# Szoftverrendszerek biztonsága

# Bevezetés / Alapfogalmak

- A számítógépes biztonság a *titkosságon*, *sértetlenségen* és *rendelkezésre álláson* alapul.
- **Bizalmasság (Confidentiality)**
  **Bizalmasság** azt jelenti, hogy az információ rejtett marad, vagy el van zárva azoktól, akik nem jogosultak rá.
  Hozzáférés-szabályozó mechanizmusok támogatják a titkosságot → az adatot oly módon alakítják át, hogy olyanok számára legyen *nem elérhető*, akik nem láthatják.
  Példák:
  • Személyes adatok
  • Banki adatok
  • Vállalati bizalmas adatok

# Integritás & Rendelkezésre állás

**Sértetlenség (Integrity)**

A *sértetlenség* azt jelenti, hogy az adatok vagy erőforrások *sértetlenek* és *oszthatatlanok*.
Integritás magában foglalja:

- adat integritását (az információ tartalma)
- eredet integritását (az adat forrása, hitelesítés

A sértetlenségi mechanizmusok lehetnek:

- megelőző mechanizmusok
- felismerő mechanizmusok

**Rendelkezésre állás (Availability)**

A rendelkezésre állás arra utal, hogy az információ vagy erőforrás *használható*.
Egy *nem elérhető* rendszer legalább olyan rossz, mint ha nem létezne.
Példa: szolgáltatásmegtagadási támadás (DoS)

# Fenyegetések

A fenyegetés a biztonság potenciális megsértését jelenti.

- A megsértésnek nem kell valóban bekövetkeznie ahhoz, hogy fenyegetésnek számítson.
- Ha bekövetkezik, azt támadásnak hívjuk.
- Azokat, akik ezeket a tevékenységeket végrehajtják vagy kiváltják, támadóknak nevezzük.

Fenyegetés osztályai:

- Kiszivárgás (Disclosure) – jogosulatlan hozzáférés információhoz
- Megtévesztés (Deception) – hamis adatok elfogadása
- Megszakítás (Disruption) – a helyes működés megszakítása vagy megelőzése
- Jogtalan átvétel (Usurpation) – egy rendszer részének jogosulatlan irányítása

# Irányelvek és mechanizmusok

Irányelv (policy) és mechanizmus

Biztonsági irányelv: olyan kijelentés, amely meghatározza, mi engedélyezett és mi nem engedélyezett.
Biztonsági mechanizmus: olyan módszer, eszköz vagy eljárás, amely végrehajtja a biztonsági irányelvet.

A biztonság céljai

- Megelőzés – a támadás meghiúsul
- Felismerés – hasznos, ha egy támadás nem előzhető meg
- Helyreállítás –
  a támadás leállítása és a
  károk kijavítása
  a rendszer továbbra is helyesen működik a támadás alatt

# Minőségbiztosítás a biztonságkritikus rendszerekben

- A minőségbiztosítás olyan konkrét lépéseket igényel, amelyek biztosítják, hogy a rendszer megfelelően fog működni:
- részletes specifikációk a kívánt (vagy nem kívánt) viselkedésről;
- a hardver, szoftver és egyéb komponensek tervezésének elemzése annak bizonyítására, hogy a rendszer nem sérti meg ezeket a specifikációkat;
- dokumentumok, bizonyítékok, hogy a végrehajtás, az üzemeltetési és karbantartási eljárások a kívánt viselkedést eredményezik.

# Specifikáció, tervezés, implementáció

**Specifikáció**

A specifikáció a rendszer kívánt működésének (formális vagy informális) leírása. Lehet:

- Matematikai
- formális specifikációs nyelv
- természetes nyelv (mint az angol)

**Tervezés**

- A rendszer tervezése átalakítja a specifikációt olyan komponensekké, amelyek végrehajtják azokat.
- A tervezés akkor elégíti ki a specifikációkat, ha minden lehetséges körülmény között nem engedi azok megsértését.

**Implementáció**

- A tervezés alapján az implementáció létrehozza a rendszert, amely kielégíti azt a tervet.
- Ha a terv megfelel a specifikációknak, akkor az implementáció is meg fog felelni.

