BIZTONSÁGPOLITIKA, BIZTONSÁGI SZABÁLYZAT

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

IT Biztonság definíciója

- **Informatikai biztonság alatt valamely informatikai rendszer azon állapota értendő, amelyben a kockázatokat – amelyek ezen informatikai rendszer bevezetésekor a fenyegető tényezők alapján adottak – elfogadható intézkedésekkel elviselhető mértékűre csökkentettük.**
- **A biztonság nem állapot, hanem folyamat** (Bruce Schneier)
- Az IT biztonság megteremtésének alapvető eszközei
  - IT Biztonságpolitika – hosszabb távú célkitűzések, statikus
  - IT Biztonsági Szabályzat (IBSZ) – folyamatos követő változtatások
- Az IT biztonsági feladatok fenti megosztása átláthatóbbá, hatékonyabbá teszi az IT menedzsment folyamatát.
  - Mivel kijelöli a vezetőség és a végrehajtók elkülönült feladatait.

IT Biztonságpolitika

- Biztonságpolitika – kidolgozója/jóváhagyója = felsővezető/CEO
  - Biztonsági alapelvek megfogalmazása
  - Vezetői feladatok definiálása
- Nem foglalkozik a megvalósítás részleteivel, hanem
  - Meghatározza a védekezés által elérendő célokat
  - A célok eléréséhez szükséges főbb vezetői teendők mibenlétét
  - Rendelkezik a kockázatok áthárításának mikéntjéről
    - Biztosítás, avagy felelősség áthárítás vevő/beszállító partnerre
      - Biztosítás ritka, mert nehéz a kárt előre számszerűsíteni
      - Az előzetes felmérések komoly szaktudást igényelnek (pl. min. védelem meghat.)
      - Nehezen bizonyítható a káresemény bekövetkezte (nem szándékos volta)
  - Azonosítja a felvállalt (már ismert) kockázatok körét
- Bonyolult feladat, könnyű teljesíthetetlen célokat kitűzni
  - A lehetetlen célok kitűzése rontja a végrehajtás hatékonyságát
  - A túlzott igények elvárása határtalanul megnöveli a költségeket

IT Biztonsági Szabályzat (IBSZ)

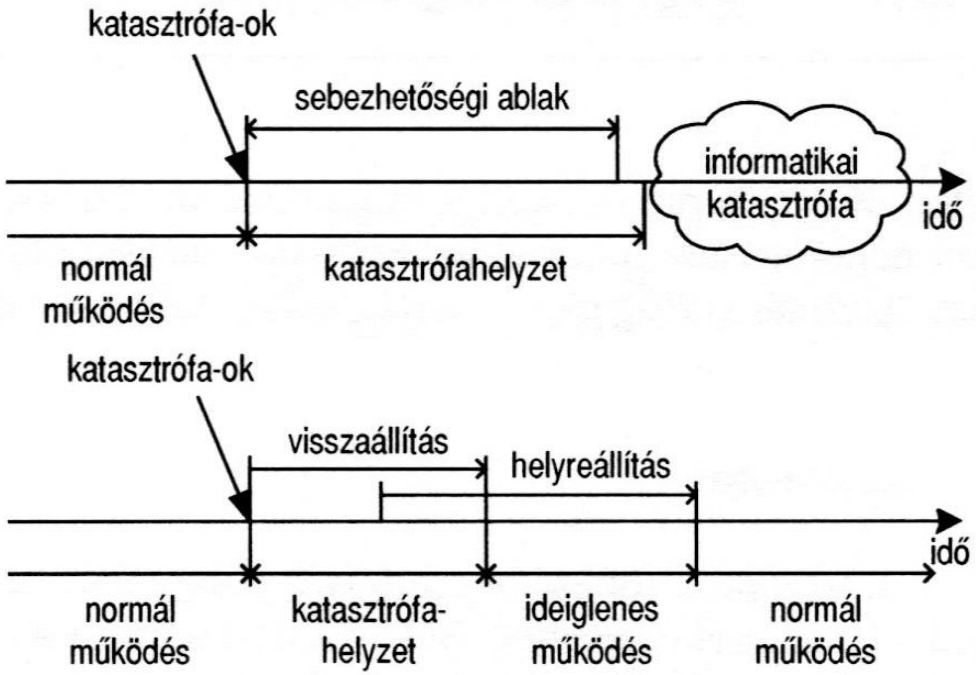
- Informatikai Biztonsági Szabályzat (IBSZ)
  - Utasítás szintű konkrét feladat meghatározások
  - Széleskörű szakmai ismereteket feltételez, folyamatosan módosul
  - Rendelkezik a szabályok betartásának (kül/bel-ső) ellenőrzéséről is
  - IT munkaköröket definiál (Szervezeti Szabályzatban is definiálni!)
  - Szervesen illeszkedjen a vállalat egyéb szabályozási rendszerébe
- Az IBSZ kialakítását befolyásoló tényezők
  - Adatvédelmi törvények, irányelvek
  - Ágazati, tárcaszintű elvárások, utasítások (pl. titoktartási elvárások)
  - Műszaki szabványok, normatívák, rendeletek
  - Helyi (házi) szabályzatok, szokások

