Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Stav IB v SR a globálne riešenie IB

doc. RNDr. Daniel Olejár, PhD.,
mim. profesor UK
olejar@dcs.fmph.uniba.sk

KPMG
cutting through complexity™

Obsah prednášky

- Východiská
- stav IB vo verejnej správe,
- Stratégia IB,
- bezpečnostné povedomie a vzdelávanie v IB,
- klasifikácia informácie a systémov,
- bezpečnostné štandardy,
- legislatíva IB.

Vývoj IKT a IB

- IB sa vyvíja
- Začiatky: IKT sústredené vo výpočtových strediskách, obmedzený prístup používateľov, kvalifikovaná obsluha, jednotná správa (vlastníci:štát, banky, univerzity)
  - IB: fyzická ochrana, režimové opatrenia
- Rozšírenie počítačov aj do komerčnej sféry, lokálny prístup používateľov, potreba vytvárania zložitých systémov a garantovanej úrovne bezpečnosti:
  - systematické riešenia, Orange book a Rainbow series,
  - klasifikácia systémov, certifikácia
  - Vytváranie zložitých systémov z certifikovaných subsystémov
- Internet, vytvorenie globálnej infraštruktúry
  - Masový výskyt počítačov
  - Vzdialený prístup k systémom
  - Malware, hackeri
  - Zaujímavé aplikácie (bankovníctvo, obchodovanie, komunikácia), počítačový zločin

Akútne bezpečnostné problémy

- Cybercrime n x 100 mld USD ročne (Kaspersky, Guardian 2013)
  - Čína
  - Hispánske krajiny a Brazília
  - Turecko
  - Rusko
- Malware (množstvo aj kvalita)
- Botnety (desiatky tisíc až milióny PC)
- Krádeže údajov
- Útoky na bankové systémy
- Odpočúvanie
- Krádeže identity (USA 2009, 11.1 mil ľudí, straty 54 mld USD)
- Útoky na technické systémy (Stuxnet 2010)
- Intelektuálne vlastníctvo (ACTA)
- ...

Východiská (2)

- Eugene Kaspersky: We are living not inside of some perimeter. We are living in the open world. And we need to change our mind about security -- we need to protect all the devices.
- Potreba systematického riešenia IB:
  - Národné stratégie (celkový obraz, priority)
  - Budovanie bezpečnostného povedomia
  - Špecialisti IB v komerčnej sfére
  - Špecializované štátne orgány
  - Legislatíva (počítačová kriminalita, ochrana údajov, autorské práva, štátne informačné systémy, informatizácia,...)
  - Štandardy (národné a medzinárodné)
  - Zosúladenie národných kritérií (interoperabilita technologická a bezpečnostná)
  - Technologické riešenia (I&A, EP, kryptografia, protokoly,...)
  - Medzinárodná koordinácia a kooperácia

Stav IB v SR

- Ako sme na tom s IB na Slovensku?
- Pesimistický pohľad (Prieskum stavu IB, MF 2013)
  - Slabé bezpečnostné povedomie
  - Málo kvalifikovaných odborníkov
  - Nedostatok prostriedkov
  - Nedostatočné know-how
  - Neúplná legislatíva, fragmentácia digitálneho priestoru, kompetencií
  - Slabá koordinácia
  - Slabá spolupráca štát-súkromný sektor-akademická sféra

Stav IB v SR

- Ale
  - Vieme čo treba robiť
  - Existujú čiastkové riešenia (utajované skutočnosti, kritickú infraštruktúru, osobné údaje, elektronický podpis, ISVS,...)
  - Vieme o problémoch, možnostiach riešení aj potenciálnych partneroch
  - Národná stratégia, Koncepcia vzdelávania schválené Vládou SR
  - CSIRT a CSIRT.mil
  - Budujeme know-how (vš štúdium, ISACA, vzdelávanie MF)
  - Odborné kontakty (každý po svojej línii)
  - Komunikácia a záujem o spoluprácu
  - Legislatíva a štandardizácia
  - Existujúca a pripravovaná legislatíva EU
- Je šanca na rýchly posun na vyššiu úroveň

