INFORMATIKAI BIZTONSÁG ALAPJAI

2. előadás

Göcs László
főiskolai tanársegéd
Neumann János Egyetem GAMF Műszaki és Informatikai Kar
Informatika Tanszék

2018-19. 1. félév

Informatikai Tárcaközi Bizottság ajánlása
Informatikai rendszerek biztonsági követelményei

12. sz. ajánlás

A BIZTONSÁGI STRATÉGIA MEGHATÁROZÁSA

Milyen úton érjük el a célt?

Honnan indulunk?

Hova akarunk eljutni?

A BIZTONSÁGI STRATÉGIA MEGHATÁROZÁSA

- meghatározzuk a védelmi **célokat**,
- kiválasztjuk és elhatároljuk azokat a **területeket**, amelyeken a biztonsági rendszereket kialakítani és az intézkedéseket érvényesíteni kell,
- meghatározzuk a biztonsági tervezés **módszerét**,
- körvonalazzuk a **minimális követelményeket**,
- megtervezzük és ütemezzük az intézményre vonatkozó **biztonsági intézkedéseket**, beleértve a katasztrófa-elhárítást is,
- meghatározzuk a követhetőség és a **menedzselhetőség** követelményeit, valamint a **felügyelet** és az ellenőrzés rendszerét.

A BIZTONSÁGI STRATÉGIA MEGHATÁROZÁSA

Az informatikai biztonsági stratégia

- része az intézmény globális biztonsági stratégiájának
- összhangban kell lennie az intézmény működési és informatikai stratégiájával
- ki kell szolgálnia az intézmény célkitűzéseit

Alkalmazások és adatok fenyegetettsége

- bizalmasság elvesztése,
- sértetlenség elvesztése,
- hitelesség elvesztése,
- rendelkezésre állás elvesztése,
- funkcionalitás elvesztése.

alapfenyegetettségeknek

AZ INFORMÁCIÓVÉDELEM A

- bizalmasság,
- sértetlenség, védelme.
- hitelesség,

A MEGBÍZHATÓ MŰKÖDÉS A

- rendelkezésre állás,

biztosítását jelenti.

- funkcionalitás,

Az informatikai rendszer szakaszai:

- az informatikai rendszer **tervezése**;
- az informatikai rendszer **fejlesztése**;
- az informatikai rendszer **bevezetése**, illetve **üzembe helyezése**;
- az informatikai rendszer **üzemeltetése, fenntartása**;
- az informatikai rendszer **megszüntetése**, felszámolása vagy **rekonstrukciója**.

A szakaszokban folyamatosan ellenőrizni kell:

- a fenyegetettség szintjét,
- a biztonság meglétét,
- a biztonsági intézkedések végrehajtását és hatékonyságát.

Tervezési módszerek

- a kockázatelemzés, ⇒ értékkel arányos védelem megteremtése
- a kritikus működési jellemzők elemzése, ⇒ védelmi intézkedések súlya
- az értékek sérülési hatásainak elemzése. ⇒ várható károk nagyságrendjére

Minimális biztonsági követelmények

Információvédelem

- az azonosítás és a hitelesítés folyamatának kialakítása,
- a hozzáférés rendszerének felépítése - **jogosultság kiosztás** (alanyok, eszközök meghatározása, attribútumok rögzítése, hozzárendelések - megengedő, illetve tiltó módszer a szigorodó követelményekre),
- a hozzáférés-ellenőrzés rendszerének megvalósítása - **jogosultság ellenőrzés**,
- a hitelesség garantálása
- a sértetlenség garantálásának kiépítése,
- a bizonyítékok rendszerének és folyamatának kialakítása.

Minimális biztonsági követelmények

Megbízható működés

- a hibaáthidalás folyamatának kialakítása,
- az újraindítási képesség megvalósítása,
- a rendszer funkcionalitásának biztosítása.

