

**6.b** Mi indokolja a kockázatelemzés szükségességét? Adjon példát a kockázatelemzés gyakorlati megvalósítási lehetőségére (pl. táblázatos módszer)!

### Kockázatelemzés hasznossága

- Segítséget nyújt a rendszer leggyengébb pontjainak.
- Legnagyobb kockázatot jelentő fenyegető tényezők azonosítása.
- Ezek ismeretében költséghatékony, kockázatarányos védekezést lehet kialakítani.

### Egyenszilárdságú védelem

- Kockázatok meghatározása alapvető szerepet játszik.
- Értelmetlen túlzottan védekezni, amíg más területeken sokkal nagyobb kockázatú veszélyek is vannak a rendszerben. **(pl.: Erős ajtó, de az ablakon be lehet mászni.)**

### Kockázatmenedzsment

- Kockázatok, károk.
- Kockázatbecslés problémáit a kockázatmenedzsment módszerével szokás kezelni a gyakorlatban, ami a kockázatok értékeit nem határozza meg konkrét érték formájában.
  - o Olyan összehasonlításra lehetőséget adó elemzést alkalmaz, ami alapján legcélszerűbb védelmi intézkedések meghatározhatóak.
- Egyes kockázati tényezőket egymáshoz hasonlítva határozzuk meg a gyenge láncszemeket, ahol a legcélszerűbb védekezni.

### Problémák

- Veszélyforrások bekövetkezésének gyakoriságára nincsenek jó statisztikák.
- Okozott károk anyagilag sem határozhatóak meg.

### Kockázati paraméterek becslése

- Veszélyforrások támadási folyamatának hatásmechanizmusa
  - o Informatikai rendszerek konkrét rendszerelemeinek támadása.
  - o Egyes rendszerelemek sérülése hat a velük kapcsolatban lévő alkalmazásokra.
  - o Nem sikerül jól kezelni a károkat, akkor az ügyfeleknél is érzékelhető lesz.

### 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 módszerei

- Egyetlen módszertan sem vállalkozik arra, hogy informatikai rendszerek esetén a kockázat pénzügyi nagyságát közvetlenül megbecsülje.

## Kockázatelemzés táblázatos módszere

- Alapja a veszélyforrások számbavétele és részletes elemzése, egy kockázatelemzési tábla szisztematikus, oszlopról-oszlopra haladó kitöltésével.

## Kockázatelemzés lépései

### 1. Kategóriák felállítása:

Bekövetkezési valószínűség, Kár, Kockázati, Kockázati szorzótábla meghatározása

2. **Veszélyforrások meghatározása**
3. **Bekövetkezési valószínűségek nagyságrendi meghatározása**
4. **Kárérték nagyságrendi meghatározása**
5. **Kockázati tényezők származtatása**
6. **Elviselhetetlen kockázatok kezelése**
7. **Védelmi intézkedések számbavétele és a megfelelő alternatívák kiválasztása**

## Kategóriák felállítása

- A bekövetkezés valószínűségének, a támadási potenciálnak leírása.
- A bekövetkező kár becslése.
- A kockázat veszélyforrásonkénti nagyságának meghatározása.
- Meghatározzuk a közöttük lévő kapcsolatot a kockázati szorzótáblával.

## Veszélyforrások listájának összeállítása

- **Veszélyforrások:** A rendszer helyes működését fenyegető események.
- A kockázatelemzési tábla sorait alkotják.
- Egyértelmű azonosítóval látjuk el.
- **Helyzetfelmérés:** Dokumentumok elemzésével, Interjúkkal, Szemlével
- **Veszélyforrások feltárása**
  - o Tapasztalatok felhasználásával és a rendszer elemzéséből felderített hiányosságok számbavételével történhet.
- A lista soha nem lehet teljes, de lehet részletes.
- Kimaradó veszélyforrásokat kockázatként kezelhetjük.

