Implementácia Bezpečnostnej politiky IS v rezorte kultúry Slovenskej republiky

RNDr. Anna Levčíková, odbor informatizácie MK SR
Mgr. Ivan Kopáčik, Gordias, s.r.o.

Národná konferencia o digitalizácii
Senec 16.6. – 17.6.2009

Požiadavky na informačnú bezpečnosť

Koncepčne a metodicky vychádzajú úlohy na zaistenie bezpečnosti IS rezortu kultúry :

- zo zákona NR SR č. 275/2006 Z.z. o IS VS v znení neskorších predpisov,

V zmysle § 3 ods. 2) písm. b) a písm. c) tohto zákona povinné osoby :

– zabezpečujú plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy,

–zodpovedajú za zabezpečenie informačného systému proti zneužitiu.

V zmysle § 3 ods.3) písm. a) správca IS VS :

- je povinný zabezpečiť, aby IS VS vyhovoval štandardom

- z Výnosu Ministerstva financií Slovenskej republiky z 8. Septembra 2008 č. F/013261/2008-132 o štandardoch pre IS VS: bezpečnostné štandardy § 27 - § 41

- z Národnej stratégie pre informačnú bezpečnosť v SR, ktorá bola schválená uznesením vlády SR č.570/2008 dňa 27.8.2008

Bezpečnostná politika

Bezpečnostná politika IS rezortu MK SR

- bola schválená Poradou vedenia MK SR 15.7.2008
- vymedzuje komplexný systém riadenia a podpory informačnej bezpečnosti podľa platných bezpečnostných štandardov
- riadenie informačnej bezpečnosti je rozpracované podľa 11-ich oblasti riadenia, tak ako ich vymedzuje štandard STN ISO/IEC 17799:2005 (STN ISO/IEC 27002:2005)
- vzťahuje na všetky aktíva tvoriace IS rezortu MK SR, t.j. všetky IS na MK SR a IS organizácií v zriaďovacej pôsobnosti MK SR a ich súčasti (tzn. fyzické komponenty, softvér, údaje , ľudské zdroje a nehmotné aktíva : služby a dobré meno) s výnimkou aktív spadajúcich pod zákon o ochrane UTS.

Bezpečnostná politika

Hlavným cieľom bezpečnostnej politiky pre informačné systémy je zavedenie jednotných postupov a pravidiel na systematické a kontinuálne riešenie bezpečnosti a ich trvalú podporu v celom rezorte kultúry, t.j. na MK SR a v organizáciách v jeho zriaďovacej pôsobnosti.

Súčasťou úloh na úseku informačnej bezpečnosti sú aj úlohy vyplývajúce zo zákona o ochrane osobných údajov.

Úlohy na úseku informačnej bezpečnosti sa zabezpečujú v gescii odboru informatizácie MK SR so spol. GORDIAS s.r.o. , ako odborným garantom procesu.

Implementácia bezpečnostnej politiky

Proces implementácie bol rozvrhnutý na obdobie rokov 2008-2010

- Rok 2008 : Organizácia bezpečnosti, Klasifikácia a riadenie aktív, Nákup, vývoj a údržba systémov
- Rok 2009 : Personálna bezpečnosť, Riadenie komunikácií a prevádzky, Riadenie prístupov, Riadenie bezpečnostných incidentov
- Rok 2010 : Riadenie kontinuity procesov závislých na IKT, Súlad s platnou právnou úpravou, Fyzická bezpečnosť a bezpečnosť prostredia, Politika informačnej bezpečnosti (revízia)

Súčasťou realizovaných opatrení je aj odborná príprava zamestnancov organizácií rezortu zodpovedných za oblasť IB (školenia, workshopy)

Implementované oblasti riadenia

Organizácia a riadenie IB

Vydaný záväzný interný právny predpis (riadiaci akt) :

Metodický MP pre organizáciu a riadenie informačnej bezpečnosti zo dňa 15. 4. 2009, ktorý upravuje systém organizácie a riadenia informačnej bezpečnosti MK SR a organizácií v jeho zriaďovacej pôsobnosti

Cieľom je

-zadefinovať a následne zriadiť kľúčové role vyplývajúce z bezpečnostnej politiky (bezpečnostný manažér, bezpečnostní správcovia),

-ustanoviť pravidlá pre prístup tretích strán k informačným systémom rezortu kultúry,

-zaviesť systém riadenia (plánovanie – tvorba bezpečnostných plánov t.j. navrhovanie bezpečnostných opatrení, ich realizácia, monitorovanie a kontrola, udržiavanie a zlepšovanie)

Implementované oblasti riadenia

Nákup, vývoj a údržba IS

Vydaný záväzný interný právny predpis (riadiaci akt) :

Metodický pokyn pre nákup, vývoj a údržbu IS zo dňa 15. 2. 2009, ktorý upravuje bezpečnostné zásady a požiadavky pre nákup, vývoj a údržbu IS

Cieľom je zabezpečiť napĺňanie požiadaviek na informačnú bezpečnosť vo všetkých fázach životného cyklu IT projektu t.j.

