Bezpečnostný projekt

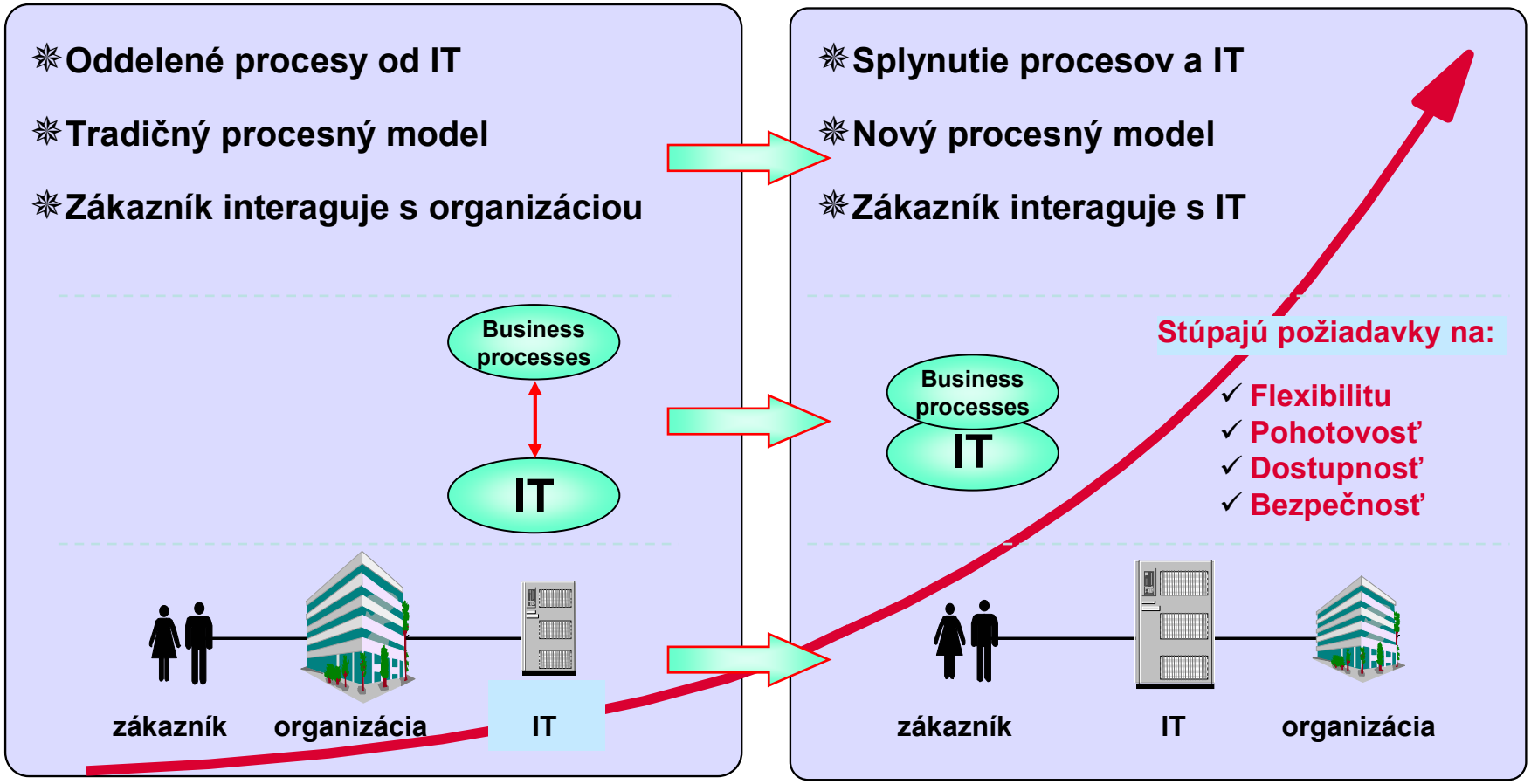
Ing. Samuel Kušnierik
IBM Slovensko, spol. s r.o.

