Biztonság alapvető fogalmak

Számítástechnika tanár szak

Rendszertechnika II.

előadás

Biztonság

- A biztonság fogalma
  - Adatbiztonság
  - Szolgáltatás biztonsága
  - Security (titkosítás)
  - Fizikai biztonság

Fizikai biztonság

- Az üzemeltetés során felmerülő problémák azon együttese, melyek szándékos vagy tőlünk független történések, de az adatok és használt rendszerek biztonságával, ha úgy tetszik a hardver-eszközök biztonságával kapcsolatosak.
  - Fizikai hozzáférés
  - Lopás
  - Elemi károk (tűz, villám, stb.)

Szerverszoba kialakítása

- Megfelelően kialakított, zárható ajtó
- Klimatizáció
- Automatikus tűzjelzés, tűzoltó készülék(ek)
- Riasztó
- Telefon
- Saját főkapcsoló, biztosítékok, vészvilágítás
- Antisztatikus burkolat
- Ablakok védelme

Szerverszoba kialakítása

- Bőséges hely a szükséges eszközöknek
  - Kiszolgálók
  - Szünetmentes tápegység
  - Hálózati eszközök
- Kamerás megfigyelés
- Kerülendő
  - Munkahely kialakítása
  - Felesleges eszközök tárolása (raktár)
  - A szerverszoba helyének jelzése

Szoftver biztonság

- Általános szoftveres biztonsági hibák toplistája (FBI / SANS / NIPS):
  - Alapértelmezetten installált operációsrendszerek és programok
  - Felhasználói nevek jelszó nélkül, vagy gyenge jelszavakkal
  - A mentések hiánya, vagy gyengeségei
  - A nyitott portok nagy száma
  - Az érvénytelen ki vagy bemenő című csomagok szűrésének hiánya
  - A naplózás hiánya, vagy gyengeségei
  - Törhető CGI programok

Szoftver biztonság

- A leggyakoribb biztonsági hibák a UNIX-okon:
  - puffer túlcsordulások az RPC (Remote Procedure Call) szolgáltatásokban
  - Sendmail (levelezőrendszer) hibák
  - BIND (Berkeley Internet Name Daemon) gyengeségek
  - „R" parancsok (rlogin, rsh, rexec, stb.)
  - LPD (Line Printer Daemon)
  - sadmind (system admin daemon) és mountd (mount daemon)
  - alapértelmezett SNMP (Simple Network Management Protocol) sorok

Felügyelet

- Jólképzett rendszer adminisztrátorok
- Vállalati hierarchia és szabályzatok
- Felhasználók tájékoztatása, oktatása
  - Rendszer használatáról
  - A rájuk leselkedő veszélyekről
  - A jelszavak fontosságáról
  - A hanyagság következményeiről
- Felhasználók szankcionálása

Adatbiztonság

- Mentés
  - Rendszer mentése
  - Felhasználói állományok mentése
- Automatizált mentések
- Mentések megfelelő tárolása
- Feleslegessé vált archívum megsemmisítése
- Naplózás (journaling) alkalmazása az adatok fájlrendszerén (ResierFS, Ext3)

Adatbiztonság - RAID

- **R**edundant **A**rray of **I**nexpensive **D**isks
- **R**edundant **A**rray of **I**ndependent **D**isks

- Hozzáférési idők minimalizálása
- Adatvesztés kockázatának minimalizálása
- Szoftveres vagy hardveres megoldás
- hotplugable disks

RAID szintek

- **RAID 0** - striping (darabolás)
- **RAID 1** - mirroring (tükrözés)
- RAID 0+1
- RAID 2
- RAID 3
- RAID 4
- **RAID 5**
- RAID 6

Ami ellen a RAID sem véd …

- Áramszünet, tápegység hiba
  - Cache tartalma elveszik
  - Félbemaradt írási műveletek
- Lemez meghibásodása
- Egyidejűleg több lemez meghibásodása
- Vezérlők meghibásodása
- Elemi csapások
- Szoftverhibák

Erőforrás-hozzáférési kontroll

- A minimális jogosultság elve
- /etc/security/limits.conf
  - `domain` - ki(k)re vonatkozik az adott szabály
  - `type` - korlátozás típusa (soft, hard)
  - `item` - korlátozandó erőforrás
  - `value` - a korlátozás (item) értéke
- Kvóta (quota)
- Szolgáltatásokhoz való hozzáférés

Rendelkezésre állás

- Erőforrások mindenkori elérhetősége
- Uptime
- 24 órás szolgáltatások
- Üzemszerű leállások
- Hálózat rendelkezésre állása

- Optimális megoldás?

Gazdaságos biztonság

- A biztonság plusz költséget jelent
- A gépidő mint költségtényező
  - Ingyenes szoftveres megoldások vs.
  - Hardveres megoldások
- Meddig éri meg növelni a biztonságot?

  → Amíg a rendszerben lévő komponensek (szolgáltatások, adatok, stb.) védelme még megéri.

Biztonság és …

- Teljesítmény
  - Gyakran csak a teljesítmény rovására növelhető
  - Ezért sem érdemes túlbiztosítani a rendszert
- Kényelem
  - Nehezítheti a normál munkavégzést
  - Csökkentheti annak hatékonyságát
  - Felhasználó keresi a kényelmesebb kerülőket

Mentés és archiválás

- Mentés
  - Rövid tárolási idő (néhány nap vagy hét)
  - Több példányban és generáció megőrzése
- Archiválás
  - Hosszú tárolási idő
  - Speciális eszközök és szoftverek
  - Több generáció és példány megőrzése
- Mentési és archiválási szabályzat!
- Dokumentálás, naplózás, tárolás.

Biztonsági minősítések

- **ITSEC** (Information Technology Security Evaluation Criteria)
- **TCSEC** (Trusted Computer System Evaluation Criteria)
- **CCITSE** (Common Criteria for Information Technology Security Evaluation), vagy ismertebb nevén **CC** (Common Criteria)

Ki vagy mi ellen védekezzünk?

- **Véletlenek, (a)vagy hozzá nem értés**
- **Ártó szándékú programok**
  - **Vírus**
  - **Makró-vírus**
  - **Trójai programok**
  - **Férgek**
  - **Kiskapu**
- **Ártó szándékú emberek**

Támadások fajtái

- Megszakítás (Interruption)
- Elfogás (Interception)
- Módosítás (Modification)
- Gyártás (Fabrication)

- Passzív: elfogás
- Aktív: megszakítás, módosítás, gyártás

Támadások fajtái