Stratégia IB

- Vytvorená v roku 2007, schválená Vládou SR v auguste 2008
- Východiská
  - Stav a problémy IB na Slovensku
  - Trendy rozvoja IKT a IB
  - Riešenia IB v informačne vyspelých krajinách
- 3 úrovne
  - Strategická (ciele)
  - Prioritné oblasti
  - Kľúčové úlohy

Strategické ciele

1. **prevencia;** zaistenie adekvátnej ochrany digitálneho priestoru Slovenska, aby sa v maximálnej možnej miere predchádzalo bezpečnostným incidentom v ňom,
2. **pripravenosť;** zaistenie schopnosti efektívne reagovať na bezpečnostné incidenty, minimalizovať ich dosah a čas potrebný na obnovu činnosti informačných a komunikačných systémov po bezpečnostných incidentoch,
3. **udržateľnosť;** dosiahnutie, udržiavanie a rozširovanie kompetencie Slovenska v oblasti informačnej bezpečnosti.

Strategické priority a kľúčové úlohy

1. ochrana ľudských práv a slobôd v súvislosti s využívaním NIKI
   - Práva vs. bezpečnostné opatrenia
   - Ochrana osobných údajov/osobnosti
2. budovanie povedomia a kompetentnosti v informačnej bezpečnosti
   - Pôsobenie na verejnosť
   - Vzdelávanie v školách
   - Vzdelávanie ľudí so špeciálnymi potrebami (informatici)
3. vytváranie bezpečného prostredia
   - Legislatíva
   - Kompetencie
   - Koordinácia
   - Normy, metodiky, najlepšie praktiky

Strategické priority a kľúčové úlohy

4. zefektívnenie riadenia informačnej bezpečnosti
   - Monitorovanie hrozieb
   - Včasné varovanie
   - Pomoc pri riešení bezpečnostných incidentov
   - Koordinácia ochrany jednotlivých systémov/organizácií
5. zaistenie dostatočnej ochrany štátnej IKI a IKI podporujúcej kritickú infraštruktúru štátu
   - ISMS
   - Spoľahlivé systémy
   - Bezpečnostné štandardy
   - Ochrana CRITIS

Strategické priority a kľúčové úlohy

6. národná a medzinárodná spolupráca
7. rozširovanie národnej kompetencie
   - Kvalifikačné potreby a systém vzdelávania
   - Výskum
   - Spolupráca štát – akademická sféra – súkromný sektor
   - Sprístupňovanie poznatkov IB verejnosti

Realizácia

- Systém vzdelávania (2009)
- Terminologický slovník
- CSIRT
- Bezpečnostné štandardy
- Prieskum stavu IB
- Príprava Zákona o IB
- Prieskum stavu prvkov CRITIS
- Spolupráca
  - Štát – Univerzity
  - Štát – súkromný sektor
  - Spoločné pracovisko UK-STU-ESET - neúspech

Aktualizácia Národnej stratégie?

- Pokrývala obdobie 2008-2013
- Viac úsilia, ako sa očakávalo, pomalší postup
- Hlasy zo súkromného sektora volajúce po novej stratégii
- Čo zmeniť?

Bezpečnostné povedomie a vzdelávanie v IB

- Bezpečnosť IKT závisí od všetkých používateľov, ktorá s nimi prichádzajú do styku
- Veľká väčšina ľudí nemá záujem poškodiť IKT, ale robí tak z nevedomosti
- Nemusia byť špecialistami v IB, potrebujeme ich naučiť minimum, čo potrebujú na to, aby mohli vykonávať svoju prácu
- 5 kategórií používateľov (Národná stratégia)
  - Laici
  - Vedúci
  - IT špecialisti
  - IB špecialisti
  - Učitelia IB

Systém vzdelávania v IB (1)

- Znalostné štandardy pre jednotlivé kategórie používateľov IKT
- základy: CBK, EBK a ISO 27002
  1. Legislatíva a štandardy IB
  2. Riadenie IB
  3. Správa rizík
  4. Obstarávanie, vývoj a zmeny IKT systémov
  5. Fyzická bezpečnosť
  6. Riadenie prístupu
  7. Bezpečnosť komunikácie
  8. Správa bezpečnostných incidentov
  9. Prevádza IKT systémov a kontinuita činnosti
  10. Audit informačnej bezpečnosti

Systém vzdelávania v IB (2)