ITAPA,
Bratislava, 27. október 2003

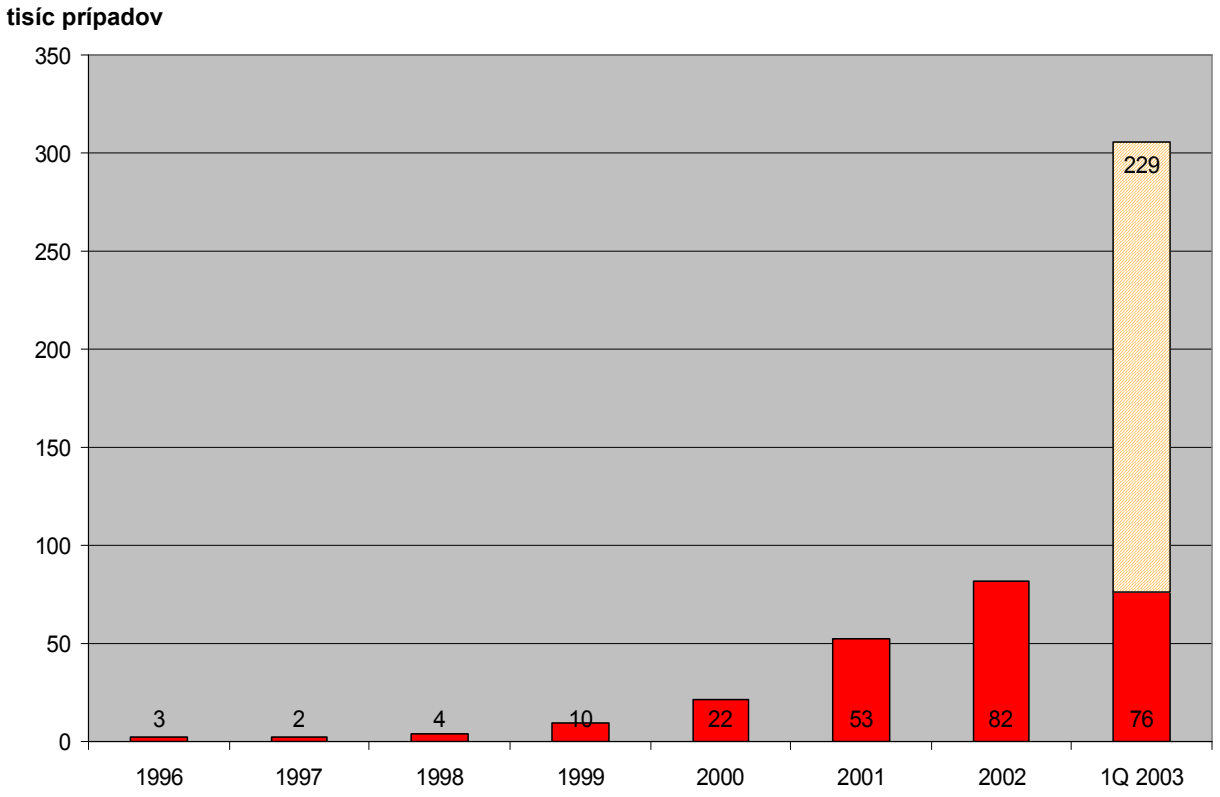
Agenda

- Identifikácia relevantných zákonných noriem
- Typy legislatívneho prístupu k bezpečnostným projektom
- Úlohy orgánov a zamestnancov verejnej správy pri riešení bezpečnostných projektov