# Helyesség és tesztelés

Helyesség (Correctness)

- Egy program akkor helyes, ha a végrehajtása megfelel a specifikációnak.
- A helyesség bizonyítása azt jelenti, hogy a forráskód minden sorát matematikailag ellenőrzik.

Tesztelés (Testing)

- Mivel a formális helyesség-bizonyítás időigényes, a tesztelés elterjedt gyakorlat.
- A tesztelő futtatja a programot adatokkal, hogy meghatározza, a kimenet megfelel-e az elvártnak, és mennyire valószínű, hogy hibát tartalmaz a program.

# Költség-Haszon elemzés

- Egy összetett rendszerben a számítógépes biztonság előnyeit a teljes költséggel (beleértve a rendszer kompromittálódásának többletköltségét is) kell mérlegelni.
- Ha az adatok vagy erőforrások alacsonyabb értékűek, mint a védelmük költsége, akkor a biztonsági intézkedések bevezetése nem gazdaságos.

# Kockázatelemzés

- Annak meghatározásához, hogy egy erőforrást védeni kell-e és milyen szinten, elemezni kell a rá potenciálisan leselkedő fenyegetéseket és azok bekövetkezésének valószínűségét.
- A védelmi szint függ a támadás valószínűségétől és az okozott hatástól.

# Emberi tényezők

- A biztonsági rendszer központja az ember.
- Különösen a számítógépes biztonságban, ahol a technológiai kontrollokat gyakran az emberi beavatkozás működteti.
- A legtöbb veszélyes támadás belső felhasználóktól érkezik, akik jogosultak a rendszerek használatára.
- A képzetlen személyzet ugyancsak fenyegetést jelent.
- Sok támadás social engineering módszerekkel történik.

# Jogi, szabályzási és szervezeti tényezők

**Szabályzatok**

- A törvények, szabályzatok korlátozzák a technológia elérhetőségét és használatát, és befolyásolják az eljárási kontrollokat. Ezért bármilyen irányelvnek és mechanizmusválasztásnak figyelembe kell vennie a jogi szempontokat.

**Szervezeti kérdések**

- A biztonság nem közvetlen pénzügyi hasznot hoz. Korlátozza a veszteségeket, de erőforrásokat is igényel: időt, pénzt, szakembereket és képzést.

# Jogi kérdések - stratégiák

- **Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. Határozat – „Biztonságos Magyarország egy változékony világban”**
- **1393/2021. (VI.24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról**
- **1089/2025. (III. 31.) Korm. Határozat Magyarország Kiberbiztonsági Stratégiájáról**
- **az Európai Parlament és a Tanács 2022/2555 irányelve (NIS 2)**

# Jogi kérdések

- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény;
- a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény;
- a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény;

- SZTFH rendeletek (10/2023. (V.15.), 15/2023. (VII.31.), 23/2023. (XII.19.), 7/2024. (VI.24.), 10/2024. VIII.8.), 1/2025. (I.31.), 2/2025. (I.31.), 3/2025. (IV.17.), 5/2025. (VI.20.);

# EIR

**Elektronikus információs rendszer**nek minősül:
a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy
c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

EIR-nek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében:
- az adatok, információk kezelésére használt eszközök (ideértve a környezeti infrastruktúrát, hardvert, hálózatot és az adathordozókat),
- az adatok, információk kezelésére használt eljárások (ideértve a szabályozást, a szoftvert és kapcsolódó folyamatokat),
- az ezeket kezelő személyek együttesét.

+ *kiber-fizikai rendszer*: olyan programozható EIR-ek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével és/vagy vezérlésével;

# EIR biztonsága

Az EIR azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

# EIR védelme

**Zárt, teljes körű, folytonos és a kockázatokkal arányos védelem elve**

Az EIR olyan védelme:
*a)* amely az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósul (folytonos),
*b)* amely az EIR valamennyi elemére kiterjed (teljes körű),
*c)* amely az összes számításba vehető fenyegetést, veszélyt figyelembe veszi (zárt),
*d)* amely során a védelmi intézkedésekre fordított költségek arányosak a fenyegetések által okozható károk értékével *(*kockázatokkal arányos védelem

# Védelmi intézkedések

*7/2024. (VI.24. MK rendelet)*

k

*logikai* – az EIR-ben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;
*fizikai* – a fizikai térben megvalósuló fenyegetések elleni védelem;
*adminisztratív* – a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.