- Základná úroveň (pre všetkých 5 kategórií) 400 ľudí, 40 a 80 hodinové kurzy, 3 učebnice, študijné materiály, prehľad IB, problémy a ich riešenie
- Postgraduál
  - Pôvodný zámer 5 predmetov na úrovni vysokoškolských prednášok
  - Uvoľňovanie ľudí
  - Pre koho?
- Riešenie: menšie bloky, virtuálne skupiny
- Okrem toho:
- Odborné semináre, reprofilácia konferencie SASIB
- Metodické materiály (MF a Univerzity)
- Vysokoškolské štúdium (pregraduál aj doktorandské)

Systém vzdelávania v IB (3)

- V budúcnosti:
  - Zimný a letný kurz základov IB
  - Postgraduál
  - Semináre
  - Rozširovanie ponuky vš. vzdelávania (informatici, právnici)
  - Laici
    - Lektori v organizáciách (vzdelávanie dospelých)
    - Stredné školy (doplnenie IB do obsahu informatiky)
    - Modul ECDL pre ostatných
- Otvorené otázky
  - Vedecký výskum (a doktorandské štúdium)
  - Medzinárodná spolupráca
  - Tematický výskum

Klasifikácia informácie a kategorizácia systémov

Podstata klasifikácie

- Neriešiť bezpečnosť jednotlivých aktív, ale
- Zoskupiť aktíva s podobnými bezpečnostnými požiadavkami do tried
- Navrhnúť bezpečnostné opatrenia pre triedy
- Zaradiť aktívum do klasifikačnej triedy je jednoduchšie, ako analyzovať jeho bezpečnostné potreby individuálne

Klasifikačné kritériá

- Klasifikačné kritériá (aktuálne používané)
  - Charakter, resp. účel použitia (údajov a systémov)
  - Bezpečnostné požiadavky na ochranu aktív
- Problém: veľa a rôznych
- Riešenie (USA, Nemecko)
  - Klasifikačné kritériá = bezpečnostné požiadavky (neutrálne)
  - Definovať úroveň ochrany pre typy informácie
- Kritériá
  - Dôvernosť
  - Integrita (aj autentickosť a non repudiation of origin)
  - Dostupnosť
- Rozšírenie integrity je umelé, pridáme autentickosť

Klasifikácia informácie (1)

- Tri úrovne významnosti: nízka, stredná, vysoká + n.a.
- nízka: malé finančné straty, lokálny dopad, neohrozuje činnosť organizácie
- stredný: významné ale zvládnuteľné straty, obmedzenie činnosti organizácie, vplyv na iné organizácie, zdravie ľudí, právne dôsledky
- vysoký: straty ohrozujúce existenciu organizácie, neschopnosť plniť základné funkcie, významný vplyv na iné organizácie, život a zdravie ľudí, ohrozenie mena a záujmov SR
- N.a. – kritérium sa v danom prípade nedá použiť

Klasifikácia informácie (2)

- Klasifikujeme typy a nie jednotlivé položky informácie
- Napr. informácie zverejnené na webovej stránke, osobné údaje, utajované skutočnosti, zdravotné záznamy, kryptografické kľúče
- Štvorica:
  - Vážnosť dopadu pri poušení dôvernosti
  - Vážnosť dopadu pri poušení integrity
  - Vážnosť dopadu pri poušení dostupnosti
  - Vážnosť dopadu pri poušení autentickosti
- Napr. verejná informácia (webová stránka)
  - Dôvernosť: n.a.
  - integrita: stredná
  - Dostupnosť: nízka
  - Autentickosť: stredná

Klasifikácia systémov

- Na základe klasifikácie všetkých typov informácie, ktoré sa v systéme vyskytujú
- Najprv maximá z úrovne jednotlivých požiadaviek (výnimka n.a.) = úrovne ochrany info v systéme vzhľadom na dôvernosť, integritu, dostupnosť a autentickosť (stĺpce tabuľky)
- Klasifikácia systému = maximum z úrovní jednotlivých požiadaviek na ochranu info v systéme (posledný riadok tabuľky)

info	dôvernosť	integrita	dostup.	autentic.
Typ1	n.a.	nízka	vysoká	nízka
Typ2	n.a.	stredná	nízka	n.a.
Typ3	n.a.	nízka	n.a.	nízka
systém	nízka	stredná	vysoká	nízka

