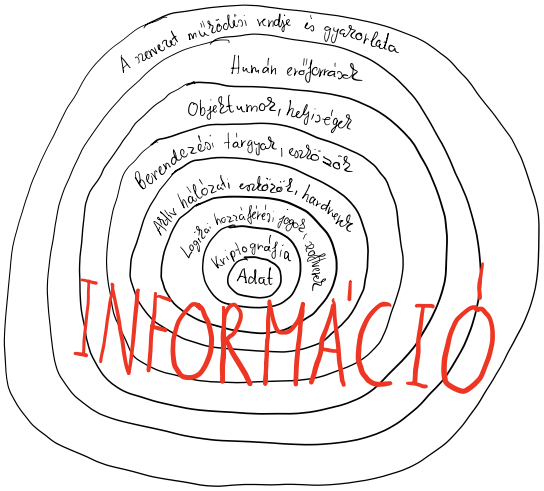
Biztonsági tervezési elvek

• 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 integrálni kell.
4. Legyen a rendszer felhasználóbarát.
5. Ha lehet, akkor kerüljük az egész rendszer felett "teljes hatalommal bíró" rendszergazda koncepciót.
    - 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 rövid időn védik a bizalmas vállalati adatokat a visszaélésszerű használattól, a jogosulatlan hozzáféréstől, 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

- Confidentiality -> Adatok kiszivárgásának megakadályozása, vagyis titkosítás.
- Integrity -> Sértetlenség, vagyis integritást védő algoritmusok.
- Availability -> Rendelkezésre állás, vagyis hálózati eszközök és adatok elérhetősége.
- Példa -> Az áramszünet nem okozza a bizalmasság sérülését, de hatással van a rendelkezésre állásra és a&á a tárolt adatok is sérülhetnek.

· Információbiztonsági célok elérése használható intézkedés típusok

- Kockázatok csökkentése intézkedések alkalmazásával.

· Kontrol

- 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 bekövetkezésének teljes mértékben való megakadályozását célzó intézkedés, amennyiben kifizetendő lenne, minden esetben megelőző kontrollt használnánk.
  - 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 csökkentjük 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 ellenőrző összeg egy pénzügyi lista elektronikus átvitele során lehetővé teszi, hogy annak megérkezésekor az esetleges hamisítást vagy rendszerhibát érzékeljük.
- Hatáscsökkentő (mitigating, palliative) → Az esemény bekövetkezésekor fellépő negatív hatást csökkenti.
  - Példa → A biztonsági mentések csökkentik egy bekövetkezett rendszerhiba hatását azzal, hogy rendelkezésünkre áll az adatnak egy korábbi verziója.
- Javító, helyreállító (corrective, recuperative)
  - Az eredeti állapot visszaállítását célzó intézkedések. → Előre meg kell tervezni.
  - Fontos, hogy maguk a helyreállító intézkedések ettől még nem lesznek preventív jellegűek, mert az eseményeket nem előzik meg.
    - Példa → Patch management, tehát frissítések, patch-ek telepítése az esetleges sérülékenységek megelőzésére.