IB digitálneho priestoru v Slovenskej republike

- **Predmet zákona**

  Terminológia, kompetencie, štandardy, proces riadenia, klasifikácia IS, postavenie CSIRT.SK, minimálne znalostné štandardy, minimálne bezpečnostné požiadavky pre el. verejnú správu, minimálne požiadavky pre bezpečnosť internetu

- **Vymedzenie základných pojmov**
  - Informačná bezpečnosť: ochrana IS a informácií ktoré sú v nich prenášané a spracovávané,
  - Elektronický priestor / digitálny priestor / kybernetický priestor,
  - Informácia / citlivá informácia / údaj,
  - Informačné a komunikačné technológie – IKT,
  - Informačný systém / informačný systém verejnej správy,
  - Aktívum (to čo inštitúcia vlastní, používa, vytvára, poskytuje a má pre ňu hodnotu)
  - Dostupnosť / dôvernosť / integrita / autentickosť,
  - Entita,
  - Identita / súkromnosť / nepopretie prijatia pôvodu,
  - Hrozba / nositeľ hrozby / zraniteľnosť / riziko,
  - Analýza rizík / prijateľné riziko / zvyškové riziko / opatrenie,
  - Bezpečnostný zámer / bezpečnostná politika,
  - Klasifikácia / bezpečnostná požiadavka,
  - Bezpečnostná záruka,
  - Národná informačná komunikačná infraštruktúra – NIKI.

Kategorizácia informačných systémov verejnej správy

- kritické (ich poškodenie má negatívny dosah na iné IS, resp. na KIIŠ, eKII)
- prevádzkové (základná úroveň ochrany, zvýšené požiadavky na bezpečnosť),

povinnosti povinných osôb (bezpečnostný projekt / politika, integrita, dôvernosť,

informácie: limitované, verejné, interne prístupné, kategorizácia informácií a IS,.....)

Bezpečnosť elektronickej verejnej správy

komunikácia medzi el. službami a registrami VS
minimálne bezpečnostné opatrenia pre základné prístupové komponenty
autentifikácia, identifikácia, EP / ZEP
audit a kontrola
cezhraničné a medzisektorové elektronické interakcie medzi EÚ inštitúciami VS

Ministerstvo financií
Slovenskej republiky

EFQM

Návrh zákona o elektronizácii administratívnych procesov

1. Legislatívny zámer zákona

(uznesenie vlády SR č. 657/2010 zo dňa 29. septembra 2010)

2. Predpokladaný časový harmonogram legislatívneho procesu

–	MPK	23. 9. 2011 – 13. 10. 2011
➢	Pracovné stretnutia	12. 9. 2011 – 20. 10. 2011
➢	Zapracovanie MPK	14. 10. 2011 – 15. 12. 2011
–	Legislatívna rada vlády	?
–	Parlament	?
–	predpokladaná účinnosť	rok 2012 ?

3. Návrh § - ého znenia

Ministerstvo financií
Slovenskej republiky

EFQM

Predmet úpravy návrhu zákona

- Všetky ISVS, vrátane obrany, utajovaných skutočností a medzinárodných zmlúv pokiaľ osobitný predpis neustanoví inak,
- Spôsob komunikácie a základné pravidlá prepojiteľnosti – interoperabilita,
- Služby a správa elektronických osobných schránok,
- Základné registre a univerzálny register,
- Identifikátory právnických a fyzických osôb a ich použitie,
- Referenčné údaje a narábanie s nimi,
- Podmienky zaobchádzania s elektronickými dokumentmi,
- Podmienky konverzie elektronických dokumentov (obojsmerne).

Ministerstvo financií
Slovenskej republiky

EFQM

Štruktúra návrhu zákona - 1

1. Vymedzenie základných pojmov a definície
2. Referenčné údaje a základné registre
3. Zaobchádzanie s referenčnými údajmi
4. Spoločné moduly - sú samostatnými ISVS
5. Správca základného registra
6. Správca identifikátorov
7. Správca transakcií
8. Univerzálny základný register
9. Identifikátor fyzickej osoby (základný, sektorový, iný)
10. Použitie identifikátorov
11. Register rozhodnutí
12. Prístup k údajom a notifikácia
13. Elektronické služby verejnej správy
14. Elektronické osobná schránka (fyzická osoba, právnická osoba)

Štruktúra návrhu zákona - 2

15. Aktivácia elektronickej osobnej schránky
16. Prístupové údaje, deaktivácia a zrušenie el. osobnej schránky
17. Služby poskytované elektronickou osobnou schránkou
18. Identifikácia používateľa elektronickej osobnej schránky
19. Elektronické podanie
20. Elektronické rozhodnutie
21. Elektronické doručovanie
22. Doručovanie prostredníctvom elektronickej osobnej schránky
23. Vykonávanie úkonov prostredníctvom elektronickej osobnej schránky
24. Úradný záznam
25. Konverzia dokumentu
26. Právne aspekty konvertovaných dokumentov
27. Zodpovednosť za škodu

Ministerstvo financií
Slovenskej republiky

EFQM

Reálne riziká ohrozujúce dosiahnutie vytýčených cieľov (8):

- ! Nevyhovujúci existujúci právny rámec, ktorý ako celok, bude bariérou v rozvoji eGovernmentu, napr. nepodarí sa prijať zákon o informačnej bezpečnosti, sfunkčniť vytvorenú jednotku CSIRT.SK,
- ! Budú naďalej zotrvávať prekrývania sa kompetencií v oblasti koordinácie informačnej bezpečnosti, resp. sa bude účelovo a neodborne zasahovať do tvorby kľúčových zákonov a do kompetencií, vrátane vydávania štandardov,
- ! Riziko, že do riešení nebude v primeranom čase a rozsahu zakomponované hľadisko európskej interoperability,
- ! Reálna hrozba nevyčerpania finančných prostriedkov vyčlenených na informatizáciu verejnej správy v rámci OPIS a zo štátneho rozpočtu,
- ! Finančné prostriedky nebudú efektívne využité a tým postačujúce pre uskutočnenie všetkých potrebných projektov,
- ! Financovanie IKT nebude v súlade s aktuálnym procesom tvorby štátneho rozpočtu,
- ! Prejavia sa nedostatočné odborné kapacity zainteresovaných subjektov pri zabezpečovaní koordinácie, programového a projektového manažmentu pre prierezové projekty,
- ! Do procesu informatizácie VS sa nepodarí úspešne zahrnúť územnú samosprávu a ďalšie možno ich nazvať aj neočakávané riziká.

Ministerstvo financií
Slovenskej republiky

EFQM

Ďakujem za pozornosť

Jan Hochmann
Ministerstvo financií SR