Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Úvod do informačnej bezpečnosti

Daniel Olejár

Máj 2013

KPMG
cutting through complexity™

Úvod (1)

- NR SR v roku 2011 schválila Zákon 45/2011 Z. z. o kritickej infraštruktúre
- Organizácie, v ktorých pracujete, sú prevádzkovateľmi prvkov kritickej infraštruktúry, patriacich do sektora Informačných a komunikačných technológií
- Zo zákona o kritickej infraštruktúre vyplýva pre prevádzkovateľa prvku kritickej infraštruktúry rad povinností, ktoré v samotnom zákone nie sú podrobne špecifikované
- Na informačné systémy organizácií sa vzťahujú aj iné zákony (minimálne Zákon č. 275/2006 Z.z. o ISVS, prípadne iné), stanovujúce pre prevádzkovateľa ďalšie povinnosti
- Podstata právnych požiadaviek – zaistenie informačnej bezpečnosti prvku kritickej infraštruktúry a ďalších informačných systémov

Úvod (2)

- **Cieľ prednášky**:
  - Identifikovať a vysvetliť povinnosti vyplývajúce zo zákonov
  - Ukázať, ako ich efektívne splniť
- **Výhoda:**
  - Prvky, o ktorých hovoríme sú informačné a komunikačné systémy
  - ochrana informačných a komunikačných technológií je aktuálna problematika,
  - Existujú prepracované postupy, normy a množstvo dostupných materiálov
- **Postup:**
  - Vysvetlíme, čo je informačná bezpečnosť
  - V zákonoch – veľa nových pojmov (vysvetlíme a zosúladíme)
  - Rozoberieme bezpečnostné požiadavky vyplývajúce z právnych predpisov
  - Popíšeme ako efektívne riešiť definované úlohy
- Viaceré témy len spomenieme, aby sme ukázali celkový obraz, rozvedené budú podrobne v samostatných prednáškach

Prečo sa zaoberať informačnou bezpečnosťou?

- Potreba informačnej bezpečnosti nevyplýva len zo zákonov, ale je skutočne objektívna, pretože
  - Každá organizácia potrebuje na zaistenie svojej činnosť spracovávať informácie
  - Objem potrebných informácií presahuje možnosti ručného spracovania
  - Informačné a komunikačné technológie (IKT) – automatizácia spracovania informácie/údajov
  - IKT priniesli zmenu tradičných procesov spracovania IKT
  - Dôsledky:
    - návrat k tradičným „manuálnym“ metódam spracovania informácie nie je z kapacitných dôvodov možný
    - Znefunkčnenie IKT by organizácii mohlo spôsobiť vážne problémy
- Informáciu a systémy, v ktorých sa spracováva je potrebné primerane chrániť

Čo je informačná bezpečnosť (IB)?

- Aj keď sa určite zhodneme na potrebe IB, predstavy o tom, čo IB je, sú rozdielne
- IB sa používa minimálne v troch rozličných významoch (zdroj nedorozumení)
  - Želaný stav IKT (všetko funguje v súlade s požiadavkami a potrebami organizácie) [úroveň IB v organizácii]
  - Činnosť smerujúca k dosiahnutiu ideálneho stavu [Systém manažmentu informačnej bezpečnosti] [BSI to nazýva IB proces]
  - Medziodborová vedná disciplína zaoberajúca sa vývojom metód ochrany informácie a IKT
- Pojem IB budeme používať vo všetkých troch významoch, najmä však v druhom

Ciele informačnej bezpečnosti

- Všeobecný cieľ (čom očakávame od IB) je jasný (zaistiť aby povolané osoby a len oni mali k dispozícii informácie, na ktoré sa môžu spoľahnúť), ale treba ho konkretizovať, aby sa dali spraviť kroky na jeho dosiahnutie
- Začneme pojmami
- *Informácia* – základný, ťažko definovateľný pojem (filozofia: obsah odrazu)
- Nepotrebujeme univerzálnu definíciu. Informácie sú zaznamenané v podobe údajov (*údaj* = forma, informácia obsah), ak to nebude podstatné, budeme pojmy údaje a informácia chápať ako synonymá
- *Spracovanie informácií*: vytváranie, získavanie, prenos, uchovávanie, vlastné spracovávanie, využívanie, archivovanie, ničenie informácií
- Čo potrebujeme chrániť: informáciu od vytvorenia až po zničenie
  Chrániť = zaistiť dôvernosť, integritu, dostupnosť údajov
- CIA = *základné bezpečnostné atribúty* údajov/informácie alebo základné bezpečnostné požiadavky na ochranu údajov
- Okrem CIA existujú aj iné bezpečnostné požiadavky na ochranu údajov

Základné bezpečnostné požiadavky

- **Dôvernosť údajov (confidentiality)** – k informácii, ktorú údaje obsahujú nemajú mať prístup nepovolané osoby
- **Integrita údajov (data integrity)** – údaje nemôžu byť modifikované bez toho, aby si to oprávnená osoba všimla
- **Dostupnosť údajov (data availability)** – oprávnená osoba má údaje k dispozícii kedykoľvek, keď o to požiada
- Poznámky
  - Rozdiel medzi prístupom k údajom a prístupom k ich obsahu
  - Spôsob zabezpečenia dôvernosti (ochrana prístupu a šifrovanie)
  - Dôvernosť – všeobecný pojem a dôverné = druhý stupeň klasifikačnej schémy utajovaných skutočností
  - Integrita: absolútna požiadavka – nemennosť údajov – je nerealistická
  - Riešenie integrity – ochrana prístupu, logy a kryptografické prostriedky
  - Dostupnosť – prípustné omeškanie, alebo max. % nedostupnosti

Základné pojmy (1)

Čo a pred čím je potrebné chrániť?