- príprava (verejné obstarávanie, zmluvy)
- analýza a špecifikácia požiadaviek na bezpečnostné funkcie)
- vývoj a dodávka
- testovanie a akceptačné konanie
- zavedenie do produkčnej prevádzky a dokumentácie
- riadenie zmien a podpora

Implementované oblasti riadenia

Klasifikácia a riadenie aktív IS

Vydaný záväzný interný právny predpis (riadiaci akt) :

Metodický pokyn pre klasifikáciu a riadenie aktív IS zo dňa 20. 2. 2009, ktorý upravuje pravidlá, resp. bezpečnostné zásady a požiadavky pre evidenciu a klasifikáciu aktív

Cieľom je

- Zavedenie jednotných postupov na evidenciu aktív a priradenie zodpovednosti za aktíva (zariadenia IKT, záznamové média, APV, agendy a elektronické informácie spracovávané organizáciou)
- Zavedenie systému klasifikácie aktív a pravidiel na označovania aktív
- Zavedenie nástrojov na podporu riadenia aktív

ROZPRACOVANÉ OBLASTI RIADENIA

1. Riadenie incidentov informačnej bezpečnosti
2. Analýza a riadenie rizík

Ďalšie aktuálne úlohy

Zabezpečovanie súladu s platným výnosom MF SR a s internou legislatívou v oblasti informačnej bezpečnosti pre všetky nové projekty (ORES, DMS a BPM)

Súčinnosť s MF SR

MF SR ako ústredný orgán štátnej správy pre informatizáciu spoločnosti vykonal dňa 4.6.2009 na MK SR kontrolu dodržiavania bezpečnostných štandardov

POSTUP V ROKU 2009

- Zvládanie bezpečnostných incidentov, personálna bezpečnosť, riadenie prístupov do IS, riadenie komunikácií a prevádzky IS
  - Školenia k implementovaným oblastiam bezpečnosti (pre špecialistov z MK SR a organizácií v zriaďovateľskej pôsobnosti MK SR ako aj pre riadiacich pracovníkov MK SR a organizácií rezortu MK SR)
  - Vypracovanie riadiacej dokumentácie k implementovaným oblastiam bezpečnosti
  - Reakcie na zmeny legislatívy (pripravovaná novela zákona o ISVS)

VZŤAH K DIGITALIZÁCII

Výnos MF SR č. MF/013261/2008-132 o štandardoch pre IS VS

Bezpečnostná politika IS rezortu MK SR

MP MK SR pre nákup, vývoj a údržbu IS

MP MK SR pre klasifikáciu a riadenie aktív IS

MP MK SR pre organizáciu a riadenie bezpečnosti IS

.....

Metodický manuál pre zabezpečenie informačnej bezpečnosti

HIERARCHIA

- Bezpečnostné štandardy Výnosu o štandardoch ISVS – univerzálne platné pre ISVS /všeobecné (rámcové požiadavky)
- Bezpečnostná politika IS rezortu MK SR + súvisiace metodické pokyny –zohľadňuje špecifiká rezortu MK SR
- Metodický manuál pre zabezpečenie informačnej bezpečnosti – špecifický pre projekty OPIS2/digitalizáciu

CIELE MANUÁLU

Metodický manuál pre zabezpečenie informačnej bezpečnosti:

- Čiastkové bezpečnostné ciele a spôsoby ich napĺňania v kontexte digitalizácie
- Mechanizmy určovania a napĺňania bezpečnostných požiadaviek v kontexte digitalizácie

CIELE MANUÁLU II.

Metodický manuál pre zabezpečenie informačnej bezpečnosti:

- Interpretácia (konkretizácia) požiadaviek vyplývajúcich z praxe a vyšších právnych noriem
- Rozpracovanie relevantných okruhov všetkých 11-tich oblastí informačnej bezpečnosti
- Spôsob dosahovania súladu (s bezpečnostnými štandardami, metodickými pokynmi rezortu kultúry a všeobecne záväznými predpismi)

PRÍKLADY

- **Koncepcia bezpečnosti a bezpečnostná architektúra v procese vývoja/dodávky IS a jeho služieb**
- **Riadenie komunikácií a prevádzky**
  - **Prevádzkové postupy a zodpovednosti**
  - **Riadenie dodávok tretích strán**
  - **Ochrana pred škodlivými programami a mobilnými kódmi**
  - **Zálohovanie/archivácia**
  - **Riadenie sieťovej bezpečnosti**
  - **Bezpečnosť pri narábaní s médiami**
- **Požiadavky na riadenie prístupu**
- **Riadenie kontinuity činností digitalizácie**
- **Zvládanie bezpečnostných incidentov v procese digitalizácie**
  - **Hlásenie bezpečnostných udalostí a slabín**
  - **Zvládanie bezpečnostných incidentov a kroky k náprave**
- **Analýza a riadenie rizík vo vzťahu k aktívam IKT a DO**

Ďakujeme za pozornosť

Nech sa páči, otázky ....