Az IBSZ tartalma

- Csak általános kitételek adhatók, helyi viszonyok függvénye
  - Rendelkezzen az IBSZ minősítéséről – titkos, nyilvános, stb.
  - Határozza meg az IBSZ hatókörét (HW/SW/szervezet egységek)
  - Rendelkezzen a kapcsolódó szabályozások köréről
  - Határozza meg az egyes elemek konkrét védelmi intézkedéseit
    - Infrastruktúrához kapcsolódó (fizikai védelem, áramellátás …)
    - Hardverekhez kapcsolódó (csere, tárolás, spec. eszközök kezelése …)
    - Adathordozókhoz kapcsolódó (backup stratégia, nyilvántartási rend …)
    - Dokumentumokhoz kapcsolódó (leírások, logok, felhasználói adatok …)
    - Szoftverekhez kapcsolódó (verzióváltás, vírusellenőrzés, programfejlesztési/tesztelési előírások …)
    - Adatokhoz kapcsolódó (személyes adatok kezelése, adatellenőrzés …)
    - Kommunikációhoz kapcsolódó („adatzsilipelés”, adat ki/be szállítás …)
    - Személyekhez kapcsolódó (felelősségi körök, munkafolyamatok …)
  - Definiálja az üzemeltetés folyamatait, munkaköreit, felelősségeit

IT Katasztrófák elhárítása

- Tekintettel fontosságára, külön irányelvek vonatkoznak rá
  - Előzetes felkészülés nélkül pánikhelyzet alakulhat ki
- Néhány alapvető fogalom magyarázata



Informatikai katasztrófa bekövetkezése

Informatikai katasztrófa elhárítása

Katasztrófákkal kapcsolatos fogalmak

- Katasztrófa-ok – Azon ok, melynek hatására a rendszer normál működése leállhat, ha nem teszünk semmit
- Katasztrófa helyzet – Katasztrófa-ok bekövetkeztétől a minimális működés visszaállításáig eltelt időszak
- Informatikai katasztrófa – IT rendszer működése annyira sérül, hogy az üzleti folyamatok elviselhetetlen károkat szenvednek
- Visszaállítás (Recovery) – a legkritikusabb, minimálisan szükséges rendszerműködés legrövidebb időn belüli visszaállítása
- Helyreállítás (Restoration) – a teljes informatikai rendszer normál működési állapotának helyreállítása
- Sebezhetőségi ablak – az az időszak, ameddig az IT rendszer leállása/degradációja elviselhetetlen üzleti következmények nélkül tolerálható

Katasztrófa-elhárítási módszertanok 1

- **DRP – Disaster Recovery Plan**
  - Katasztrófa-elhárítási terv IT rendszerek védelmére, hangsúlyai:
    - megelőző intézkedések (pre disaster activities) halmaza
    - katasztrófahelyzetben végzett visszaállító tevékenységek (disaster recovery activities) halmaza
    - katasztrófahelyzet elhárítását követő helyreállításra (post disaster activities) koncentrálnak;
    - kiegészítő tevékenységek halmaza (követelmények feltérképezése, katasztrófa-elhárítás tesztelése, oktatás, rendszeres karbantartás)
- **BCP – Business Continuity Plan**
  - DRP-n túl ideiglenes üzleti folyamatokat is definiál a sebezhetőségi ablak megnyújtása érdekében
- **BRP – Business Recovery Plan**
  - Hasonló a BCP-hez, de annál kevésbé terjed ki az üzleti folyamatokra

Katasztrófa-elhárítási módszertanok 2

- **BIA – Business Impact Analysis**
  - Üzleti hatásmechanizmus elemzés, célja az üzleti folyamatok IT-től függésének megállapítása, vagyis az egyes alkalmazásokkal szemben támasztott sebezhetőségi ablak meghatározása (ideje)
  - Másként: az IT rendszer legrosszabb visszaállítási ideje esetében milyen hatások várhatók az üzleti folymatokban
- **Backup-Recovery Strategy** – Mentés-Visszaállítás Terv
  - Biztonsági mentések ütemezésével kapcsolatos döntés-halmaz
  - Eldöntendő kérdések (minden rendszerre külön-külön):
    - mentés ideje, időtartama
    - gyakorisága
    - visszaállítás ideje, időtartama
    - adatvesztés mértéke (ha van)

Katasztrófa-elhárítási terv

- Katasztrófa-elhárító módszertanok végeredménye
- Katasztrófahelyzettel kapcsolatos legfontosabb teendők
- Minimális tartalma (napra-készen aktualizálva!):
  - Katasztrófa-elhárításban résztvevők meghatározása (adataik!)
  - Felelősségi, döntési jogkörök meghatározása
  - Felkészülési tevékenységek definiálása
    - biztonsági mentés stratégia, tartalék eszközök listája
  - Visszaállítási tevékenységek meghatározása
    - ki jogosult a katasztrófahelyzet elrendelésére, riadóztatási lánc, visszaállítás ütemterv, minimálisan szükséges funkciók/szolgáltatások listája, visszaállításhoz szükséges konkrét információk/technikai adatok, ellenőrző lista (check list) az újraindítás megfelelő elvégzésének eldöntéséhez.
  - Helyreállítási tevékenységek meghatározása
    - a helyreállítandó funkciók, szolgáltatások listája, a helyreállításban részt vevő személyek és feladataik, adatvesztés pótlásának, az adatbázisok konzisztencia-biztosításának módja
  - Tesztelési útmutató
  - Oktatási terv
  - Karbantartási terv

Tesztelés, oktatás, karbantartás

- Tesztelés
  - A katasztrófa-védelmi terv tesztelés nélkül értéktelen
  - Ezért el kell érni a tervek gyakorlati ellenőrzését
  - Ez nehézségekbe ütközhet, mivel nincs teljes értékű pót-rendszer
  - A teszt menetét (egyes lépések idejét) dokumentáljuk elemzésekhez
- Oktatás
  - A K-V terv tartalmát meg kell ismertetni az érintettekkel
  - Az oktatás segít a tudatosság, a biztonsági szemlélet kialakításában
- Karbantartás
  - A K-V terv folyamatos aktualizálása létkérdés
  - Minimálisan ½-1 évenként felül kell vizsgálni
  - A teljes felülvizsgálat ellenőrzése felsővezetői kompetencia