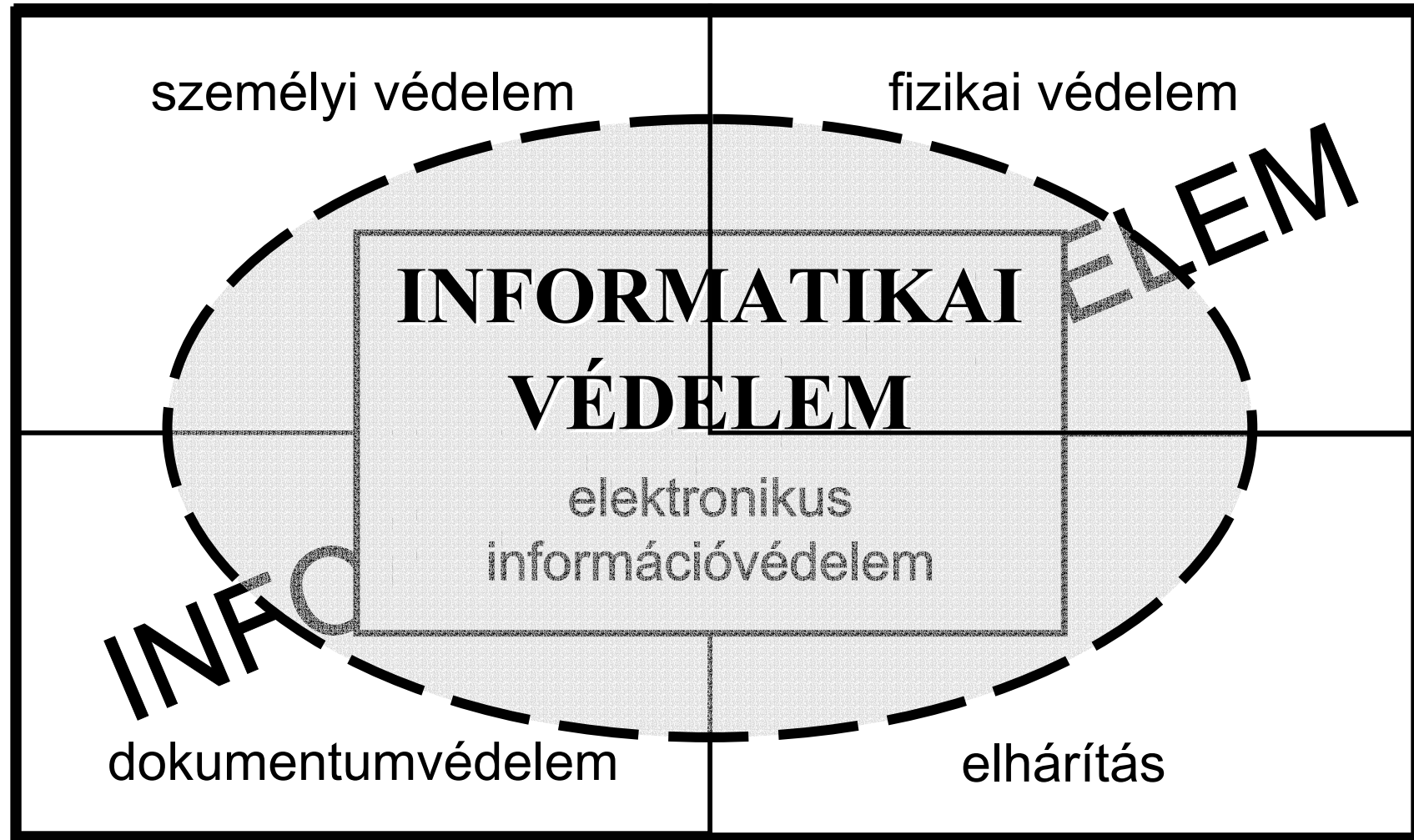


ROBOTHADVISELÉS 8.

Az információbiztonság egy lehetséges taxonómiája

Muha Lajos PhD, CISM
egyetemi docens
ZMNE BJKMK IHI Informatikai Tanszék

Előszó



Előszó

A **rendszer**tan, idegen szóval **taxonómia** (görög taxis = rend és nomos = törvény) vagy a dolgok hierarchikus osztályozására, vagy az osztályozás alapjául szolgáló elvekre vonatkozik. Matematikai értelemben a dolgok egy halmazának faszerkezetű osztálybesorolásai vagy kategorizálása.

ROBOTHADVISELÉS 8.