Vývoj modelu spracovania

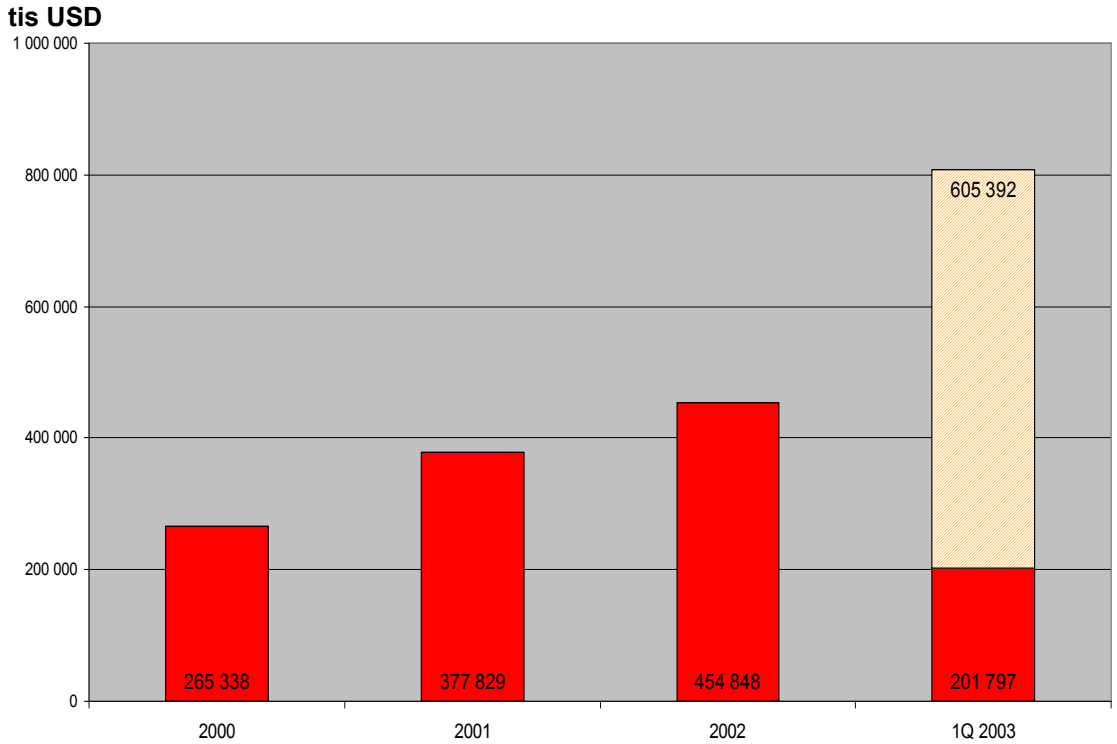


Počet hlásených bezpečnostných incidentov



Zdroj: ***www.cert.org/stats/cert_ststs.html***

Škody spôsobené bezpečnostnými incidentmi



Zdroj: CSI/FBI Computer Crime and Security Survey

Bezpečnosť IT ako otázka prežitia

Bezpečnostný incident naruší

- Procesy
- Vzťahy
- Vedomosti
- Schopnosť konať

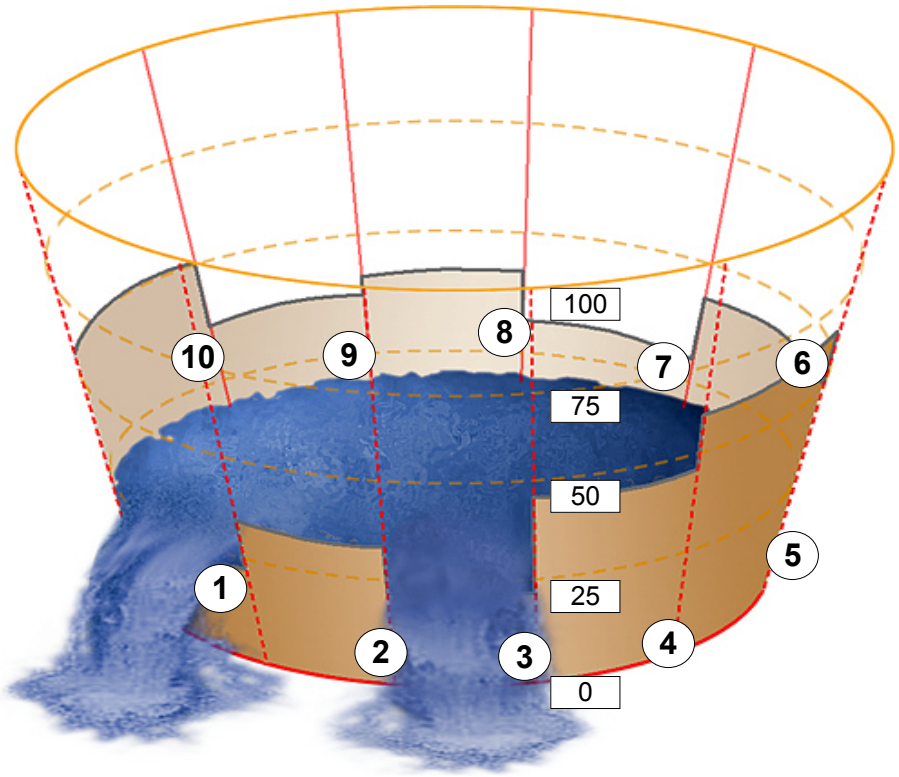
Ohrozí

- Plnenie úloh
- Činnosť

Ochrana sa stáva otázkou bytia alebo nebytia

Zložky riešenia bezpečnosti

1. Bezpečnostné zásady (bezpečnostná politika)
2. Organizačná bezpečnosť
3. Klasifikácia a riadenie aktív
4. Personálna bezpečnosť
5. Fyzická bezpečnosť
6. Komunikačná a prevádzková bezpečnosť
7. Riadenie prístupu
8. Vývoj a údržba systémov
9. Kontinuita procesov
10. Zhoda