- Z hľadiska IB je primárnym cieľom ochrany informácia (= CIA?) počas celého jej životného cyklu
- Stále príliš všeobecná požiadavka:
  - informácia má rôzne formy, v rozličných systémoch, pracujú s ňou rozliční ľudia;
  - Navyše rôzne informácie môžu mať rôzne požiadavky na ochranu
- Vnesieme do ochrany informácií systém a konkretizujeme všeobecný cieľ
- *Aktívum (asset)* – čokoľvek, čo má pre organizáciu hodnotu a vyžaduje si ochranu (príklady: pracovné procesy, činnosti a služby organizácie, informácie, hw, sw, sieť, personál, sídlo, organizačná štruktúra, dobré meno,...)
- Špeciálne: *informačné aktíva* (údaje, programy, dokumentácia, know-how,...)
- *Hrozba* - objektívne existujúca možnosť, ktorej naplnenie môže poškodiť niektoré aktívum (prírodné javy, technické poruchy, chyby, omyly, ľudia)

Základné pojmy IB (2)

Hrozby

- Hrozby (napríklad)
  - Prírodné (*vis major*) požiar, záplava, poveternostné vplyvy, zemetrasenie, sopky, blesk...
  - Technické poruchy (IKT a podporných zariadení, budov, infraštruktúry)
  - Chyby SW
  - Ľudský činiteľ (úmyselné a neúmyselné)
  - Organizačné nedostatky
  - Právne (dôsledky porušenia právnych noriem)
  - iné
- Hrozba má *nositeľa* (hrozba záplavy, nositeľ rieka, kanalizačné potrubie)
- *Zraniteľnosť* : chyba, nedostatok, spôsob použitia aktíva, ktoré spôsobujú, že sa hrozba voči aktívu môže uplatniť (príklad: hrozba krádeže, zraniteľnosť – umiestnenie počítača v nezabezpečenej miestnosti)
- Existujú rozsiahle katalógy hrozieb aj zraniteľností

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Základné pojmy (3)

Bezpečnostné incidenty

- Naplnenie hrozby, v širšom zmysle akákoľvek odchýlka od stanovených pravidiel, ktorá môže viesť k narušeniu bezpečnosti – *bezpečnostný incident*
- *Útok* – cieľavedomý pokus o narušenie informačnej bezpečnosti
- Pôvodca útoku: *útočník*
- *Útočný potenciál:*
  - Motivácia
  - Znalosti
  - Príležitosť
- Príklad: krádež PC a krádež údajov z databázy organizácie

KPMG
cutting through complexity™

Základné pojmy IB (4)

Riziká

- *Dopad* – negatívne dôsledky toho, že sa naplnila hrozba voči aktívu (ukradnutý počítač, prezradené heslo)
- *Riziko* = pojem umožňujúci merať závažnosť hrozieb: stredná hodnota dopadu hrozby (dopad x pravdepodobnosť nastatia hrozby)
- Príklad: organizácia má 100 PC, pravdepodobnosť poruchy 15%, cena opravy 200 Euro, riziko poruchy je 100 x 0.15 x 200 = 3000 Euro
- *opatrenie*: riešenie (technické, organizačné, personálne, právne, iné), ktoré znižuje riziko (pravdepodobnosť naplnenia a/alebo dopad hrozby)
- *Analýza rizík* – stanovenie a ohodnotenie rizík vyplývajúcich z hrozieb relevantných vo vzťahu k aktívam organizácie
- *Hranica akceptovateľného rizika* – úroveň rizika, ktorú sa organizácia rozhodla znášať (napr. preto, lebo znižovanie rizika pod akceptovateľnú úroveň nie je z ekonomického hľadiska efektívne)

Prečo máme riešiť IB v organizácii?

- Objektívna potreba ochrany informácií
- (najdôležitejšie) právne požiadavky na ochranu informácií
  - Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
  - Výnos č. 312/210 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy
  - Zákon 45/2011 Z. z. o kritickej infraštruktúre,
  - Zákon č. 215/2004 Z.Z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
  - Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení zákona č. 602/2003 Z. z., zákona č. 576/2004 Z. z. a zákona č. 90/2005 Z. z.
  - Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Zoznam určite nie je úplný a bude sa neustále rozširovať

Kde začať?

- Objektívna požiadavka: musíme zaistiť **primeranú** úroveň IB v každej organizácii
- Nemusíme znova objavovať to, čo je už dávno známe:
  - ISO normy radu 27000
  - Metodické materiály amerického NISTu, nemeckého BSI a iných inštitúcií
- Vychádzame z vybraných ISO noriem a noriem BSI
- Základ: dokument Politika informačnej bezpečnosti (Bezpečnostná politika) organizácie
- Úlohou bezpečnostnej politiky je povedať každému zamestnancovi organizácie **čo môže, čo nesmie, čo musí** a **za čo je zodpovedný**
- Bezpečnostú politiku musí schváliť vedenie a
- Musí byť dostupná každému zamestnancovi, prípadne externým spolupracovníkom

Obsah bezpečnostnej politiky (1)

- Bezpečnostná politika bude predmetom samostatnej prednášky, na tomto mieste uvedieme len základné informácie, aby sme o nej mali predstavu
- Deklarácia vedenia organizácie
  - O význame ochrany informácií
  - Identifikácia hlavných aktív
  - Stanovenie cieľov IB v organizácii
  - Podpora vedenia organizácie pri ich napĺňaní
- Oblasť použiteľnosti bezpečnostnej politiky
- Štruktúra a obsah bezpečnostnej dokumentácie nadväzujúcej na bezpečnostnú politiku
- Stanovenie zodpovednosti zamestnancov za presadzovanie a dodržiavanie bezpečnostnej politiky
- Klasifikácia informácie (klasifikačná schéma)
- Spôsob analýzy rizík a hranica akceptovateľného rizika

Obsah bezpečnostnej politiky (2)