Az informatikai biztonság egy lehetséges rendszerterana

Muha Lajos PhD, CISM
egyetemi docens
ZMNE BJKMK IHI Informatikai Tanszék

Előszó

Prof. Dr. Munk Sándor:

INFORMÁCIÓBIZTONSÁG VS. INFORMATIKAI BIZTONSÁG

2007. november 27., ROBOTHADVISELÉS 7. konferencia

„a terminológiai kérdések vizsgálata során a megnevezéssel szemben a tartalomnak van elsődlegessége”

Előszó

„Információbiztonság területén a dokumentumok, jogszabályok, publikációk és egyéb források (pl. szabványok, ajánlások, kézikönyvek) eltérő szakkifejezéseket alkalmaznak, mutatva, hogy hazánkban még nem alakult ki egységes nyelvezet. A magyar katonai terminológia információbiztonság területén kidolgozatlanak ... tekinthető, aminek következménye a doktrínákban tapasztalható fogalmi pontatlanság.”

KASSAI Károly: A magyar honvédség információvédelmének feladatrendszere

Előszó

A Magyar Akkreditációs Bizottság (MAB) 2004. júliusában az akkreditációs útmutató 1.sz. mellékletében kötelező „főtantárgyként” írta elő a mérnök informatikus képzésben az informatikai biztonság alapjainak oktatását.

Oktatjuk !!!

De mit???

Az informatikai rendszer

Az adatok gyűjtésére, felvételére, tárolására, feldolgozására (megváltoztatására, átalakítására, összegzésére, elemzésére, stb.), továbbítására, törlésére, hasznosítására (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozására használt elektronikus eszközök, eljárások, valamint az üzemeltető és a felhasználó személyek együttese.

Az informatikai rendszer

- az informatikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
- a vezetékes, a mobil, a rádiós és műholdas távközlés;
- a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
- a rádiós vagy műholdas navigáció;
- az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
- a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

SCADA = Supervisory Control and Data Acquisition

Az informatikai védelem

A rendszerben kezelt adatok bizalmosságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának védelme.

Adatkezelés

Az alkalmazott eljárástól függetlenül a adatok gyűjtése, felvétele, tárolása, feldolgozása (megváltoztatás, átalakítás, összegzés, elemzés, stb.), továbbítása, törlése, hasznosítása (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozása.

A védelem feladatai

1. megelőzés és korai figyelmeztetés
2. észlelés
3. reagálás
4. incidens vagy krízis menedzsment