Projekt riešenia bezpečnosti

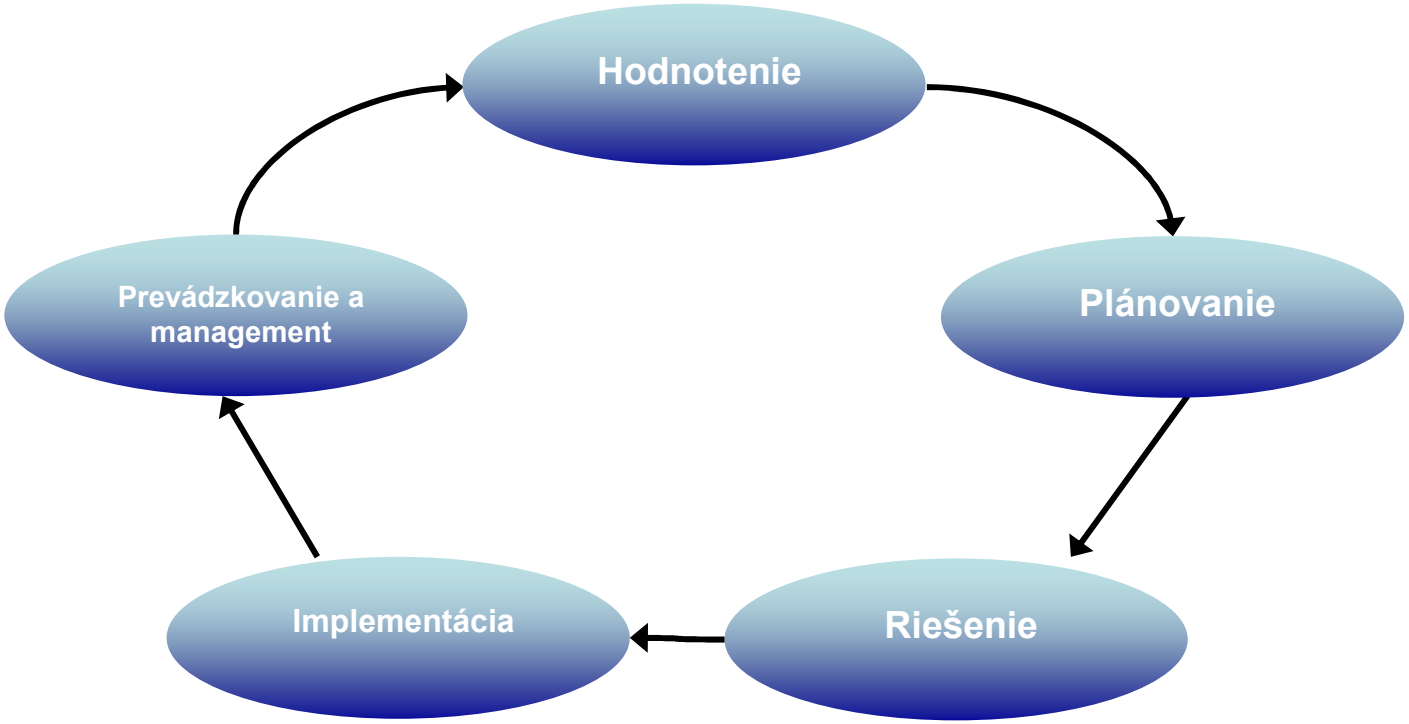
- Vymedzenie rozsahu projektu (bezpečnostnej hranice)
- Identifikácia chránených aktív
- Vyhodnotenie súčasného stavu bezpečnosti
- Definícia základných požiadaviek na ochranu
- Definícia zásad bezpečnosti (politiky
- Analýza bezpečnostných rizík
- Návrh protiopatrení na obmedzenie vplyvu rizík
- Návrh bezpečnostných štandardov
- Návrh bezpečnostnej infraštruktúry