- Monitoring, kontrola a audit informačných a komunikačných systémov (IKS) organizácie
- Riešenie bezpečnostných incidentov
- Zaistenie kontinuity činnosti organizácie
- Správa bezpečnostnej politiky organizácie (riadne a mimoriadne revízie bezpečnostnej politiky)

* * *

- Bezpečnostná politika nerieši všetko – spravidla vysokoúrovňový dokument (1. úroveň)
- Podrobnosti v špecializovaných bezpečnostných politikách alebo bezpečnostných štandardoch (2. úroveň)
- Pravidlá na uplatňovanie bezpečnostnej politiky: bezpečnostné praktiky (3. úroveň)
- Podrobnosti v samostatnej prednáške

Analýza rizík (1)

(ako na tom v organizácii s IB sme)

- Tiež bude náplňou samostatnej prednášky
- Dosiahnutie potrebnej úrovne IB – čas, ľudia, prostriedky, organizačné zmeny, administratíva; a prinesie aj obmedzenia
- Cost/benefit skôr ako začneme radikálne riešiť IB v organizácii, potrebujeme poznať skutočné bezpečnostné potreby systému alebo organizácie
- Rozsah analýzy (čoho sa bude týkať)
- Identifikácia
  - aktív (vlastníci, umiestnenie)
  - (relevantných) hrozieb
  - bezpečnostných požiadaviek (legislatíva)
  - existujúcich opatrení
  - Zraniteľností
  - Dopadov hrozieb

Analýza rizík (2)

- **Odhad rizík**
- Dva základné prístupy:
  - Kvantitatívny (číselné vyjadrenie)
  - Kvalitatívny (slovné vyjadrenie: {pravdepodobnosť, dopad, riziko} → {vysoké, stredne vysoké, nízke}
- Výsledok odhadu rizík = zoznam riziko + odhad; napr. (prezradenie prístupových hesiel; vysoké r.)
- **Vyhodnotenie/ohodnotenie rizík**
  - Porovnanie odhadnutej rizík s kritériami na ohodnotenie rizík
  - Potrebná súčinnosť majiteľov aktív
- Výsledok
  - Ktorými rizikami sa organizácia zaoberať (stanovenie priorít)
  - Ktoré riziká akceptuje (ale bude spravovať)

Ošetrenie rizík

- Máme zoznam rizík podľa závažnosti
- 4 možnosti:
  - Redukcia rizika (prijatie opatrení na zníženie pravdepodobnosti a/alebo dopadu hrozby na aktívum)
  - Prijatie rizika (ak jeho úroveň nepresahuje úroveň akceptovateľného rizika)
  - Vyhnutie sa riziku (iné riešenie, napr. presťahovanie výpočtových kapacít na bezpečnejšie miesto)
  - Prenesenie rizika (zapojenie tretej strany – poistenie, outsourcing bezpečnostných služieb, zmluvné podmienky – zásah do x hodín)

Po analýze rizík

- Analýzu rizík robia odborní pracovníci, ale návrh na ošetrenie rizík sa týka chodu organizácie (opatrenia) – schvaľuje vedenie (v norme = akceptovanie rizík)
- Informovanie o rizikách (všetky zainteresované strany)
- Implementácia opatrení
- Monitorovanie rizík a revízie odhadu/ohodnotenia rizík (zmeny)
- Celý proces = spravovanie rizík (podstata zaistenia IB v organizácii)
- Metaúroveň: posudzovanie a vylepšovanie samotného systému spravovania rizík

Systematický prístup k IB

- Zaistenie potrebnej úrovne IB v organizácii – trvalý proces
- Opatrenia na zaistenie IB zasahujú do činnosti (procesov) organizácie
- Potreba súčinnosti všetkých zamestnancov a tretích strán (nedá sa uplatniť uniformný prístup, lebo majú rôzne práva aj povinnosti)
- Nie je zadarmo (náklady na IB sa pritom ťažko zdôvodňujú)
- V malých systémoch/organizáciách sa možno dá uplatňovať *ad hoc* prístup (problém - riešenie), v ostatných je potrebné zaviesť nejaký systém manažmentu IB
- ISO rad noriem 27000 venovaných manažmentu IB (budeme o nich ešte hovoriť)
- Bezpečnostné štandardy Výnosu o štandardoch pre ISVS vychádzajú z normy ISO/IEC 27002
- Rozdiel: mať v organizácii systém manažmentu IB a mať certifikovaný systém manažmentu IB v súlade s ISO 27001-2
- Výnos MF SR nepožaduje certifikáciu

Prehľad systému manažmentu IB

- Tiež bude predmetom samostatnej prednášky
- Budeme vychádzať z ISO noriem radu 27000, najmä ISO/IEC 27002
  - Bezpečnostná politika
  - Organizácia IB
  - Správa aktív
  - Personálna bezpečnosť
  - Fyzická bezpečnosť
  - Manažment vzťahov s dodávateľmi/poskytovateľmi služieb
  - Prevádzka systémov a komunikácie
  - Manažment aplikačných sieťových služieb
  - Riadenie prístupu
  - Obstarávanie, vývoj a údržba systémov
  - Riešenie bezpečnostných incidentov
  - Manažment kontinuity činnosti
  - Súlad s právnymi predpismi

Prehľad systému manažmentu IB (2)

- Bezpečnostná politika
- O obsahu a význame sme už hovorili
- Vedenie Bezpečnostnou politikou
  - definuje smerovanie IB v organizácii
  - Deklaruje záväzok/odhodlanie presadzovať ju

Prehľad systému manažmentu IB (3)

Organizácia IB

- Cieľ: vytvoriť organizačné podmienky pre zavedenie (ak nie je) a riadenie IB v organizácii
- Vedenie:
  - Schvaľuje politiku IB
  - Zaraďuje zamestnancov do bezpečnostných rolí (zriaďuje bezpečnostný manažment a schvaľuje štruktúru bezpečnostných rolí)
  - Posudzuje a reviduje implementáciu IB v organizácii
  - Presadzuje IB v organizácii (napr. zohľadnenie bezpečnostných aspektov v projektovom manažmente)
- Organizácia nadväzuje a udržuje kontakty na štátne inštitúcie, relevantné organizácie, dodávateľov a poskytovateľov služieb pre prípad mimoriadnych udalostí