Az informatikai biztonság

Az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

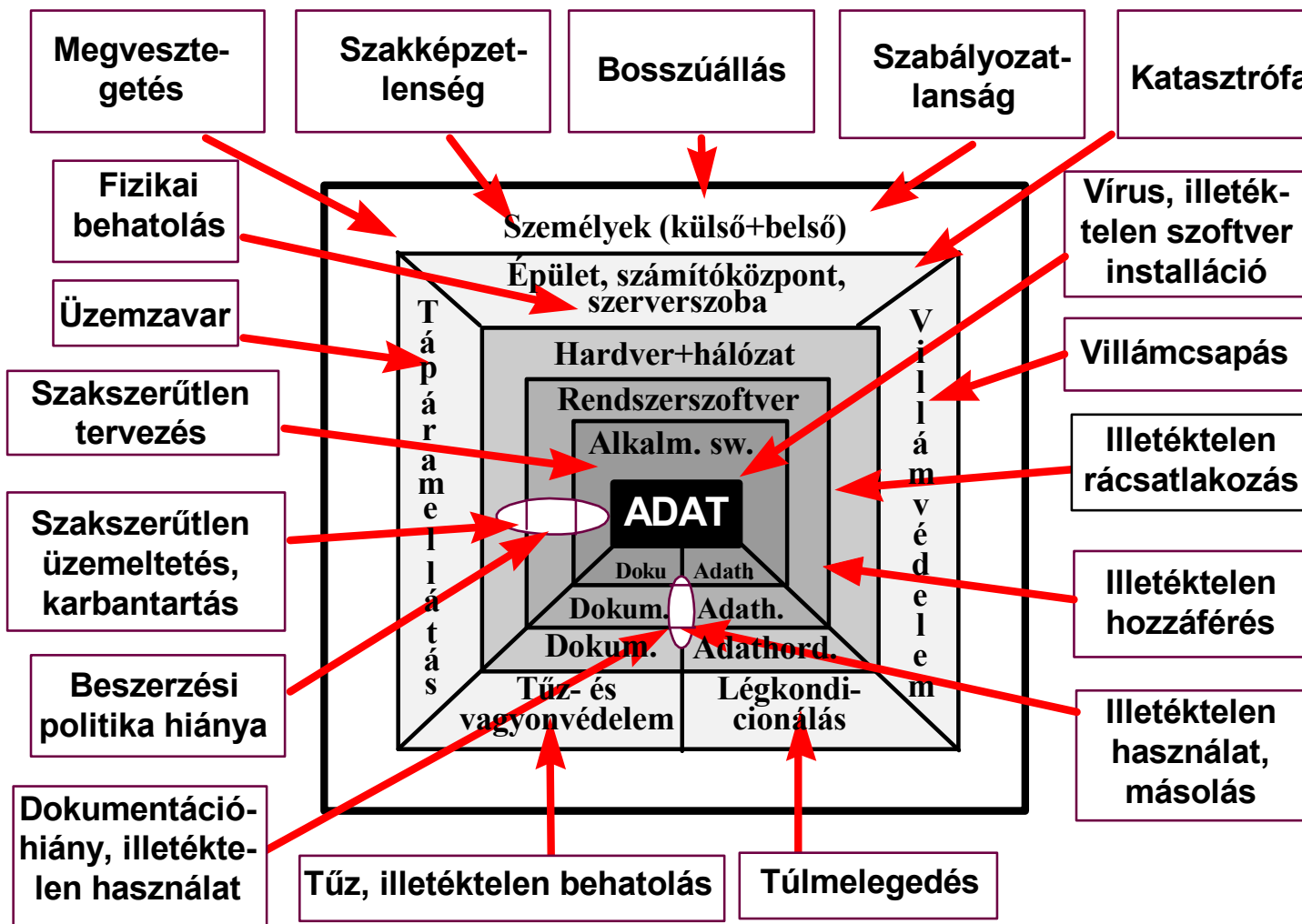
A biztonság összetevői

- **Zárt védelem:** az összes releváns fenyegetést figyelembe veszi;
- **Teljes körű védelem:** a rendszer valamennyi elemére kiterjed;
- **Folytonos védelem:** az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul;
- **Kockázattal arányos védelem:** egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

A biztonság összetevői

- **Zárt védelem:** az összes releváns fenyegetést figyelembe veszi;
- **Teljes körű védelem:** a rendszer valamennyi elemére kiterjed;
- **Folytonos védelem:** az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul;
- **Kockázattal arányos védelem:** egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

ZÁRT és TELJES KÖRŰ



Rendszerelemek

1. az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra;
2. hardver;
3. szoftver;
4. kommunikáció és hálózat;
5. adathordozók;
6. szabályozás és dokumentáció;
7. személyek.

1. fizikai környezet és infrastruktúra

1. építészeti (statikai) védelem;
2. tápáramellátás;
3. klimatizálás;
4. tűzvédelem;
5. vagyonvédelem;
6. vízvédelem;
7. ki- és besugárzás elleni védelem.

hardver

1. hibatűrés;
2. funkcionális redundancia;
3. ki- és besugárzás elleni védelem.

szoftver

1. azonosítás és a hitelesítés;
2. hozzáférés-jogosultsági és ellenőrzési rendszer;
3. rosszindulatú programok elleni védelem;
4. biztonságos programozás;
5. adatbázis biztonság.

kommunikáció és hálózat

1. kriptográfia és biztonsági protokollok:

rejtjelzés; digitális aláírás; SSL; VPN; WiFi;

2. Hálózatszegmentálás:

routerek; switchek; WAP; DMZ;

3. Határvédelem:

tűzfalak; behatolás érzékelők és elhárítók;
rosszindulatú programok elleni védelem.

adathordozók

1. adatredundancia;

2. kriptográfia és kódolás:

rejtjelzés; digitális aláírás; hibadetektáló és javító kódok; tömörítő kódok;

3. kezelés:

nyilvántartás; címkézés; tárolás.

szabályozás és dokumentáció

1. szervezeti biztonság;
2. személyi biztonság;
3. az eszközök biztonsági besorolása és ellenőrzése;
4. fizikai és környezeti biztonság;
5. számítógépes hálózati szolgáltatások és az üzemeltetés menedzsmentje;
6. hozzáférés menedzsment
7. fejlesztés és karbantartás;
8. biztonsági incidensek kezelése;
9. működésfolytonosság;
10. jogszabályi (és társadalmi) megfelelés.

személyek

1. az alkalmazás előtt:

a felvétel és a munkaköri leírások; a személyzet biztonsági átvilágítása és a személyzeti politika; a foglalkoztatás feltételei;

2. az alkalmazás alatt:

a vezetőség felelősségei; az informatikai biztonsági oktatás és képzés; fegyelmi eljárás

3. az alkalmazás megszűnésekor vagy változásakor:

a munkaviszony megszüntetésének biztonsági kérdései; az eszközök visszaadása; a hozzáférési jogok visszavonása; az átszervezés biztonsági kérdései

Köszönöm a figyelmet!

ZMNE BJKMK IHI Informatikai Tanszék

Muha Lajos PhD, CISM
egyetemi docens

e-mail: muha.lajos@zmne.hu