  Smernice, procedúry, organizácia, manažment bezpečnosti, riešenie kontinuity a zotavenia
- Riešenie bezpečnostnej architektúry

  bezpečnostné služby, mechanizmy komponenty, riadenie bezpečnosti, monitoring
- Audit bezpečnosti

Systém bezpečnosti

Životný cyklus bezpečnosti



Reflexia úlohy bezpečnosti IT v legislatíve SR

- Zákon 241 / 2001 o ochrane utajovaných skutočností
- Vyhláška NBÚ 90 / 2002 o bezpečnosti technických prostriedkov
- Vyhláška NBÚ 91 / 2002 ktorou sa stanovujú podrobnosti o šifrovej ochrane informácií
- Vyhláška NBÚ 88 / 2002 o fyzickej bezpečnosti a o objektovej bezpečnosti
- Zákon 417 / 2002 o používaní deoxyribonukleovej kyseliny na identifikáciu osôb
- Zákon 428 / 2002 o ochrane osobných údajov
- Zákon 215 / 2002 o elektronickom podpise
- Vyhláška NBÚ 541 / 2002 o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách na výkon certifikačných činností
- Vyhláška NBÚ 542 / 2002 o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku

Požiadavky zákona 241 / 2001 Z.z. o ochrane utajovaných skutočností

§ 54 Bezpečnostný projekt na technické prostriedky

- Definuje

  Rozsah a spôsob použitia TP a prostriedky a metódy ochrany utajovaných skutočností

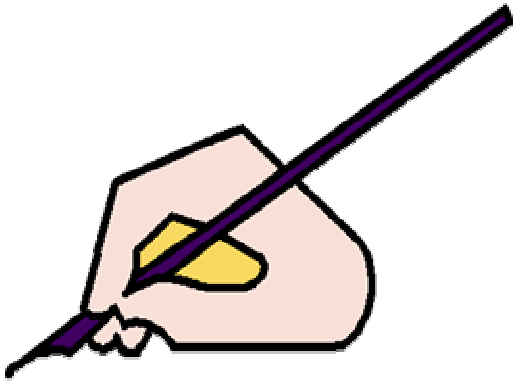
- Obsahuje
  - Bezpečnostný zámer
  - Opis chránených TP
  - Analýzu ochrany utaj. Skutočností
  - Štandardy, metódy a prostriedky ochrany
  - Protiopatrenia
  - Špecifikáciu hrozieb zabezpečených a nezabezpečených protiopatreniami

Normy súvisiace so zákonom 241 / 2001 Z.z.

Upresňujú podmienky na bezpečnostný projekt

- Vyhláška 90 / 2002 NBÚ o bezpečnosti technických prostriedkov
  - Certifikácia používanie a schvaľovanie technických prostriedkov
  - Bezpečnostné požiadavky na technické prostriedky
  - Bezpečnosť informačných systémov
- Vyhláška 91 / 2002 NBÚ ktorou sa stanovujú podrobnosti o šifrovej ochrane informácií
  - Certifkácia a schvaľovanie prostriedkov šifrovej ochrany pre jednotlivé stupne utajenia, evidencia a používanie šifrových materiálov
- Vyhláška 88 / 2002 NBÚ o fyzickej bezpečnosti a objektovej bezpečnosti
  - Špecifikácia budov a priestorov
  - Technické podmienky zabezpečenia budov fyzickou ochranou

Požiadavky zákona 215 / 2002 Z.z. o elektronickom podpise



Zákon 215 / 2002 Z.z. požaduje pre:

- CA – vypracovanie a dodržiavanie bezpečnostných pravidiel (§ 14.(1)a))
- akreditovanú CA – preukázanie spoľahlivosti nevyhnutnej na poskytovanie služieb (§ 14.(3)a))
- Produkt pre elektronický podpis - (§ 24)
  - Bezpečné zariadenia na vyhotovovanie elektronických podpisov
- Ukladá povinnosť bezpečnostného auditu pre akreditovanú CA

Vyhláška NBÚ 541 / 2002 Z.z.

o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a na výkon certifikačných činností

- § 9 (1) Bezpečnostné pravidlá akreditovanej certifikačnej autority obsahujú:

  bezpečnostnú politiku, bezpečnostný zámer, bezpečnostný projekt, havarijný plán, bezpečnostné smernice

- § 10 Bezpečnostná politika

  základné požiadavky na ochranu a záväzky

- § 11 Bezpečnostný zámer

  požiadavky na ochranu informácií

- § 12 Bezpečnostný projekt

  analýza rizík, popis rizík, popis opatrení na obmedzenie rizík,popis nasadenia , využívania a kontroly bezpečnostných opatrení

- § 13 Havarijný plán

  postupy pri mimoriadnych udalostiach, plán obnovy

Vyhláška NBÚ č 542 / 2002 Z.z.

o spôsobe a postupe používanie elektronického podpisu v obchodnom a administratívnom styku

- § 6 (1) Ak orgán verejnej moci, alebo verejnej správy využíva zaručený elektronický podpis, zriaďuje elektronickú podateľňu...