Bezpečnostné požiadavky na ochranu systému

- Tri úrovne (USA) nízka, stredná, vysoká
- Pre každú úroveň je definovaný minimálny súbor opatrení
- Úprava súboru opatrení (znižovanie podľa úrovne jednotlivých požiadaviek platnej pre systém) systém: vysoká, ale dôvernosť stredná
- Potom implementácia opatrení a štandardná správa rizík
- Nemecko: zdola nahor, základný súbor opatrení, analýza rizík pre informácie a systémy, kde základná úroveň nestačí
- Katalóg opatrení je priebežne aktualizovaný

Kategórie opatrení

1. Riadenie prístupu/access control (18)
2. Bezp. Povedomie a tréning/awareness and training (4)
3. Audit a dosledovateľnosť/audit and accountability (10)
4. Certifikácia, akreditácia a hodnotenie bezpečnosti /certification, accreditation and security assesment (7)
5. Manažment konfigurácie/confuguration management (6)
6. Plánovanie kontinuity činnosti/Contingency planning (10)
7. Identifikácia a autentizácia/Identification and authentizacion (7)
8. Reakcia na incidenty/Incident response (7)
9. Údržba/Maintenace (6)
10. Ochrana médií/Media protection (8)

Kategórie opatrení (2)

11. Fyzická bezpečnosť a bezpečnosť prostredia/Physical and enviromental protection (20)
12. Plánovanie/Planning (5)
13. Personálna bezpečnosť/Personnel security (8)
14. Odhad rizík/Risk assesment (4)
15. Nadobúdanie systémov a služieb/System and services acquirement (9)
16. Ochrana systémov a komunikácií/System and communication protection (18)
17. Integrita systémov a informácií/System and information integrity (7)

Príklad povinných opatrení v oblasti Fyzickej bezpečnosti (SP 800-53)

Physical and Environmental Protection				
PE-1	Physical and Environmental Protection	X	X	X
PE-2	Physical Access Authorizations	X	X	X
PE-3	Physical Access Control	X	X	X
PE-4	Access Control for Transmission Medium	---	---	X
PE-5	Access Control for Display Medium	---	X	X
PE-6	Monitoring Physical Access	X	X (1)	X (1) (2)
PE-7	Visitor Control	X	X (1)	X (1)
PE-8	Access Logs	X	X (1)	X (1)
PE-9	Power Equipment and Cabling	---	X	X
PE-10	Emergency Shutoff	X	X	X
PE-11	Emergency Power	X	X (1)	X (1) (2) (3)
PE-12	Emergency Lighting	X	X	X
PE-13	Fire Protection	X	X (1)	X (1) (2)
PE-14	Temperature and Humidity Controls	X	X	X
PE-15	Water Damage Protection	X	X	X (1)
PE-16	Environmental Controls Training	---	---	X
PE-17	Environmental Controls Testing	---	---	X
PE-18	Delivery and Removal	X	X	X
PE-19	Alternate Work Site	---	X	X
PE-20	Access Control for Portable and Mobile Systems	X	X (1)	X (1)

Čo ďalej, alebo čo si prečítať?

- Univerzálny a trvalý základ pre dynamicky sa meniacu IB sa nedá spraviť
- Základné poznatky je potrebné aktualizovať a rozširovať
- Ako to robiť efektívne?
- V minulosti nedostatok informačných zdrojov – v súčasnosti prebytok
- Veľa balastu
- Rozumné zdroje
  - Normy medzinárodných a národných štandardizačných organizácií,
  - Návody a odporúčania renomovaných organizácií (NIST, BSI)

ISO normy pre informačnú bezpečnosť

- Sústredíme sa na najdôležitejšie ISO normy, potom spomenieme užitočné normy NIST a BSI
- ISO normy pre oblasť IB cca 80, z nich niektoré vo vývoji
- Stručné delenie:
  1. Manažment IB
  2. Kryptológia
  3. Evaluácia a certifikácia systémov
  4. Bezpečnostné riešenia (Security controls)
  5. Identifikácia a autentizácia
- Z praktického hľadiska najzaujímavejšia je prvá skupina
- Prebieha systematizácia noriem, zosúlaďovanie IB s manažmentom, a manažmentom kvality
- Prečíslovanie noriem, rad 27000 vyhradený pre manažment IB

