Audit informačnej bezpečnosti a ochrany osobných údajov DO SR

- **Pavel Mozoľa**
  Daňové riaditeľstvo Slovenskej republiky
- **Slavomír Vričan, CISA**
  ESET, spol. s r.o.

ESET

Daňové riaditeľstvo Slovenskej republiky

Motivácia auditu

- Audit je súčasť kontrolného mechanizmu požadovaného legislatívou
- Uskutočňovať pravidelný audit nezávislým a odborne spôsobilým audítorom vyžaduje vnútorná bezpečnostná politika
- Očakávame, že takýto audit nám poskytne kvalifikované odpovede na otázky typu:
  - ✓ Do akej miery sme v súlade s legislatívnymi požiadavkami?
  - ✓ Aká je úroveň súladu s medzinárodne uznávanou dobrou praxou riadenia informačnej bezpečnosti?
  - ✓ Je organizácia informačnej bezpečnosti primeraná a sú jej požiadavky dostatočne podporované našim vedením?
  - ✓ Sme si vedomí všetkých podstatných rizík a riadime ich systematicky a účinne?

Motivácia auditu

- ✓ Pokrývajú vnútorné smernice všetky významné oblasti?
- ✓ Sú vnútorné pravidlá formulované účelne, v súlade s legislatívou a dobrou praxou?
- ✓ Sú si zamestnanci vedomí požiadaviek, akceptujú ich ako zmysluplné a správajú sa podľa nich?
- ✓ Došlo k zlepšeniu riadenia informačnej bezpečnosti od posledného auditu?
- ✓ V ktorých oblastiach sme dobrí a kde sa potrebujeme zlepšiť?
- ✓ Čo a s akými prioritami potrebujeme urobiť, aby sme zlepšili plnenie bezpečnostých požiadaviek?
- ✓ Ako môžeme vyhodnocovať vývoj situácie v jednotlivých oblastiach?

Ciele auditu

- Overiť úroveň:
  - ✓ dodržiavania vnútorných bezpečnostných politík a smerníc
  - ✓ súladu so zákonom č. 276/2006 o informačných systémoch verejnej správy a s Výnosom MF SR o štandardoch pre ISVS
  - ✓ súladu s požiadavkami normy ISO/IEC 27002
  - ✓ súladu s požiadavkami zákona č. 428/2002 o ochrane osobných údajov
- Navrhnúť opatrenia na odstránenie zistených nedostatkov

Výber audítora

- Výber audítora prebiehal formou verejného obstarávania
- ESET ponúkol auditný tím, kde každý člen je držiteľom aspoň jedného odborného certifikátu
  - ✓ CISA
  - ✓ CISM
  - ✓ CISSP

Rozsah auditu

Čas:

- Výber: marec 2011
- Príprava: apríl 2011
- Výkon: máj – júl 2011
- Dodanie výstupov: august 2011
- Spolu: 6 mesiacov

Auditované lokality:

- Daňové riaditeľstvo
- Dva daňové úrady
- Jedno pracovisko Daňového riaditeľstva
- Daňová škola

Systémy:

- Centrálny daňový informačný systém
- Systém vnútornej správy
- eTax
- Data warehouse
- Elektronická pošta
- Zálohovací systém
- Systém riadenia zmien
- Vzorka pracovných staníc

Priebeh auditu 1/3

Na požiadanie auditora sme predložili cca 1050 strán dokumentácie väčšinou v elektronickej forme

- Organizačná štruktúra
- Organizačný poriadok
- Bezpečnostná politika
- Bezpečnostné smernice
- Prevádzkové postupy
- Havarijné plány
- Obsah školení zamestnancov
- Výsledky predchádzajúccich auditov a kontrol
- Vzorka bezpečnostne relevantných častí zmlúv s dodávateľmi

Priebeh auditu 2/3

- Auditor realizoval fyzické obhliadky objektov zahrnutých do auditu
- Overil úroveň fyzickej bezpečnosti serverovní, technologických a telekomunikačných miestností
- Uskutočnil rozhovory s 50 zamestnancami z útvarov:

