Informačná bezpečnosť a štandardizácia

mim. prof. Doc. RNDr. Daniel Olejár, PhD.,
Univerzita Komenského, Bratislava
olejar@dcs.fmph.uniba.sk

Ľudská spoločnosť a informačné technológie

- Význam spracovania informácií pre systémy (živé, technické aj spoločenské)
- Čím zložitejší systém, tým viac informácií potrebuje a tým efektívnejšie metódy na ich spracovanie musí používať
- Druhá polovica 19. storočia (cenzus v USA) informačné potreby prevyšujú možnosti „ručného“ spracovania
- Koniec 19. a 20. storočie – rozvoj vedy, techniky aj samotnej ľudskej spoločnosti – nutnosť automatizácie spracovania informácií (protilietadlová paľba, operácia Overlord)
- Televízia, telekomunikačné systémy, masmédiá, počítače = synergia zvaná Informačné a komunikačné technológie.
- Paradox: koniec 20. storočia IKT začínajú „žiť vlastným životom“ a prenikajú do oblastí, kde ich nasadenie nebolo vôbec plánované
- Informačná revolúcia ako prostriedok k vytvoreniu postindustriálnej spoločnosti

Informatizácia a informačná bezpečnosť

- IKT prenikli prakticky do všetkých oblastí ľudskej činnosti
- Prebieha informatizácia spoločnosti (= transformácia tradičných informačných procesov tak, aby sa využili možnosti IKT)
- Vzniká digitálny priestor (prepojenosť a závislosť čiastkových systémov)
- Už v súčasnom štádiu informatizácie je prínos IKT pre rozvoj ľudskej spoločnosti nespochybniteľný
- Ale – niet cesty späť. (Na udržanie chodu na existujúcej úrovni spoločnosť potrebuje spracovať také veľké množstvo informácií, že to nie je možné bez IKT)
- Dôsledok: ľudská spoločnosť sa dostala do závislosti od IKT a výpadok, poškodenie, nefunkčnosť IKT môžu mať pre spoločnosť ďalekosiahle dôsledky
- Zaistenie bezproblémového fungovania IKT – úloha informačnej bezpečnosti (v malom – konkrétne IKT, v globálnom meradle – digitálny priestor)

Informačná bezpečnosť a (informačná) spoločnosť

- Rekapitulácia:
  - Bez informačnej bezpečnosti nebudú fungovať IKT; bez fungujúcich IKT nebude nielen informačná spoločnosť, ale nebude fungovať ani tá súčasná:
  - Informačná bezpečnosť je nutným predpokladom fungovania súčasnej spoločnosti a jej ďalšieho vývoja
  - Nestačí chrániť jednotlivé IKT systémy, treba chrániť aj celý digitálny priestor

Čo je vlastne informačná bezpečnosť?

- Ešte sa len utvára, nemá dobre definovaný predmet ani metódy a preto
- všeobecne akceptovaná definícia neexistuje:
  1. Ideálny stav IKT systému, kedy všetko funguje tak ako má
  2. Meziodborová oblasť zaoberajúca sa hľadaním/štúdiom metód ochrany IKT systémov
  3. Praktická činnosť smerujúca k zaisteniu ochrany IKT systémov
- Pozrieme sa na informačnú bezpečnosť tak z historického hľadiska (súčasný stav IB je výsledkom historického vývoja)
- Budeme kombinovať historický a logický pohľad

Čo, pred čím a ako chrániť? (aktíva)

- Všeobecný cieľ: aby IKT systémy spoľahlivo fungovali
- Prečo: potrebujeme výsledky, na ktorých správnosť sa môžeme spoľahnúť
- Čiže: to čo sa má chrániť, je v podstate informácia
- Ale, informácia sa spracováva pomocou IKT systémov (alebo ručne), na jej spracovávaní sa zúčastňujú ľudia, IKT systémy závisia od dodávky elektriny,... je veľa faktorov, ktoré môžu negatívne ovplyvniť spracovanie informácie
- Trocha to usporiadame:
- Aktíva = ľudia, počítače, komunikačné systémy, infraštruktúra, údaje, informácie, programy, dokumentácia, zmluvy, know-how, dobré meno inštitúcie a pod; všetko, čo má pre organizáciu cenu
- Ak má IKT systém (alebo organizácia) fungovať, musia byť aktíva v bezpečnom stave (upresníme neskôr)

Čo, pred čím a ako chrániť? (Hrozby a riziká)

- Akákoľvek potenciálna odchýlka od normálneho (bezpečného) stavu aktíva = hrozba
- Hrozba (threat)
  - Existuje objektívne a nezávisle od aktíva (krádež, zlyhanie, technická porucha, sabotáž, požiar, ľudská chyba, útok hackera/crackera, malware, povodeň, zemetrasenie)
  - Má svojho nositeľa (napr. zlodej, rieka)
  - Aby mohla nastať, musí mať aktívum vlastnosť, ktorá to umožňuje (zraniteľnosť, slabina, vulnerability)
- Naplnenie hrozby voči aktívu má nejaké dôsledky (poškodenie, znefunkčnenie, strata aktíva) – dopad
- Druhý faktor – pravdepodobnosť naplnenia hrozby (pád lietadla, bombový útok)
- Výsledok: riziko (risk) = dopad hrozby x pravdepodobnosť nastatia (stredná hodnota dopadu, očakávaná strata)

