10.b Mutassa be a biztonság tervezési elveit! Határozza meg az információbiztonsági célok elérésére használható intézkedés típusokat, adjon példát ezekre intézményi környezetben!

Tervezés

1. A rendszerterv és a használt biztonsági protokoll legyen nyilvános.
2. Alapértelmezés legyen az, hogy valaki valamihez nem férhet hozzá.
3. A security-vel kapcsolatos kérdéseket a rendszer tervezésének korai fázisában tisztázni kell és a security csomagot a rendszer magjába intergálni kell.
4. Legyen a rendszer felhasználóbarát.
5. Ha lehet, akkor kerüljük az egész rendszer felett „teljes hatalommal bíró” (superuser, supervisor) rendszergazda koncepciót.
    a. A rendszert bontsuk moduljaira, például egy-egy modul egy-egy fontosabb erőforrás kezelését végezze és az egyes moduloknak legyenek külön-külön felügyelői.

Információbiztonság (InfoSec)

- Az információbiztonság azoknak a biztonsági eljárásoknak és eszközöknek az összességét jelenti, amik széles körben védik a bizalmas vállalati adatokat a visszaélésszerű használattól, a jogosulatlan hozzáférésektől, a szolgáltatáskimaradástól és a megsemmisítéstől.
- Magában foglalja a fizikai és környezeti biztonságot, a hozzáférés-vezérlést és a kiberbiztonságot.

Információvédelem

- Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása.
- **Tehát az információval kapcsolatos biztonsági kockázatok folyamatos menedzselése.**

CIA

- **Confidendiality:** Adatok kiszivárgásának megakadályozása, vagyis titkosítás.
- **Integrity:** Sértetlenség, vagyis integritást védő algoritmusok.
- **Availability:** Rendelkezésre állás, vagyis hálózati eszközök és adatok elérhetősége.

Információbiztonsági célok elérésére használható intézkedés típusok

- Kockázatok csökkentése intézkedések alkalmazásával.

Kontroll

- Olyan irányelvek, szabályzatok, eljárások, gyakorlatok és szervezeti struktúrák összessége, amiket arra hoztak létre, hogy ésszerű bizonyosságot adjanak arra, hogy az üzleti célkitűzések elérhetőek, a nemkívánatos események megelőzhetőek, felismerhetőek és helyesbíthetőek.

Intézkedések (kontrollok)

Megelőző (preventív)

- Az esemény bekövetkeztének teljes mértékben való megakadályozását célzó intézkedés, amennyiben kifizetendő lenne, minden esetben megelőző kontrollt használnák.
- **Példa**
  - A jelszavas védelem célja megelőzni, hogy illetéktelen személyek érjék el az adott rendszert.

Elriasztó (deterrent, dissuasive)

- Nem biztosítja a megelőzést, a nem kívánt esemény bekövetkezésének valószínűségét csökkenti úgy, hogy a támadónak a motivációját csökkenti.
- **Példa**
  - Ha kihirdetjük, hogy minden számítógépes aktivitást monitorozunk, akkor magának az intézkedés bejelentésének tényével csökkenthetjük a visszaélések számát.

Felismerő (detective)

- Lehetővé teszi, hogy a megfelelő gyorsasággal értesüljünk a nem kívánt eseményről, annak érdekében, hogy annak hatását csökkentsük és helyreállítsuk a működést.
- **Példa**
  - Egy ellenörző összeg egy pénzügyi lista elektronikus átvitele során lehetővé teszi, hogy annak megérkezésekor az esetleges hamisítást vagy rendszerhibát észleljük.

Hatácsökkentő (mitigating, palliative)

- Az esemény bekövetkeztekor fellépő negatív hatást csökkenti.
- **Példa**
  - A biztonsági mentések csökkentik egy bekövetkezett rendszerhiba hatását azzal, hogy rendelkerésünkre áll az adatnak egy korábbi verziója.

Javító, helyreállító (corrective, recuperative)

- Az eredeti állapot visszaállítását célzó intézkedések.
- Ezeket is előre meg kell tervezi.
- Fontos, hogy maguk a helyreállító intézkedések ettől még nem lesznek preventív jellegűek, mert az eseményeket nem előzik meg.
- **Példa**
  - Valamilyen validációt hajtunk végre vagy esetleg limit értékeket vizsgálunk meg.