# *Štandardizácia v SR a bezpečnosť*

Peter Bíro

Ministerstvo financií
Slovenskej republiky

**MF SR, BA, júl 2009**

# Strategické dokumenty v oblasti inf.bezpečnosti

- Národná stratégia pre informačnú bezpečnosť SR (schválená 27. 8. 2008)
- Systém vzdelávania v oblasti IB (schválený 27. mája 2009)
- Vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov CSIRT.SK (schválený 1. júla 2009)
- Zákon o informačnej bezpečnosti (MF SR)
  - zámer zákona do konca 2009
- Zákon o kritickej infraštruktúre (MV SR)
- Zákon o ochrane utaj.informácií a ochrane kyber. priestoru (NBÚ)
- Bezpečnostné štandardy (legislatíva)
  - účinné od 1. augusta 2006, novelizované 1. októbra 2008

# Legislatíva v súvislosti so štandardizáciou IB

- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
  - účinný od 1. júna 2006
  - § 6 –Štandardom je súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných systémov verejnej správy, ktorý obsahuje charakteristiky, metódy, postupy a podmienky, najmä pokiaľ ide o bezpečnosť a integrovateľnosť s inými informačnými systémami.
  - **§ 13** - kompetencia MF SR vydávať štandardy
- Výnos MF o štandardoch pre ISVS (novela účinná od 1.10.2008)
- Metodický pokyn k výnosu o štandardoch pre ISVS
- Metodický pokyn pre hodnotenie bezpečnostných štandardov (jún 2009)
  - Ďalšie metodické pokyny – dátové štandardy, terminológia (pripravuje sa aktualizácia, ktorá bude obsahovať aj
- Novela zákona po Legislatívnej rade Vlády SR

# Koordinácia štandardizácie IB

- Ministerstvo financií SR (od 1.2.2007, predtým MDPT SR)
  - Kompetenčný zákon – MF SR ako gestor informatizácie spoločnosti, ktorá zahŕňa aj informačnú bezpečnosť pre neutajované skutočnosti
  - Zákon o ISVS - Právomoc stanovovať a vydávať štandardy
  - Kontrolný orgán
  - Na starosti má: Sekcia informatizácie spoločnosti – Odbor legislatívy, metodiky, štandardov a bezpečnosti SR
- Komisia pre štandardizáciu IS VS pri MF SR
  - Zastúpenie rezortov, súkromnej aj akademickej sféry
  - Pracovné skupiny pre jednotlivé oblasti štandardizácie (pre bezp. štandardy Komisia pre informačnú bezpečnosť)
- Komunikácia:
  - web: www.informatizacia.sk (menu: eGovernment/Štandardy pre IS VS)
  - e-mail: standard@mfsr.sk

# Koordinácia štandardizácie IB

- Ďalšie oblasti tvorby špecifickej štandardizácie, ktorá sa môže dotýkať aj bezpečnosti:
  - Zdravotníctvo (MZ SR – NCZI)
  - Priestorové informácie (ÚGKK SR)
  - Elektronický podpis (NBÚ SR)
  - Kybernetický priestor?? (NBÚ SR)

# Štandardizácia - úvod

- Životný cyklus štandardov:
  1. Odporúčaný (príloha metodického pokynu)
  2. Povinný (výnos)
  3. Zrušený (príloha metodického pokynu)
- Schvaľovací procesov vydávania štandardov
  1. Príslušná PS
  2. Komisia pre štandardizáciu IS VS
  3. VPK MF SR
  4. MPK
  5. Technická komisia pri Legislatívnej rade Vlády SR

# Základné oblasti štandardizácie

1. Skupina - vydané
   - Technické štandardy (pre prepojenie, pre prístup k elektronickým službám, pre webové služby, pre integráciu dát)
   - Štandardy prístupnosti a funkčnosti webových stránok
   - Štandardy použitia súborov
   - Štandardy názvoslovia elektronických služieb
   - **Bezpečnostné štandardy** (štandardy pre architektúru riadenia, štandardy minimálneho technického zabezpečenia)
   - Dátové štandardy

# Základné oblasti štandardizácie

2. Skupina - pripravované

- Štandardy pre elektronické formuláre (t.j. formuláre elektronickej verejnej správy)
- Štandardy pre priestorovú identifikáciu
- Štandardy pre projektové riadenie
- Terminologické štandardy v oblasti informatizácie spoločnosti
- Štandardizované číselníky (čiastočne vydané)

3. Skupina – zatiaľ nezačaté prípravné procesy

- Štandardy pre metadáta

# Všeobecné princípy kontroly informačnej bezpečnosti

- Informácie o bezpečnosti IKT, architektúra, softvér, OS, aplikácie sú citlivé informácie – ich znalosť = útočník má 50% cesty za sebou (využitie známych chýb)
- Kontrolór samotný musí vždy dodržiavať pravidlá informačnej bezpečnosti, konať v rámci právnych predpisov a tak, aby neohrozil kontrolovaný subjekt
- Kontrolór by mal dodržiavať bezpečnostnú politiku kontrolovaného subjektu, tá však nesmie obmedzovať výkon kontroly
- Cieľom kontroly je obojstranná snaha o dosiahnutie požadovaného stavu a nie dokazovanie pocitu nadradenosti
- Súčasné kompetencie:
  - Bezpečnostné štandardy pre IS VS kontroluje MF SR (túto právomoc nemôže „outsourcovať")
  - NBÚ kontroluje požiadavky pre utajované skutočnosti
  - ÚOOÚ kontroluje ochranu osobných údajov
  - NKÚ SR kontroluje záležitosti, súvisiace s financiami a majetkom, nie však IKT a bezpečnosť ako takú

# Princípy správnej implementácie bezp. štandardov

- Všeobecné princípy:
  - Zmluvy, zmluvy, zmluvy! - dodávatelia majú dodržiavať platnú legislatívu, odporúča sa explicitne uvádzať samotný zákon 275/2006, prípadne platný výnos o štandardoch
  - Čítanie metodík
  - Komunikácia s kontrolným orgánom (MF SR) – standard@mfsr.sk a s ostatnými povinnými či inými osobami navzájom
  - Zdravý rozum – informácie a služby sú poskytované pre ľudí a to spôsobom, aby sa k nim dostali, pochopili ich a použili a nie iba preto, lebo „tak je písané"
  - Kritériá hodnotenia dodržiavania štandardov zohľadňujú istú mieru tolerancie
- Cieľom nie je rozdávať pokuty, ale zabezpečiť, aby boli štandardy skutočne implementované.