Prehľad systému manažmentu IB (4)

Správa aktív

- Cieľ: adekvátna ochrana aktív organizácie
- Inventarizácia aktív
  - každé aktívum musí mať vlastníka, zodpovedného za jeho správu a ochranu
  - Pre informačné aktíva: pravidlá používania (vlastník)
- Klasifikácia informácie
  - Úroveň ochrany
  - Spôsob nakladania s klasifikovanými údajmi
- Vedenie organizácie:
  - Schvaľuje klasifikačnú schému
  - Iniciuje inventarizáciu aktív

Prehľad systému manažmentu IB (4)

Personálna bezpečnosť

- Cieľ: aby zamestnanci, externí spolupracovníci a tretie strany
  - Rozumeli svojim povinnostiam a vedeli, za čo nesú zodpovednosť
  - Stačili na rolu, do ktorej sú zaradení
  - A tým sa redukovalo riziko podvodu a krádeže
- Pred zamestnaním
  - Výber zamestnancov
  - Povinnosti v IB zaradené do pracovnej zmluvy (rámcovo)
- Počas zamestnania
  - Informovať zamestnancov o povinnostiach vyplývajúcich z roly
  - Úvodné školenie
  - Priebežné vzdelávanie v IB (adekvátne prac. zaradeniu)
  - Segregácia povinností
  - Formálny disciplinárny proces pri porušení povinností v IB

Prehľad systému manažmentu IB (5)

Personálna bezpečnosť

- Ukončenie zamestnania alebo zmena pracovného zaradenia
  - Spolupráca personálneho oddelenia a útvaru IT
  - Vrátenie zariadení
  - Odňatie/zmena prístupových práv
- Poznámka. Nespokojný zamestnanec je jedným z najčastejších príčin bezpečnostných incidentov
- Vedenie: schválenie a presadzovanie bezpečnostných opatrení v personálnej bezpečnosti

Prehľad systému manažmentu IB (6)

Fyzická bezpečnosť

- Cieľ: zabrániť neoprávnenému fyzickému prístupu k aktívam organizácie; ochrana aktív pred prírodnými vplyvmi a technickými poruchami
- Bezpečné priestory (perimeter, kontrola prístupu, zabezpečené priestory, iné prístupové možnosti)
- Bezpečnosť vybavenia
  - Umiestnenie a ochrana zariadení
  - Podporná infraštruktúra
  - Ochrana káblov (vnútorných sietí)
  - Údržba zariadení
  - Odnášanie zariadení z priestorov organizácie
  - Používanie zariadení mimo priestorov organizácie
  - Vyraďovanie zariadení

Prehľad systému manažmentu IB (7)

Manažment vzťahov s dodávateľmi a poskytovateľmi služieb

- Cieľ: nastaviť a udržiavať vzťahy s dodávateľmi a poskytovateľmi služieb tak, aby nebola narušená IB organizácie
- Externé subjekty majú prístup k zariadeniam, informáciám organizácie a môžu ovplyvniť jej činnosť
- Bezpečnostná politika upravujúca vzťahy s externými subjektmi
- Bezpečnostné požiadavky v zmluvách
- Kontrola dodržiavania zmlúv
- Vedenie
  - Politika a jej premietnutie do zmlúv

Prehľad systému manažmentu IB (8)

Prevádzka systémov a komunikácie

- Táto (a nasledujúce časti) majú technický charakter, uvedieme len prehľad a upozorníme na vybrané otázky
  - Dokumentácia procedúr a zodpovedností
  - Ochrana proti škodlivému softvéru
  - Zálohovanie
  - Redundancia hardvéru
  - Manažment bezpečnosti sietí
  - Narábanie s pamäťovými médiami
  - Prenos informácie
  - Monitorovanie a logovanie
  - Kryptografické prostriedky
  - Mobilné zariadenia a práca na diaľku

Prehľad systému manažmentu IB (9)

Manažment aplikačných služieb na sieti

- integrita a dostupnosť zverejnenej informácie
- Podstatne komplikovanejšie: Bezpečnosť aplikačných služieb ponúkaných prostredníctvom počítačových sietí
  - Autentifikácia zúčastnených strán
  - Požiadavky na dôvernosť, nepopretie pôvodu, prijatia, záväznosť dohodnutých podmienok
  - Integrita a dôvernosť prenášanej informácie
  - Atď.
- Vedenie:
  - Aké informácie organizácia bude zverejňovať prostredníctvom sietí a akú úroveň ochrany im zaručí
  - Aké služby bude organizácia poskytovať pomocou sietí a bezpečnostné požiadavky na ne kladené

Prehľad systému manažmentu IB (10)

Riadenie prístupu

- **cieľ:** zamedziť/obmedziť neoprávnený prístup k (informačným) zdrojom organizácie
- Riadenie prístupu na základe pracovných potrieb a bezpečnostných požiadaviek (roly, bezpečnostná politika)
- Správa prístupových práv používateľov
- Zodpovednosť používateľov (dodržiavanie politiky riadenia prístupu, ochrana autentizačných prostriedkov)
- Riadenie prístupu do systémov a aplikácií
- Vedenie:
  - Klasifikačná schéma
  - Bezpečnostná politika (zásady politiky riadenia prístupu)

Prehľad systému manažmentu IB (11)

