Infokommunikációs rendszerek biztonságos üzemeltetési lehetőségének vizsgálata

Előadó Rinyu Ferenc

A biztonság üzemeltetés (állapot) elérése nem elsősorban technikai kérdés, sokkal inkább rendszerszintű fogalom

Biztonságos üzemeltetés területei

- **Fizikai környezet;** (fizikai biztonság, ki az aki hozzáfér, épület stb…)
- **Hardver- és szoftver** környezet;
- **Hálózatok;** (vezeték nélküli hálózatok problémája, biztosítani kell a védelmet)
- **Input/output** dokumentumok;
- Külső és belső **személyi környezet**;

  (összekapcsolódik a hálózattal)

A vizsgálat lépései

- Az eszközök meghatározása és értékelése:
- A fenyegetések felbecslése:
- A sebezhetőség felbecslése:
- Kockázatbecslés:
- Ellenintézkedések kiválasztása

Speciális felmérési ismérvek:

- az objektumban milyen anyagok dokumentumok keletkeznek.
- ezek védelme milyen szintű?
- veszélyességi fokuk milyen?

Épületek állapota:

- egyszintes, vagy többszintes?
- anyaga tégla, beton, egyéb?
- kerítések állapota, külső kapuk állapota?
- ablakok állapota (zárási mélység, van-e rés feszítővasnak, rögzítettség, rács) ajtók állapota (zárási mélység, van-e rés feszítővasnak, rögzítettség, rács)

Be és kiléptetési rend:

- milyen a belépés ellenőrzési rend, és hol történik?
- alkalmazottak szabadon mozoghatnak-e az objektumban?
- vendégek mozgása korlátozott-e?
- fényképes kitűző van-e?
- csomag átvizsgálás van-e?
- takarítószolgálat felügyelete megoldott-e?
- nyilvántartás mindenkori létszámról van-e?

Járműforgalommal kapcsolatos kérdések:

- van-e alkalmazotti parkoló?
- ha van, alkalmazott bemehet-e munkaidőben?
- biztonsági szolgálat irányítja-e a belső közlekedést?

Személyzet (őrök és alkalmazottak) kérdései:

- végeznek-e az alkalmazottaknál háttér vizsgálatokat?
- háttér vizsgálatot kik végzik?
- belépés előtt elbeszélgetés történik-e?
- fizikai, szakmai, intelligencia felmérés felvételkor történik-e?
- kilépett alkalmazottakkal történik-e elbeszélgetés?
- rögzítve van-e az őrök feladata?
- milyen az őrök ellenőrzési rendje?
- változtatják-e az őrök a járőr útvonalakat, időpontokat?
- egyértelmű-e az alá és fölérendeltségi viszony?
- titkos adatok, információk védelme megoldott-e?

Zárak, riasztók állapota, kulcskezelés:

- kulcsokat kinek, hogyan lehet kiadni (naplózzák-e)?
- kulcsokat hol őrzik?
- milyen a kulcs-ellátottság?
- milyen kulcs veszett el?
- zárak javításával ki foglalkozik?
- páncélszekrény őrzése, védése hogyan van megoldva?
- Kulcsok ellenőrzése milyen időközönként történik?
- riasztók felszerelése, bekötése, ellenőrzési rendje (külső, belső)?
- riasztók beszerelését ki végezte?
- riasztók karbantartása kinek a feladata?

Zárak, riasztók állapota, kulcskezelés:

- van-e utasítás riasztó működése esetére?
- zártláncú videó rendszer van-e kiépítve?
- ajtók, ablakok zárása kinek a feladata?
- riasztót, mozgásérzékelőt idegen állat (pl. kutya) beindíthatja-e?
- riasztó hangos, vagy néma riasztású?
- az épületet utolsónak elhagyók felelősek-e a nyílászárók bezárásáért?

- A környezettanulmány eredményei alapján készítendő a védelmi terv.
- **FONTOS:**
- **Minden veszélyeztetett helyet, személyt, információt, technológiát a veszélyeztetettségi fokának <u>megfelelően kell védeni!</u>**
- **A védelmi rendszerhez élőerős védelmet, technikai eszközöket (mechanikai, elektronikai), valamint védelmi rendszabályokat kell hozzáilleszteni.**

Biztonsági felmérés célja

- jelenlegi biztonsági szint meghatározása
- objektív tényfeltárás
- mindenki számára érthető megfogalmazás
- Az objektumvédelmi terveket az informatikai rendszer és a technológia működésének megismerésére irányuló támadási lehetőségnek megfelelően kell elkészíteni. Olyan módszer is lehetséges, hogy az objektumvédelmi tervnek van egy általános része és az egyes cselekményekre vonatkozó különös része.

Létesítményvédelem

- objektum és technológia fizikai védelme
- (személy és járműbeléptetés, „jelenlét érzékelés” rádiófrekvenciás személy, jármű és tárgyazonosítás, többszintű behatolás védelem, cctv rendszer, őrség mozgásának, tevékenységének távellenőrzése, őrszolgálat elektronikus személyvédelme, duplikált,-szabotázsvédett figyelőközponti kapcsolat, technológiát érintő támadás estén előre megírt forgatókönyv szerinti rendszerleállítás, kritikus rendszerelemek automatikus megsemmisítése

Információvédelem

- megfelelő szintű kommunikációs biztonság megteremtése (telefon, tárgyalóterem)
- munkatársak napi tevékenységével kapcsolatos eljárási rend (számítógép terminál jogosult használata, keletkezett dokumentumok biztonságos tárolása)
- informatikai rendszerelemek beszerzésének, üzembe állításának rendje, külső adathordozók csatlakoztatásának korlátozása.
- biztonságos adattovábbítás rendjének kialakítása (elektronikus posta, futár)
- titkos információ birtokos személyek, kapcsolataik ellenőrzése