9.b CIA

Kockázatelemzés hasznossága

* Segítséget nyújt a rendszer leggyengébb pontjainak és a legnagyobb kockázatot jelentő

fenyegető tényezők azonosításában.

* Költséghatékony, kockázatarányos védekezést lehet kialakítani.

Kockázatmenedzsment

* Kockázatbecslés problémáit a kockázatmenedzsment módszerével szokás kezelni a

gyakorlatban, ami a kockázatok értékeit nem határozza meg konkrét érték formájában.

* Egyes kockázati tényezőket egymáshoz hasonlítva határozzuk meg a gyenge láncszemeket,

ahol a legcélszerűbb védekezni

Károk

- Hatás továbbterjedése = elsődleges, másodlagos, harmadlagos, stb. károk

- Veszélyforrás elbírálása meddig terjedhet ki, mivel a másodlagos, harmadlagos károk

nagyobbak az elsődleges károknál.

- Elsődleges kár = Merevlemez meghibásodás

- Másodlagos kár = Nagy mennyiségű adat visszaállíthatatlanul megsemmisül.

- Harmadlagos kár = Üzleti haszon elmaradása a károk miatt

Kockázatelemzés táblázatos módszere

* Alapja a veszélyforrások számbavétele és részletes elemzése, egy kockázatelemzési tábla

szisztematikus, oszlopról-oszlopra haladó kitöltésével.

Kockázatelemzés lépései

1. Kategóriák felállítása

2. Veszélyforrások meghatározása

3. Bekövetkezési valószínűségek nagyságrendi meghatározása

4. Kárérték nagyságrendi meghatározása

5. Kockázati tényezők származtatása

6. Elviselhetetlen kockázatok kezelése

7. Védelmi intézkedések számbevétele és a megfelelő alternatívák kiválasztása

Kárértékek nagyságrendi meghatározása

A károk meghatározásának szempontjai:

CIA

Confidentiality

* Adatok kiszivárgásának megakadályozása (titkosítás)

Integrity

* Sértetlenség (integritást védő algoritmusok)

Availability

* Rendelkezésre állás (hálózati eszközök és adatok elérhetősége)

Pl.: az áramszünet nem okozza a bizalmasság sérülését, de hatással van a rendelkezésre állásra, valamint következtében akár a tárolt adatok is sérülhetnek; ezt a hatásmechanizmust az I és A oszlopok megfelelő kitöltésével, a C oszlopban kihúzással jelölhetjük.