Obstarávanie, vývoj a údržba systémov

- Bezpečnosť počas celého životného cyklu
- Bezpečnostné požiadavky na informačné systémy (súčasť celkových požiadaviek na systémy)
- Bezpečnosť pri vývoji a podporných procesoch (vývoj, zmeny, zmeny platforiem, procedúry vývoja systému, bezpečnostné vývojové prostredie, vývoj tretími stranami), schvaľovanie systému
- Bezpečnosť systémových súborov (pravidlá/procedúry pre inštalovanie sw na bežiace systémy, ochrana testovacích dát, prístup k zdrojovým kódom)
- Manažment technických zraniteľností

Prehľad systému manažmentu IB (12)

Manažment bezpečnostných incidentov

- Cieľ: konzistentné a účinné riešenie bezpečnostných incidentov
- Stanovenie zodpovednosti a vypracovanie/zavedenie postupov riešenia incidentov v organizácii
- Oznamovanie bezpečnostných incidentov (rýchle, v súlade s postupmi)
- Oznamovanie odhalených/možných zraniteľností
- Vyhodnotenie a rozhodnutie o nahlásenom bezpečnostnom incidente
- Reakcia na bezpečnostný incident
- Poučenie z bezpečnostných incidentov
- Zber forenzných dôkazov

Prehľad systému manažmentu IB (13)

Manažment kontinuity činnosti

- Organizácia má/mala by riešiť udržanie kontinuity svojej činnosti
- bezpečnostné požiadavky na ochranu informácie zostávajú nemenné za každej situácie
- Plánovanie kontinuity IB
- Implementácia opatrení na zachovanie kontinuity IB
- Vývoj a zavedenie plánov kontinuity činnosti vrátane IB
- Testovanie, údržba a prehodnocovanie plánov kontinuity činnosti

Prehľad systému manažmentu IB (14)

Súlad

- Zákonom stanovené povinnosti a zmluvné záväzky
  - Identifikácia relevantných zákonov a z nich vyplývajúcich požiadaviek
  - Ochrana duševného vlastníctva
  - Ochrana klasifikovanej informácie
  - Ochrana osobných údajov
  - Kryptografické prostriedky
- Štandardy
  - Bezpečnostná politika a štandardy
- audit

Ochrana prvku kritickej (informačnej) infraštruktúry (CRITIS)

- Zákon č. 45/2011 o kritickej infraštruktúre
- Všeobecný a veľmi stručný zákon
- Prvky kritickej infraštruktúry sú systémy rôzneho charakteru a určenia
- Je ťažké stanoviť spoločné požiadavky a pritom vyhovieť špecifikám rôznych systémov
- V zákone – dôraz na fyzickú a organizačnú bezpečnosť, špecifiká informačnej bezpečnosti sa uvádzajú minimálne
- Cieľ: nie je kritika zákona, ale analýza ako sa rozumne dajú interpretovať jeho požiadavky a zabezpečiť primeraná úroveň informačnej bezpečnosti prvku CRITIS
- Využijeme poznatky, ktoré sme prezentovali v predchádzajúcich prednáškach
- Najprv uvedieme požiadavky zákona, potom ich vyjadríme vo forme štandardnej pre IB a popíšeme postup na ich naplnenie a nakoniec sa pozrieme na požiadavky ďalších zákonov relevantné pre prvok CRITIS

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (1)

- Zákon č. 45/2011 o kritickej infraštruktúre, §9 Povinnosti prevádzkovateľa

(1) Prevádzkovateľ je povinný ochraňovať prvok pred narušením alebo zničením. Na ten účel prevádzkovateľ je povinný

a) uplatniť pri modernizácii prvku technológiu, ktorá zabezpečuje jeho ochranu,

- Kľúčová je úvodná veta; v IB by dokonca bola postačujúca (due care, náležitá starostlivosť)
- Požiadavka podľa písm. a) v prípade IKT trocha zavádza, pretože
  - sa uplatňuje pri zmenách prvku, ktoré znamenajú jeho technologický upgrade (čo dovtedy?)
  - Predpokladá, že na zabezpečenie ochrany prvku budú stačiť samotné technológie (nestačia)
- V záujme adekvátneho zaistenia bezpečnosti prvku budeme hľadať aj iné riešenia

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (2)

§9 ods 1) písm b) zaviesť bezpečnostný plán po predchádzajúcom vyjadrení príslušného ústredného orgánu do šiestich mesiacov od doručenia oznámenia o určení prvku a o jeho zaradení do sektora, ak sa vo výnimočnom odôvodnenom prípade nedohodne s príslušným ústredným orgánom na predĺžení tejto lehoty; lehotu je možné predĺžiť iba jedenkrát, maximálne o tri mesiace,

- Zákon podrobnejšie špecifikuje požiadavky na bezpečnostný plán a spôsob jeho vytvárania v § 10 a v prílohe 2:

Bezpečnostný plán (§ 10)

(1) Bezpečnostný plán obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.

(2) Bezpečnostné opatrenia na ochranu prvku sú najmä mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.

(3) Rozsah bezpečnostných opatrení na ochranu prvku sa určuje na základe posúdenia hrozby narušenia alebo zničenia prvku.

(4) Minimálny postup pri vypracúvaní bezpečnostného plánu je uvedený v prílohe č. 2.

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Príloha č. 2 k zákonu č. 45/2011 Z. z. (1)

MINIMÁLNY POSTUP PRI VYPRACÚVANÍ BEZPEČNOSTNÉHO PLÁNU

Pri vypracúvaní bezpečnostného plánu sa postupuje takto:

A. Určujú sa dôležité zariadenia prvku.

B. Vyhodnocuje sa riziko hrozby narušenia alebo zničenia jednotlivých zariadení prvku, ich zraniteľné miesta, predpokladané dôsledky ich narušenia alebo zničenia na funkčnosť, integritu a kontinuitu činnosti prvku.