Čo, pred čím a ako chrániť? (Opatrenia)

- Vysoké riziko = potenciálny problém je vysoko pravdepodobný a má neprijateľný dopad
- Opatrenia = čokoľvek, čo eliminuje alebo aspoň zníži riziko (uzavretá miestnosť, trezor, vyššie poschodie, školenie zamestnancov, zálohovanie údajov, náhradný zdroj energie, poistenie,...)
- Principiálne je to jasné, ale ako zaistiť bezpečnosť rozsiahleho konkrétneho systému alebo organizácie?
- Doplníme:
- Cieľavedomý pokus o naplnenie hrozby = útok
- Činiteľ, ktorý uskutočňuje útok = útočník
- Útočný potenciál
  - Kvalifikácia útočníka
  - Motivácia
  - príležitosť

Základné bezpečnostné aspekty informácie

- Základ: chránime informáciu
- ale pred čím, resp. čo chceme dosiahnuť?
- A čo to je informácia?
- Ešte potrebujeme rozlíšiť údaje (forma zápisu informácie) a informáciu (obsah údajov)
- Dôvernosť (confidentiality)
  - Zabrániť, aby sa k obsahu údajov (informácii) nedostali nepovolané osoby
- Integrita (integrity)
  - Zabrániť nepozorovanej zmene údajov
- Dostupnosť (availability)
  - Oprávnená osoba musí mať prístup k údajom kedykoľvek o to požiada

Ďalšie bezpečnostné aspekty informácie a bezpečnostné požiadavky

- Autentickosť (authenticity) autorstvo a integrita
- Súkromnosť (privacy)
  - Osoba má možnosť rozhodnúť, kto bude mať a aký prítup k údajom, ktoré sa jej týkajú
- Anonymnosť (anonymity)
- Nepopretie pôvodu (non repudiation of origin)
- Nepopretie prijatia (non repudiation of receipt)
- Zodpovednosť (accountability) určenie osoby, ktorá vykonala danú činnosť v systéme

Od *ad hoc* riešení k štandardom (historické skúsenosti)

- Špecifické oblasti – dlhá tradícia (fyzická ochrana majetku, protipožiarna ochrana a i.)
- Ochrana informácií
  - dôvernosť (vojaci, diplomati, politici) spoľahlivé komunikačné kanály, steganografia, šifrovanie
  - Integrita (samoopravné kódy) od roku 1948
- Počítače a neskôr globálne IKT – nová výzva
- Najprv pokus o tradičné riešenia (fyzická ochrana prístupu, personálna bezpečnosť, presne definované postupy) – ťažko presaditeľné v civilnom prostredí
- Nekompatibilné, neopakovateľné riešenia
- Vzrastajúci počet a rozsah systémov, potreba „konfekčných“ riešení

Od *ad hoc* riešení k štandardom
(od Orange book a Rainbow series po CC)

- Líder: USA (dve inštitúcie NIST a NSA)
- Americký NIST sa zameral na dva kľúčové smery
  - návrh noriem pre počítačovú kryptografiu a
  - noriem pre vytváranie a hodnotenie zabezpečených počítačových systémov.
- Americké DoD prostredníctvom NSA – Trusted Computer System Evaluation Criteria (1983) kritériá pre hodnotenie dôveryhodnosti (stupňa zabezpečenia) hodnoteného systému
- Neskôr Rainbow series (cca 30 dokumentov)
- Ďalšie národné kritériá (Kanada, Japonsko, Nemecko, GB. Francúzsko)
- ITSEC – harmonizované kritériá (európske, 1991)
- Common Criteria (1995), neskôr ISO/IEC 15408

Úloha štandardu ISO/IEC 15408

- Zohľadnil pozitívne skúsenosti predchádzajúcich štandardov
- Účel:
  - Posudzovanie bezpečnosti IKT systémov alebo produktov
  - Základ pre návrh bezpečných riešení (systémov, sw aplikácií)
- Protection Profile, Security Target, funkcionálne bezpečnostné požiadavky, požiadavky na bezpečnostné záruky, EAL 1-7
- Na čo sú dobré certifikované produkty
- PP ako bezpečnostný model budúceho riešenia
- Nadviazali naň ďalšie štandardy (CMM-Capability Maturity Model) ale najmä sa presadila jeho filozofia pri návrhu bezpečnostných riešení
- Veľmi rozsiahly, dostupný na adrese
- http://www.commoncriteriaportal.org/

Iné zaujímavé bezpečnostné štandardy (ISO)