- § 6 (6) Na prevádzku elektronickej podateľne a jej technických prostriedkov musí byť schválený a spracovaný bezpečnostný projekt a bezpečnostné smernice zodpovedajúci najmenej stupňu „V“

Požiadavky zákona 428 / 2002 Z.z. o ochrane osobných údajov

- § 13 (1) Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ a sprostredkovateľ tým, že ich chráni pred odcudzením, stratou, poškodením,neoprávneným prístupom, zmenou a rozširovaním.

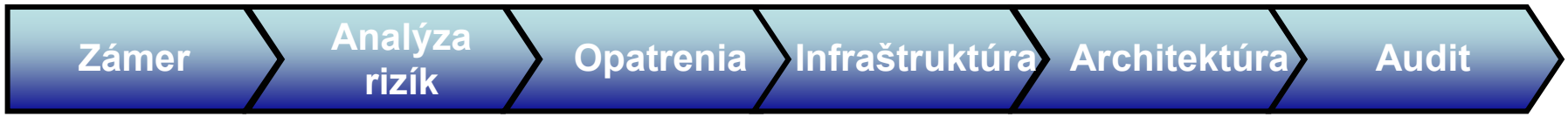
- § 13 (2) Opatrenia príjme vo forme bezpečnostného projektu ak

  Informačný systém je prepojený na verejne prístupnú počítačovú sieť, alebo ak IS spracováva osobitné kategórie osobných údajov (§8), alebo podlieha výnimkám podľa §2.

- § 16 Bezpečnostný projekt obsahuje:

  bezpečnostný zámer, analýzu bezpečnosti, bezpečnostné smernice

Bezpečnostný projekt v požiadavkách legislatívy



Spoločné:

- Idea riešenia bezpečnosti formou bezpečnostného projektu

Rozdielne:

- Požiadavky na technické podrobnosti riešenia projektu

Úlohy organizácií verejnej správy a verejnej moci

Zaistiť bezpečnosť IT systémov, tak a by IT systémy

- poskytovali spoľahlivú podporu procesom organizácií
- boli chránené pred vonkajším aj vnútorným ohrozením
- bezpečnosť zodpovedala podmienkam požiadavkám legislatívy SR a normám EU

Úlohy pracovníkov verejnej správy a verejnej moci

Vedúci pracovníci

- Evidovať stav bezpečnosti v organizácii a jeho zhodu s meniacimi sa podmienkami
- Iniciovať a podporovať bezpečnostné projekty na základe podnetov vyplývajúcich zo stavu bezpečnosti a reálnych bezpečnostných požiadaviek
- Sledovať dodržiavanie bezpečnostných pravidiel a riešiť ich porušenia

Radoví pracovníci

- Dodržiavať bezpečnostné pravidlá
- Vykonávať úlohy v súlade s predpísanými bezpečnostnými procedúrami
- Aktívne upozorňovať vedenie na prípadné slabinu v existujúcej bezpečnosti a na zmeny podmienok (zmeny v legislatíve, nové ohrozenia, objavené zraniteľnosti)
- Vykonávať zverené úlohy z oblasti bezpečnosti

Na záver

Legislatíva SR požaduje riešiť formou bezpečnostného projektu

- Ochranu utajovaných skutočností (technické prostriedky)
- Ochranu osobných údajov
- Bezpečnosť elektronických podateľní

Riešenie ochrany sa stáva povinnosťou

Riešenie bezpečnosti sa realizuje na základe jasne definovaných požiadaviek

Výsledky riešenia sú porovnateľné s očakávanými

Tento prístup znamená novú kvalitu v chápaní bezpečnosti zaručujúcu postupný prechod k stavu charakterizovanému neustálym zdokonaľovaním systému riadenia bezpečnosti

Ďakujem za pozornosť

samuel.kusnierik@sk.ibm.com