KPMG cutting through complexity™

Príloha č. 2 k zákonu č. 45/2011 Z. z. (2)

MINIMÁLNY POSTUP PRI VYPRACÚVANÍ BEZPEČNOSTNÉHO PLÁNU

c. Uskutočňuje sa výber hlavných bezpečnostných opatrení na ochranu prvku, ktoré sa členia na

a) trvalé bezpečnostné opatrenia, ktorými sú investície a postupy na zabezpečenie ochrany prvku, a to

1. mechanické zábranné prostriedky,
2. technické zabezpečovacie prostriedky,
3. bezpečnostné prvky informačných systémov,
4. organizačné opatrenia s dôrazom na postup pri vyrozumení a varovaní, ako aj na krízové riadenie,
5. odborná príprava osôb, ktoré zabezpečujú ochranu prvku,
6. kontrolné opatrenia na dodržiavanie trvalých bezpečnostných opatrení,

b) mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.

Príloha č. 2 k zákonu č. 45/2011 Z. z. (3)

MINIMÁLNY POSTUP PRI VYPRACÚVANÍ BEZPEČNOSTNÉHO PLÁNU

D. Určujú sa hlavné bezpečnostné opatrenia na ochranu prvku.

E. Bezpečnostný plán sa počas jeho tvorby konzultuje s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.

Bezpečnostný plán/projekt prvku CRITIS

Zákon o kritickej infraštruktúre	Štrandardné postupy IB
Určujú sa dôležité zariadenia prvku	Inventarizácia aktív systému
Vyhodnocuje sa riziko hrozby	Inventarizácia hrozieb
zraniteľné miesta	Zoznam zraniteľností
	Zoznam bezpečnostných požiadaviek
predpokladané dôsledky ich narušenia alebo zničenia	Dopady hrozieb na aktíva
	Analýza rizík (chýba)
výber hlavných bezpečnostných opatrení	Návrh opatrení
mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.	Správa rizík
D. Určujú sa hlavné bezpečnostné opatrenia na ochranu prvku	Implementácia opatrení
BP ... konzultuje s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.	ISMS

Kritériá informačnej bezpečnosti zákona o kritickej infraštruktúre

- V prílohe 2: Vyhodnocujú sa ... predpokladané dôsledky ich narušenia alebo zničenia (*aktív*) na funkčnosť, integritu a kontinuitu činnosti prvku.
- Postačuje nám požiadavka na funkčnosť, ak ju budeme chápať v širšom zmysle, t.j. tak, že požadujeme, aby systém fungoval v súlade s bezpečnostnou politikou.
- *Funkčnosť* v chápaní Zákona je ekvivalentná spoľahlivosti a čiastočne dostupnosti, *integrita* zariadenia znamená jeho neporušenosť a v podstate je už obsiahnutá v požiadavke na funkčnosť, *kontinuita činnosti* znamená dostupnosť služieb a zdrojov systému; t.j. jednu zo základných bezpečnostných požiadaviek na ochranu informácie
- **Záver:** štandardné bezpečnostné požiadavky na dôvernosť, integritu a dostupnosť informácie postačujú na pokrytie požiadaviek Zákona

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Postup pri zaisťovaní ochrany prvku CRITIS z hľadiska IB

- Pozrieme sa na požiadavky Zákona z hľadiska IB
- Stanovenie bezpečnostných požiadaviek na prvok CRITIS
  - Identifikácia jeho hlavných aktív
  - Identifikácia hrozieb
  - Identifikácia zraniteľností
  - Identifikácia právnych povinností a zmluvných záväzkov
- Analýza rizík
- Návrh opatrení (detailnejší pohľad)
- Správa rizík
- Komunikácia s tretími stranami

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Opatrenia na ochranu prvku CRITIS z hľadiska IB

- Uvedieme ešte raz:

  a) trvalé bezpečnostné opatrenia, ktorými sú investície a postupy na zabezpečenie ochrany prvku, a to

  1. mechanické zábranné prostriedky,

  2. technické zabezpečovacie prostriedky,

  3. bezpečnostné prvky informačných systémov,

  4. organizačné opatrenia s dôrazom na postup pri vyrozumení a varovaní, ako aj na krízové riadenie,

  5. odborná príprava osôb, ktoré zabezpečujú ochranu prvku,

  6. kontrolné opatrenia na dodržiavanie trvalých bezpečnostných opatrení,

  b) mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.

- Vráťme sa k povinnostiam prevádzkovateľa

KPMG
cutting through complexity™

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (3)

c) prehodnocovať priebežne bezpečnostný plán, a ak je to potrebné, zaviesť po predchádzajúcom vyjadrení príslušného ústredného orgánu aktualizovaný bezpečnostný plán,

d) oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom,

e) precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku,

f) určiť oprávnenú osobu, ktorá je zároveň kontaktná osoba, ak ide o prvok európskej kritickej infraštruktúry,

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (4)

g) poskytnúť príslušnému ústrednému orgánu súčinnosť,najmä údaje, doklady a vysvetlenia potrebné na

1. určenie prvku a jeho zaradenie do sektora, ako aj vyradenie prvku zo sektora,
2. posúdenie ochrany prvku vrátane zabezpečenia ochrany prvku prevádzkovateľom strážnej služby alebo ozbrojeným bezpečnostným zborom,
3. vypracovanie analýzy rizík sektora,
4. správu registra prvkov,

h) postupovať podľa bezpečnostného plánu v prípade hrozby narušenia alebo zničenia prvku.

Výnimky

(3) Na prevádzkovateľa, ktorý vypracúva havarijný plán alebo obdobný bezpečnostný dokument podľa osobitného predpisu,4) sa nevzťahuje odsek 1 písm. b), c), d) e) a h).