✓Bezpečnosť
✓Prevádzka IT
✓Vývoj IT
✓Riadenie projektov
✓Všeobecná správa

✓ Správa a výber daní
✓ Personalistika
✓ Obstarávanie
✓ Právne služby
✓ Vnútorná kontrola

Priebeh auditu 3/3

Auditor realizoval technické testy na vzorke 60 zariadení a 6 pracovných staníc

Cieľ:

Identifikovať nedostatky v oblasti riadenia bezpečnosti a vo vybraných procesoch prevádzky IT

Prostriedky:

- Zber a analýza systémových, databázových a aplikačných záznamov
- Zber a analýza bezpečnostne relevantných konfiguračných nastavení
- Skenovanie sieťových služieb a ohodnotenie zraniteľností

Metodika auditu 1/2

- Audit hodnotil plnenie každej požiadavky normy, zákona alebo vnútorného predpisu zvlášť a na záver vykonal ohodnotenie jednotlivých oblastí
- Hodnotenie bolo založené na škále, odrážajúcej stupeň vyspelosti nasadenia požadovaných opatrení:

0 – Požiadavkou sa nik nezaoberá

1 – Ad hoc prístup na základe aktivity jednotlivcov

2 – Opatrenie je formalizované ale neuplatňuje sa v praxi, alebo vice versa

3 – Opatrenie je formalizované a uplatňuje sa v praxi, ale nie je kontinuálne zlepšované (použitím metrík)

4 – Opatrenie je formalizované, uplatňuje sa v praxi a je tiež kontinuálne zlepšované

Metodika auditu 2/2

Použitá metodika umožnila získať prehľad o úrovniach vyspelosti informačnej bezpečnosti v jednotlivých oblastiach

Zobrazený graf je len ilustratívny a neznázorňuje hodnoty získané počas auditu DR SR

Výstupy auditu 1/2

Detailná auditná správa

- Opis používaných postupov a nasadených opatrení v auditovaných oblastiach
- Formulácia všetkých zistení s odkazom na príslušnú požiadavku normy, zákona alebo interného predpisu
- Závažnosť jednotlivých zistení a jej odôvodnenie
  - ✓ Vysoká – systémové nedostatky v kľúčových procesoch
  - ✓ Stredná – systémové nedostatky v podporných procesoch
  - ✓ Nízka – lokálne nedostatky v podporných procesoch
- Formulácia odporúčaní na odstránenie nedostatkov

Výstupy auditu 2/2

Zhrnutie pre manažment

- Celková charakteristika úrovne informačnej bezpečnosti
- Stručné zhodnotenie stavu v auditovaných oblastiach
- Zistenia vysokej a strednej závažnosti
- Navrhované odporúčania
- Grafické znázornenie stupňov vyspelosti nasadenia požadovaných opatrení podľa oblastí:
  - ✓ systému riadenia informačnej bezpečnosti ISO/IEC 27002
  - ✓ bezpečnostných štandardov výnosu MF SR

Hodnotenie auditu

- Z výsledkov auditu vyplynulo, že DR SR:
  - ✓ dosiahlo v minulých rokoch výrazný pokrok v presadzovaní požiadaviek informačnej bezpečnosti
  - ✓ má vypracovaný vyspelý organizačný a dokumentačný rámec pre riadenie informačnej bezpečnosti
- Audit pomenoval oblasti, ktoré je potrebné zlepšiť, aby sa zvýšila efektívnosť riadenia informačnej bezpečnosti
- Audit poskytol hodnotenie úrovne vyspelosti nasadenia jednotlivých bezpečnostných požiadaviek
- Popri odporúčaniach na zlepšenie procesov riadenia informačnej bezpečnosti sa audit venoval aj bezpečnostnej konfigurácii vybraných informačných systémov

Čo ďalej s výsledkami auditu?

- Motivácia pre spresnenie
  - ✓ metodiky analýzy a ohodnocovania rizík
  - ✓ riadenia aktív
  - ✓ klasifikácie informácií
- Vstupy do plánu bezpečnosti pre rok 2012
- Podpora pre rozhodovanie manažmentu v oblasti rozvoja informačnej bezpečnosti
- Jedno z východísk pre definovanie bezpečnostných požiadaviek pre informačné systémy a procesy v projekte zjednotenia daňovej a colnej správy

Priestor pre vaše otázky