BIZTONSÁG MENEDZSMENT

Tárgy:	Szolgáltatás menedzsment
Kód:	NIRSM1MMEM
Kredit:	5
Szak:	Mérnök Informatikus MSc (esti)
Óraszám:	Előadás: 2/hét Laborgyakorlat: 2/hét
Számonkérés:	Vizsga, (félévi 1db ZH)

A biztonság és problémái

- **Az Internetet megalapozó technikák kidolgozásakor nem gondoltak a biztonság kérdésére – „foltozgatás”**
- **Megbízhatóság (sebezhetőség?) – Reliability**
  - Az egyre növekvő rendszer egyre több ponton romolhat el
  - Egy adott pont jelentősége hihetetlen mértékben megnövekedhet
  - Az Internet egyre több szolgáltatás alapját képezi
- **Biztonság – Security**
  - Az Internet egyre több (érzékeny) adat tárháza, fontos szolgáltatás helyszíne
  - Egyre több támadási pont, egyre fejlettebb támadó eszköz, egyre jobb búvóhely
  - Új támadási módok születnek (pl. WiFi, HotSpot)
  - A probléma hólabdaként növekszik
    – CERT adat: támadások évente duplázódnak
  - A támadások mögött sokszor gazdasági/politikai előnyszerzés áll

Informatikai biztonság kérdései

- Az informatikai biztonság összefügg a szervezet- és vagyonbiztonsággal
- Biztonság – megkívánt (normál) állapot fenntartása, de a biztonság elérése folyamatos tevékenységet követel
  - Megelőző intézkedések (Prevenció)
  - Felismerő tevékenységek (Detekció)
  - Kijavító műveletek (Korrekció)
- Mit tekintünk normál állapotnak? – Control Objectives
- A kontrollcél nem egy technikát, hanem egy célt jelöl ki
  - ~~Backup-olni kell~~ – minden adatról készüljön biztonsági másolat
- A biztonság nem másodlagos kérdés – megfelelő hatáskör
- A biztonsági döntések „pártatlansága” érdekében (anyagilag is) független működés garantálása

Biztonságos IT működés elérése

- A normál állapot elérését csak hosszas előkészületek után remélhetjük – ez a folyamatot a „biztonságszervezés”
- Első lépés – Helyzetfelmérés, mi működik már, mi nem?
  - A jelen helyzet megfelel a kontrollcéloknak?
  - A gyakorlat összhangban áll a szabályzatokkal, szakmai elvárással?
- A helyzetfelmérés feltárta gyakori problémák:
  - Biztonsági célok nincsenek megfogalmazva (missing contol objectiv)
  - Hiányos (vagy nem létező) szabályzatok (missing control)
  - A szabály(zat)okat nem (vagy alig) ellenőrzik (inadequate control)
  - A gyakorlat (esetleg tudatosan) eltér az életben lévő szabályozástól
  - Az It rendszer technikai veszélyekkel terhelt (bizt. lyuk, security flaw)
- A felmérés eredményeit részletes elemzésnek kell alávetni

IT veszélyforrások feltárása

- A felmérés alapján felállítható a veszélyforrások listája
  - A lista soha se lesz teljes, de a lényeges kérdések azonosíthatók
  - A kimaradt (minimális) elemekre „maradék kockázat”-ként tekintünk

- Veszélyforrások csoportosítása
  - Szervezési gyengeségek (szervezési hiányosságokból eredő veszélyek),
  - Természeti veszélyforrások (tűz, csőtörés, villám, földrengés, stb),
  - Fizikai veszélyek (betörés, lopás, rongálás, terrortámadás, stb.),
  - Logikai fenyegetések (IT csalás, hálózati betörés, lehallgatás, stb.),
  - Emberi veszélyforrások (hanyagság, gondatlanság, visszaélés)