- Napríklad zákon č. 261/2002 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Z logického hľadiska by mohlo ísť o akýkoľvek zákon, ktorý na ochranu prvku CRITIS kladie rovnaké alebo vyššie požiadavky ako zákon o kritickej infraštruktúre
  - Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
  - Zákon č. 215/2004 Z.Z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
  - Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení zákona č. 602/2003 Z. z., zákona č. 576/2004 Z. z. a zákona č. 90/2005 Z. z.
- Kto rozhoduje o výnimke – implicitne pravdepodobne MF SR
- MF SR pripravuje zákon o IB

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (4)

§2, písm k) citlivou informáciou o kritickej infraštruktúre (ďalej len „citlivá informácia“) neverejná informácia, ktorej zverejnenie by sa mohlo zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku,

§ 12 Citlivá informácia

(1) Písomnosť alebo iný hmotný nosič, ktorý obsahuje citlivú informáciu, sa označuje slovami „Kritická infraštruktúra – nezverejňovať“.

(2) Oprávnená osoba je povinná zachovávať mlčanlivosť o citlivej informácii, a to aj po zániku jej oprávnenia oboznamovať sa s citlivou informáciou.

(3) Citlivá informácia sa nesprístupňuje podľa osobitného predpisu. (Infozákon)

Sankcie

- Fyzická osoba za prezradenie citlivých informácií (§ 14) (Priestupok)
- prevádzkovateľ za nesplnenie povinností pri ochrane prvku CRITIS (správny delikt, § 15)

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o kritickej infraštruktúre a ISMS

- Význam prvkov CRITIS a Zákonom o kritickej infraštruktúre požadovaná úroveň jeho ochrany si z hľadiska informačnej bezpečnosti vyžaduje systematické riešenie v podobe ISMS
- Zákon o kritickej infraštruktúre nerieši zvlášť špecifiká prvkov CRITIS
- Napriek (pochopiteľnej) všeobecnosti sa požiadavky, ktoré kladie, dajú zosúladiť so štandardným ISMS

KPMG
cutting through complexity™

Ochrana prvku CRITIS

- Ako zosúladiť požiadavky Zákona o kritickej infraštruktúre s potrebami ochrany prvku CRITIS?
- Požiadavky Zákona
  - Sú neúplné (z hľadiska štandardov IB)
  - Používajú neštandardný jazyk (univerzálny zákon)
  - Ale nekladú prekážky adekvátnej ochrane prvkov CRITIS
- Ideálne riešenie: výnimka podľa § 9, ods. 3) a Zákon 275/2006 o ISVS, ak má organizácia zavedený Systém riadenia informačnej bezpečnosti podľa Výnosu č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy
- Ak by aj prvok nebol ISVS, ale má zavedený ISMS podľa Výnosu č. 312/2010 Z.z., spĺňa všetky požiadavky Zakona č. 45/2011

Porovnanie bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS (1)

Súlad bezpečnostných štandardov ISVS so Zákonom o kritickej infraštruktúre:

(§ 28 Výnosu) Štandardom pre riadenie informačnej bezpečnosti je

a) vypracovanie a schválenie bezpečnostnej politiky povinnej osoby, ktorej obsahom je (o.i.)

6. zhodnotenie súladu bezpečnostnej politiky povinnej osoby so všeobecne záväznými právnymi predpismi,

7. určenie požiadaviek na informačné systémy verejnej správy, vyplývajúcich zo všeobecne záväzných právnych predpisov,

b) zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky povinnej osoby,

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Komentár

- Prevádzkovateľ ISVS (povinná osoba podľa zákona o ISVS) podľa štandardov pre ISVS vypracuje pre ISVS bezpečnostnú politiku a bude ju dodržiavať,
- Bezpečnostná politika obsahuje o.i.
  - všetky požiadavky na ISVS, vyplývajúce zo všeobecne záväzných právnych predpisov, teda aj Zákona o kritickej infraštruktúre
  - Zhodnotenie súladu Bezpečnostnej politiky a všeobecne záväzných právnych predpisov
- T.j. požiadavky Zákona o kritickej infraštruktúre sa explicitne premietnu do Bezpečnostnej politiky ISVS

KPMG
cutting through complexity™

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Porovnanie bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS (2)

- Pozrieme sa na konkrétne požiadavky Zákona o kritickej infraštruktúre:
- Zákon, §9 Povinnosti prevádzkovateľa

(1) Prevádzkovateľ je povinný ochraňovať prvok pred narušením alebo zničením.

- Výnos: Cieľom všetkých bezpečnostných štandardov (§ 28-42), je ochrana ISVS
- Zákon §9 Zákona Povinnosti prevádzkovateľa
  - prevádzkovateľ je povinný a) uplatniť pri modernizácii prvku technológiu, ktorá zabezpečuje jeho ochranu
- Výnos:
  - § 35 Aktualizácia softvéru
  - § 41 (Aktualizácia informačno-komunikačných technológií)

KPMG cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Porovnanie bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS (3)

- **Zákon §9 ods 1) písm b)** zaviesť bezpečnostný plán
- Výnos:
  - § 28 Riadenie informačnej bezpečnosti (vypracovanie bezpečnostnej politiky)
  - § 30 Manažment rizík pre oblasť IB (zavedenie ISMS. Vrátane analýzy a správy rizík)
- **Zákon §9 ods 1) písm** c) prehodnocovať priebežne bezpečnostný plán
- Výnos:
- § 28 Riadenie informačnej bezpečnosti, písm. a)
  - určenie postupu pri revízii bezpečnostnej politiky povinnej osoby vrátane periodicity pravidelných revízií a dôvodov mimoriadnych revízií bezpečnostnej politiky povinnej osoby,
  - § 31 Kontrolný mechanizmus riadenia informačnej bezpečnosti (audit)

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Porovnanie bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS (4)

- Zákon, §9 písm. d) oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom
- Výnos: § 29 Personálna bezpečnosť písm. a) (poučenie zamestnancov o BP)
- Zákon, §9 písm. e) precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku,
- Výnos:
  - § 30 Manažment rizík pre oblasť informačnej bezpečnosti (havarijné plány a plány obnovy)
  - § 36 Monitorovanie a manažment bezpečnostných incidentov (informovanosť používateľov)
- Zákon, §9 písm. f) určiť oprávnenú osobu
- Výnos: §28 Riadenie informačnej bezpečnosti, písm c), d)