ISO/IEC normy radu 27000 (1)

základné

- 4 základné:
- **ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary**
  - Úvod do ISMS (information security management systems, systémov manažmentu informačnej bezpečnosti)
  - Základné pojmy a definície pre oblasť ISMS
  - Prehľad rodiny noriem 27000
- **ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements**
  - Relatívne stručný štandard
  - Definuje požiadavky na zriadenie, implementáciu, prevádzku, monitorovanie, revíziu, údržbu a zlepšovanie systému riadenia informačnej bezpečnosti
  - Zohľadňuje činnosť, ktorú organizácia vykonáva a hrozby, ktorým čelí
  - Požiadavky sú definované všeobecne a preto je štandard všeobecne použiteľný
  - Väčšina požiadaviek je povinných, ak chce organizácia certifikovať ISMS podľa ISO 27001

ISO/IEC normy radu 27000 (2)

základné

- **ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management**
- Definuje ciele pre jednotlivé oblasti IB a uvádza zoznam bezpečnostných funkcií/opatrení na dosiahnutie stanovených cieľov
- Pokrýva nasledujúce oblasti IB:
  - 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 legislatívou

ISO/IEC normy radu 27000 (3)
základné

- **ISO/IEC 27005 Information technology — Security techniques — Information security risk management**
- Užitočný štandard, kompletná správa rizík
- Podrobne popisuje postup uvedený na nasledujúcom obrázku (citované podľa normy ISO/IEC 27003)
- **ISO/IEC TR 27008 Information technology — Security techniques — Guidelines for information security management systems auditing**
  - TR poskytuje návod na audit vhodnosti a účinnosti bezpečnostných funkcií ISMS