- CC je skôr pre špecialistov, potrebujeme praktickejšie orientované štandardy; také existujú
- ISO: JCT1 SC 27 spravuje 80 bezpečnostných štandardov, cca 50 je hotových, ostatné vo vývoji, 5 subkomisií
  - WG1- Information Security Management Systems
  - WG2- Cryptography and security mechanisms)
  - WG3- Evaluation Criteria of Information Security
  - WG4- Security controls and services
  - WG5- Identity Management and Privacy Technologies
- http://www.iso.org/iso/iso_technical_committee?commid=45306
- V SR existuje SK 27 Technickej komisie 37 STN, ktorá sa zaoberá štandardami v informačnej bezpečnosti a spolupracuje s príslušným podvýborom (SC 27) ISO
- SK 27 navrhla prebrať do STN 10 ISO štandardov v originálnom znení

Iné zaujímavé bezpečnostné štandardy (BSI.gb a BSI.de)

- Britský štandardizačný inštitút vydal BS 7799, zameraný na systém riadenia informačnej bezpečnosti
- Čo treba spraviť na to, aby organizácia dlhodobo a efektívne zaisťovala potrebnú úroveň informačnej bezpečnosti
- Neskôr ISO/IEC 17799, teraz séria ISO/IEC 270xx
- ďalšie štandardy BSI venované zaisteniu kontinuity činnosti pripravujeme na prevzatie do STN
- Nemecký Federálny úrad pre informačnú bezpečnosť (BSI)
  - BSI Standard 100-1 Information Security Management Systems
  - BSI Standard 100-2 IT Grundschutz Methodology
  - BSI Standard 100-3 Risk Analysis based on IT Grundschutz
  - IT Security Guidelines
- http://www.bsi.de/english/publications/bsi_standards/index.htm

Iné zaujímavé bezpečnostné štandardy (NIST)

- FISMA (the Federal Information Security Management Act of 2002) – bezpečnosť neklasifikovaných informačných systémov v USA
- z výročnej správy NIST
  - Affected customer organizations include federal, state, and local governments, the healthcare community, colleges and universities, small businesses, the private sector, and the international community.
  - We continued to develop standards, metrics, tests, and validation programs to promote, measure, and validate security in systems and services.
  - We also developed guidance to increase secure IT planning, implementation, management, and operation.
- Kde: FIPS a SP-800
- http://csrc.nist.gov/

Štandardizácia v informačnej bezpečnosti na Slovensku - 1

- Prečo potrebujeme štandardy:
  - Dobre premyslené riešenia (načo vymýšľať horšie)
  - Kompatibilita (doma i v zahraničí)
  - Legislatíva nestačí
- Normy a štandardy
  - SÚTN – normy (medzinárodné) – STN
  - de facto štandardy (RFC, PKCS,...)
  - Štandardy ministerstvá a štátne orgány (NBÚ, ÚOOÚ, MF SR a i.)
- Roztrieštenosť, nekoordinovanosť
- Stratégia informačnej bezpečnosti (2008) – koordinácia ochrany celého digitálneho priestoru, vrátane štandardizácie, zodpovedné MF SR
- Záujem má aj NBÚ – kybernetický priestor (Zákon o ochrane utajovaných informácií ...)
- Podobná situácia vo svete (NSA a NIST, BSI,...)

Štandardizácia v informačnej bezpečnosti na Slovensku - 2

- Čo máme:
  - Niekoľko medzinárodných noriem v STN
  - Špecifické a nekompatibilné štandardy vydané rozličnými štátnymi orgánmi
- Po prijatí Stratégie, MF SR – systematický postup
  - Výnos k Zákonu o ISVS (bezpečnostné štandardy vychádzajú z medzinárodných noriem)
  - Štúdia o stave noriem a štandardov v informačnej bezpečnosti v SR a vo svete
  - Výkladový slovník Informačnej bezpečnosti (1400 termínov)
  - Terminologický slovník pre informatizáciu spoločnosti
  - Terminologická komisia
  - Spolupráca (personálne prepojenie) na komisiu SUTN
  - Legislatíva (vyhlášky NBÚ, zákon o kritickej infraštruktúre, zákon o utajovaných informáciách)
  - Nie vždy sa to stretáva s pochopením

Štandardizácia, vzdelávanie a metodiky

- nedostatok informácií a prebytok informácií = nevedomosť
- *Need to know principle* – každému to, čo potrebuje
- Príklad BSI, NIST, nakoniec aj ISO
- Štandardizácia potrebuje spätnú väzbu (príliš zložitým štandardom nebude nikto rozumieť a nebudú sa používať)
- Primeraná forma, vzdelávanie používateľov, metodické materiály
  - Stratégia,
  - Koncepcia vzdelávania,
  - Terminologická komisia a ďalšie aktivity MF SR,
  - snaha o spoluprácu so všetkými zainteresovanými (štátne orgány, súkromný sektor, školy, medzinárodné organizácie)

* * *