## Veszélyforrások csoportjai

- Szervezési gyengeségek
- Természeti veszélyforrások (tűz, villám), Fizikai veszélyek (betörés, lopás)
- Logikai fenyegetések (hálózati betörés, lehallgatás)
- Humán veszélyforrások (visszaélések, munkatársak gondatlansága)

## Bekövetkezési valószínűségek nagyságrendi becslése

- **Probability oszlop**
- Tapasztalatok alapján történik.
- A támadási potenciál meghatározásánál figyelembe kell venni a gyengeség kihasználásához szükséges felkészültségi szintet és, hogy mennyire érdemes támadást végrehajtani az adott rendszer ellen.
- **Felkészülési szintek alapján:**
  - o Automatizált eszközökkel végrehajtható
  - o Átlagos felhasználó által kihasználható
  - o Profi támadót igénylő gyengeség

## Kárérték nagyságrendi meghatározása

- Komplex feladat
- Hatás megfigyelése egy adott rendszerelem sérülése esetén.
- **Okozott kár természete:** Érintett rendszerelem milyen tulajdonsága sérült.
- Károk meghatározásának szempontjai
  - o Bizalmasság (Confidentiality) megsértése, jogtalan információ szerzés.
  - o Sértetlenség (Integrity) elvesztése, a tárolt adatok manipulálása.
  - o Rendelkezésre állás (Availability) elvesztése.

## Kockázati tényezők származtatása

- Risk oszlop kitöltése a kockázati szorzótábla segítségével.
- A szorzótábla sorát a veszélyforrás előfordulási gyakorisága
  - o Oszlopát általában a CIA szempontok közül a legnagyobb kárral járó kár-kategóriája határozza meg. Sor és oszlopnak megfelelő cella tartalmazza a kockázatot.

## Elviselhetetlen kockázatok

- Helyrehozhatatlan, hosszabb távon is kiható tényezők által jelentett veszély.
- Védelmi intézkedések kiválasztásakor a cél:
  - o Olyan védelmi intézkedések alkalmazása, amik költsége kevesebb, mint az általuk kiküszöbölt kockázat.
  - o Hosszú távon, és egyéb üzletpolitikai szempontok figyelembe vétele.
- A szorzótáblában és a kockázatelemzési táblában általában külön (pl.: \*-gal) jelölhetők.
- Az elviselhetetlen kockázatú veszélyforrás kockázatát legalább elviselhető mértékűvé csökkentése.

## Lehetséges védelmi intézkedések számbavétele

- Felírjuk az összes elképzelhető védelmi intézkedést.
- Mindegyiknél megadjuk, hogy milyen hatása van.
- Majd az összes lehetséges kombináció értékelésével megkaphatjuk, hogy miket kell kiválasztani.
  - o Választás legfontosabb szempontja az ár és az elért hatás.
  - o Költségeknél célszerű megkülönböztetni az egyszeri beruházási költségeket az éves fenntartási költségektől.
  - o Rövid és hosszú távú pénzügyi célok jól elkülöníthetők.
- Védelmi intézkedések egymásra hatással vannak, ezért a veszélyforrásokra gyakorolt hatásaikat már nem szokás kategorikusan meghatározni.
- A veszélyforrásokra gyakorolt hatást a valószínűség és a hatás csökkentésének mértékével adhatjuk meg.
- A hatás leírásában meg kell adni az intézkedés által befolyásolt veszélyforrás azonosítóját és a befolyásolás módját.

## Hatásmegjelölés magyarázat

- E: (eliminates) a veszélyforrás teljes kiküszöbölés.
- D: (decreases damage) az okozott kár egy kategóriával csökken.
- DD: (decreases damage) az okozott kár két kategóriával csökken.
- P: (decrease probability) a bekövetkezési valószínűség egy kategóriával csökken.
- PP: (decrease probability) a bekövetkezési valószínűség két kategóriával csökken.