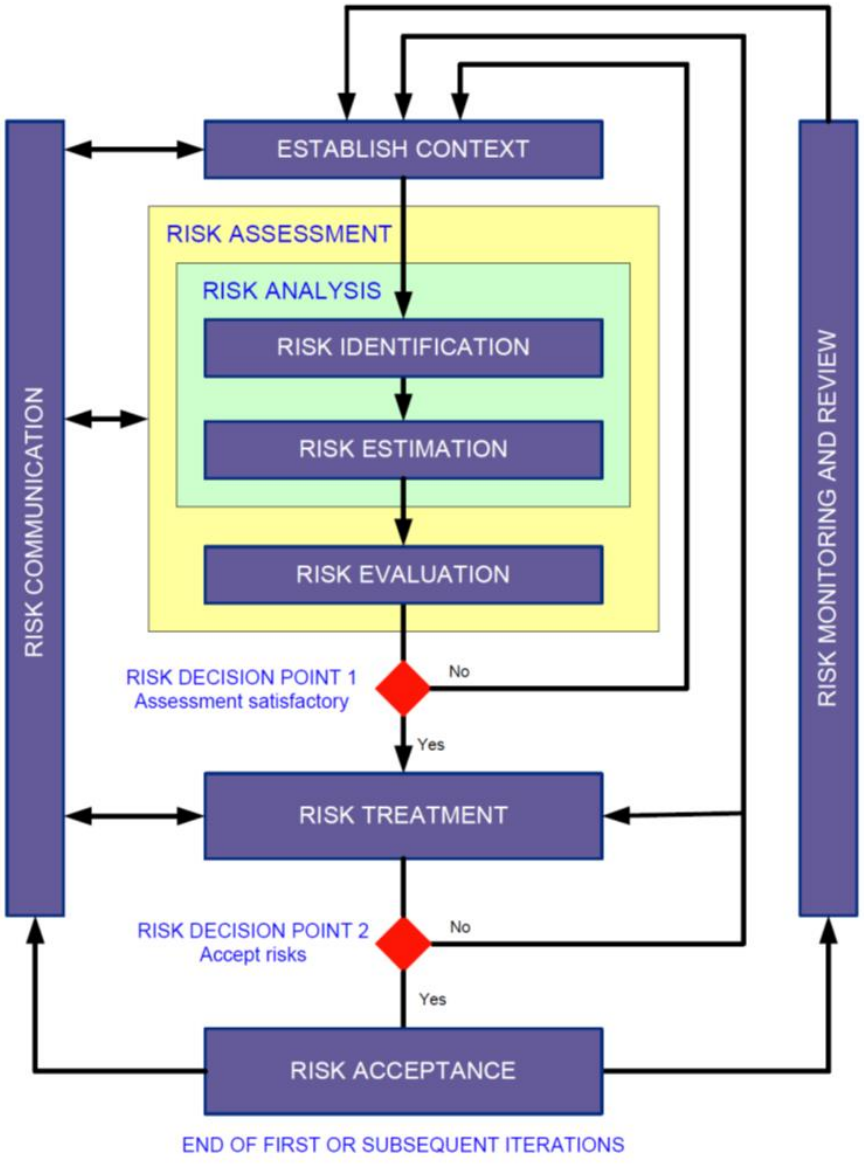

Figure 1 Information security risk management process

Common Criteria

- ISO/IEC 15408 **Common Criteria**
  - Rozsiahly, voľne dostupný štandard pre certifikáciu systémov
  - Bezpečnostné požiadavky na systémy sa formulujú v podobe ST a PP podľa Common Criteria
  - Zaujímavá filozofia, katalógy bezpečnostných funkcií a bezpečnostných záruk, 7 preddefinovaných úrovní (EAL)

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Vydáva dobre spracované, zrozumiteľné, voľne dostupné a použiteľné materiály
- Prepracovaný systém základných požiadaviek na IB : IT Grundschutz, podporený rozsiahlym manuálom a štandardami
- Momentálne 4 BSI štandardy, obsahujúce odporúčania BSI týkajúce sa metód, procesov, procedúr, prístupov a opatrení týkajúcich sa informačnej bezpečnosti
- Sú určené štátnym inštitúciám aj súkromným spoločnostiam
- Zohľadňujú medzinárodné normy
- Okrem štandardov – viacero špecializovaných publikácií, analýz, správ
- https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html

Filozofia BSI pri ochrane IKT

- Analýza rizík je náročná (expertíza, čas, peniaze)
- Organizácie používajú štandardné riešenia (hw aj sw)
- Bezpečnostné podmienky aj požiadavky na IKT sú podobné
- Väčšinou je možné použiť štandardné riešenia (s uspokojivým výsledkom)
- BSI's IT Baseline Protection Manual
  - Bezpečnostná aspekty týkajúce sa celej organizácie (personálna b. riadenie bezp. zálohovanie)
  - Architektúrne a štrukturálne faktory (fyzická bezpečnosť)
  - IT systémy (typické systémy)
  - Siete
  - IT aplikácie (napr. el. pošta, webové aplikácie, databázy)
- Udržiavaný a aktualizovaný
- Modulárny

Štandardy BSI (1)

- **BSI Standard 100-1 Information Security Management Systems (ISMS)**
  - definuje všeobecné požiadavky na ISMS
  - Kompatibilný s ISO/IEC 27001
  - Zohľadňuje aj odporúčania ostatných noriem radu 27000
  - Detailnejšie a metodicky lepšie spracovaný dokument ako ISO normy
  - Kompatibilný s IT-Grundschutz prístupom
- **BSI-Standard 100-2: IT-Grundschutz Methodology**
  - Popisuje, ako zaviesť a prevádzkovať ISMS v praxi
  - Ako vytvoriť bezpečnostnú koncepciu, vybrať vhodné bezpečnostné opatrenia a realizovať bezpečnostnú koncepciu v praxi
  - Kompatibilný s ISO normami radu 27000

Štandardy BSI (2)

- **BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz**
  - Používajú sa štandardné („konfekčné“) bezpečnostné riešenia pre typické systémy so štandardnými nárokmi na IB (založené na katalógu IT-Grundschutz opatrení BSI)
  - Zvýšené/špecifické požiadavky – individuálny prístup
  - Analýza rizík (a návrh opatrení)
  - Štandard obsahuje metodiku pre analýzu rizík
  - Príloha: Katalóg elementárnych hrozieb

- **BSI-Standard 100-4: Business Continuity Management**
  - Systematicky popisuje, ako vyvinúť, zaviesť a udržiavať v organizácii systém na riadenie kontinuity činnosti