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Porovnanie bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS (5)

- Zákon §9, písm. h) postupovať podľa bezpečnostného plánu v prípade hrozby narušenia alebo zničenia prvku
- Výnos: §28 Riadenie informačnej bezpečnosti, písm b)
- Zákon § 10 Bezpečnostný plán – už sme rozobrali
- Zákon § 12 Citlivá informácia
- Výnos: §28 Riadenie informačnej bezpečnosti, písm a), ods. 7,8,13 (požiadavky zákonov, rozsah a úroveň ochrany ISVS, bezpečnostná dokumentácia)

KPMG
cutting through complexity™

Prehľad bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS

Z 45/2011	požiadavka	Výnos
§9 ods. 1	Ochrana prvku pred narušením alebo zničením	§28-42
Písm. a)	Modernizácia prvku	§ 41
Písm. b)	Zavedenie bezpečnostného plánu	Najmä § 28, § 30
Písm. c)	Aktualizácia bezpečnostného plánu	Najmä §28, §31
Písm. d)	Oboznamovanie zamestnancov s BP	§ 29
Písm. e)	Cvičenia	§ 30, f) § 36
Písm. f)	Stanovenie oprávnenej osoby	§ 28 písm. c), d)
Písm. h)	Dodržiavanie BP	§28 písm. b)
§ 10	Bezpečnostný plán	
§ 12	Citlivá informácia	§ 28 a) body 7,8,13

Čo treba dopracovať?

- Všeobecnými ustanoveniami bezpečnostných štandardov sú pokryté všetky požiadavky Zákona o kritickej infraštruktúre
- Najmä ustanovenia § 28, písm. a) body 6,7,8 (požiadavky vyplývajúce zo zákonov, súlad s legislatívou, stanovenie rozsahu a úrovne ochrany) a 13 – rozpracovanie bezpečnostnej dokumentácie
- Bude potrebné konkretizovať
  - Opatrenia na zachovanie/obnovenie Kontinuity činnosti (explicitne uviesť cvičenia v havarijných plánoch)
  - Klasifikácia informácie (doplniť citlivú informáciu a požiadavky na jej ochranu), do bezpečnostných štandardov doplniť klasifikačnú schému (pripravuje sa v zákone o IB)

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Iné zákony

428/2002 Z. z. o ochrane osobných údajov

- Len informatívne, pretože existuje novela vrátená prezidentom
- Ochrane osobných údajov je venovaná Hlava II
- Trocha nekonzistentný:
  - Chápanie bezpečnosti
  - Rozsah pôsobnosti
  - Veľa odkazov na iné zákony
- Požiadavky na ochranu údajov sa však dajú splniť bez väčšieho dodatočného úsilia
- Bezpečnosť sa chápe ako zachovanie dôvernosti, integrity, dostupnosti a zamedzenie neprípustného spracovávania (osobných údajov)
- Pod posledný pojem sa zmestí všetko

KPMG
cutting through complexity™

Iné zákony

428/2002 Z. z. o ochrane osobných údajov (2)

- Osobné údaje je prevádzkovateľ/spracovateľ povinný chrániť v každom prípade (§ 15, ods. (1)), navyše
- Ak sa v systéme spracovávajú osobitné kategórie osobných údajov
  - pripojený na verejnú sieť - bezpečnostný projekt
  - Nepripojený – len zdokumentovanie bezpečnostných opatrení
- Výnimka – bezpečnostný projekt podľa Zákona o ochrane utajovaných skutočností
- Kľúčová otázka: čo všetko spadá do osobitnej kategórie osobných údajov (rodné číslo? rodinné pomery, obmedzená pracovná schopnosť,...)
- Technické a organizačné požiadavky na ochranu prvkov CRITIS, v ktorých sa spracovávajú (aj) osobné údaje sa dajú riešiť v rámci ISMS podľa Výnosu MF SR č. 312/2010 z.z.

Iné zákony

428/2002 Z. z. o ochrane osobných údajov (3)

- Nekonzistentnosti (hrozby-riziká, bezpečnostné ciele, bezpečnostný zámer-bezpečnostná politika)
- Zaradenie osobných údajov do klasifikačnej schémy
- Splnenie administratívnych povinností (zodpovedná osoba, školenia, nahlasovanie na ÚOOÚ)
- Odporúčanie: ak sa dá, redukovať počet systémov, v ktorých sa spracovávajú osobné údaje (teoreticky – práca off-line, prakticky ???)

Iné zákony

Zákon č. 215/2004 Z. z.

- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Najvyššia priorita, ale vzťahuje sa len na vymedzený okruh systémov
- Ak sa na prvok, alebo jeho subsystém vzťahuje Zákon č. 215/2004 Z. z. treba pri ochrane prvku postupovať podľa neho (predpoklad: uplatní sa výnimka podľa § 9, ods. 3 Zákona 45/2011)
- Minimalizovať rozsah systému, kde sa spracovávajú utajované skutočnosti (kvôli zjednodušeniu prevádzky a optimalizácii nákladov na ochranu)
- Prípadné nejasnosti MF-MV-NBÚ

Záver

- Informačná bezpečnosť – nutná podmienka fungovania (kritickej) informačnej infraštruktúry spoločnosti
- Súčasný stav (kompetencie, legislatíva, štandardy, prax) je neuspokojivý; dôsledok historického vývoja
- Živelný vývoj nebude konvergovať dostatočne rýchlo do požadovaného stavu
- O IB sme sa za vyše 40 rokov niečo naučili, vieme ochraňovať jednotlivé IKS, potrebujeme však chrániť globálny digitálny priestor
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union
- V SR pripravovaný Zákon o IB, potrebné by bolo zosúladenie legislatívy a koordinovaný systematický prístup k IB na lokálnej aj globálnej úrovni

* * *

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™