National Institute of Standards and Technology, NIST

- Americký štandardizačný inštitút
- V rezorte Ministerstva obchodu
- o.i. zodpovedný za štandardizáciu IB pre oblasť neklasifikovanej informácie
- Od konca 80-tych rokov
- Vydáva štandardy a metodické materiály (zoznam CSD_DocsGuide)
- Primárne určené pre americké štátne organizácie a americké firmy, môžu byť užitočné aj v našich podmienkach
- Do pozornosti
  - NIST Special Publications 800
  - FIPS (Federal Information Processing Standard)
- Menovite SP 800-100 Information Security Handbook: A Guide for Managers

FIPS

- Federal information processing standard
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
- FIPS 140-3 Security Requirements for Cryptographic Modules

NIST SP 800

- cca 150 kvalitných a dostupných materiálov
- Určené pre federálne organizácie, ale aj komerčný sektor
- Americké reálie, ale aj tak sú v mnohom použiteľné
- Nie sú určené pre klasifikované (utajované) informácie a systémy, v ktorých sa tieto spracovávajú
- SP 800 -18 Guide for Developing Security Plans for Federal Information Systems
- SP 800 – 27 Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- SP 800 – 30 Risk Management Guide for Information Technology Systems
- SP 800 – 34 Contingency Planning Guide for Information Technology Systems

NIST SP 800

- SP 800 – 53A Guide for Assessing the Security Controls in Federal Information Systems
- SP 800 – 53 Recommended Security Controls for Federal Information Systems
- SP 800 – 61 Computer Security Incident Handling Guide
- SP 800 – 64 Security Considerations in the System Development Life Cycle
- SP 800 – 83 Guide to Malware Incident Prevention and Handling
- SP 800 – 100 Information Security Handbook: A Guide for Managers
- A iné

Iné

- ITIL Information Technology Infrastructure Library manažment IT služieb z pohľadu poskytovateľa služieb
  - cieľ efektívnosť a kvalita služieb
- Cobit (Control Objectives for Information and related Technology) popisuje metódu monitorovania rizík vznikajúcich pri používaní IKT (ISACA)
- PRINCE 2 - Projects in Controlled Environments (UK), de facto štandard na riadenie projektov

Medzinárodné inštitúcie

- OECD:
  - **The promotion of a culture of security for information systems and Networks in OECD countries**
  - **OECD Recommendation of the Council on the Protection of Critical Information Infrastructures**
- ENISA
  - Zatiaľ skôr prehľady a štúdie
  - http://www.enisa.europa.eu/publications#c2=publicationDate&reversed=on&c5=all&c0=10&b_start=0
- IETF: Vydávajú de facto štandardy pre Internet (RFC)
- ISACA, SANS Institute – de facto štandardy pre vzdelávanie odborníkov v IB
- Iné – napr. RSA laboratories: spravuje štandardy pre PKI (PKCS)

Slovensko

- SÚTN, technická komisia pre IB
- Na dobrovoľnej báze
- Preberáme štandardy do STN
- problémy:
  - Terminologické
  - Kapacitné
  - Ekonomické
- Rozumnejšie je používať medzinárodné štandardy, resp. preberať ich do STN v originále
- Využiť v štandardoch vydávaných št. orgánmi (Výnos o štandardoch ISVS)

* * *

Legislatíva

- Niekoľko špeciálnych zákonov a všeobecné zákony s ustanoveniami relevantnými pre IB
- Utajované skutočnosti
- Kritická infraštruktúra
- Osobné údaje
- ISVS
- Elektronický podpis
- Elektronický obchod
- Slobodný prístup k informáciám
- Autorský zákon
- Telekomunikačný zákon
- Trestný zákon
- ...

EÚ

- Viacero slovenských zákonov vzniklo na podnet EÚ
- ENISA – pokus o prehľad legislatívnych aktov EÚ týkajúcich sa IB
- V súčasnosti 2 zásadné dokumenty:
  - Informačná bezpečnosť (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)
  - návrh Nariadenia o ochrane údajov (General Data Protection Regulation)

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
- V SR pripravovaný Zákon o IB, potrebné by bolo zosúladenie legislatívy a koordinovaný systematický prístup k IB na lokálnej aj globálnej úrovni
- Na samostatné ucelené riešenie nemáme kapacity, budeme sa musieť zapojiť sa do medzinárodnej spolupráce (preberať a upravovať cudzie riešenia)
- EU? Nemecko alebo USA?

* * *