Biztonsági szabályzat

Az informatikai biztonságpolitika alapján ki kell dolgozni az egységes szerkezetbe foglalt, az

- **egész intézményre érvényes** és a
- **többi szabályzattal összhangban** álló

Informatikai **B**iztonsági **Sz**abályzatot.

Informatikai Biztonsági Szabályzatnak

Tartalmaznia kell

- az általános követelményeket,
- részletes intézkedésrendszert,
- eljárások rendjét,
- a felelősöket,
- az ellenőrzés rendjét,
- a szankcionálás módját.

Informatikai Biztonsági Szabályzat

- Tükröződniük kell a **munkaköri leírásokban**.
- A felhasználók részére egy **Biztonsági Kézikönyv** kiadása javasolt.
- Szabályozni kell az **Informatikai Biztonsági Felügyelő** illetékességét és hatáskörét (feladat-, felelősségi és jogkörét), valamint alá- és fölérendeltségi viszonyait.

A kár jellege:

Dologi károk, amelyeknek közvetlen vagy közvetett költségvonzatuk van

- károsodás az infrastruktúrában (épület, vízellátás, áramellátás, klímaberendezés stb.),
- károsodás az informatikai rendszerben (hardver, hálózat sérülése stb.),
- a dologi károk bekövetkezése utáni helyreállítás költségei;

A kár jellege:

Károk a **politika és a társadalom területén**

- állam- vagy szolgálati titok megsértése,
- személyiséghez fűződő jogok megsértése, személyek vagy csoportok jó hírének károsodása,
- bizalmas adatok nyilvánosságra hozatala,
- hamis adatok nyilvánosságra hozatala,
- közérdekű adatok titokban tartása,
- bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben;

A kár jellege:

Gazdasági károk

- pénzügyi károk,
- lopás károk,
- az intézmény vagy cég arculatának (image) romlása,
- rossz üzleti döntések hiányos vagy hamis információk alapján;

Károk a **tudomány** területén

- kutatások elhalasztódása,
- eredmények idő előtti, illetve hamis név alatti nyilvánosságra kerülése,
- tudományos eredmények meghamisítása.

A kár jellege:

Egyéb károk

- károk az informatikai személyzet, illetve a felhasználók személyi biztonsága területén, pl.: személyek megsérülése, megrokkanása (pl. áramütés következtében);
- károk a hatályos jogszabályok és utasítások megsértéséből adódóan;

A károk csoportosítása:

- közvetlen anyagi (pl. a mindenkori amortizált értékkel vagy az elmaradt haszonnal arányos),
- közvetett anyagi (pl. a helyreállítási költségekkel, perköltségekkel arányos),
- társadalmi-politikai, humán,
- személyi sérülés, haláleset,
- jogszabály által védett adatokkal történő visszaélés vagy azok sérülése (jogsértés).

Kár érték szintek

"0": jelentéktelen kár

- közvetlen anyagi kár: - 10.000,- Ft,
- közvetett anyagi kár **1 embernappal** állítható helyre,
- nincs bizalom vesztés, a probléma a szervezeti egységen belül marad,
- testi épség jelentéktelen sérülése egy-két személynél,
- nem védett adat bizalmassága vagy hitelessége sérül.

Kár érték szintek

"1": csekély kár

- közvetlen anyagi kár: - 100.000,- Ft-ig,
- közvetett anyagi kár **1 emberhónappal** állítható helyre,
- társadalmi-politikai hatás: kínos helyzet a szervezeten belül,
- könnyű személyi sérülés egy-két személynél,
- hivatali, belső (intézményi) szabályozóval védett adat bizalmassága vagy hitelessége sérül.

Kár érték szintek

"2": közepes kár

- közvetlen anyagi kár: - 1.000.000,- Ft-ig,
- közvetett anyagi kár **1 emberévvel** állítható helyre,
- társadalmi-politikai hatás: bizalomvesztés a tárca középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel,
- több könnyű vagy egy-két súlyos személyi sérülés,
- személyes adatok bizalmassága vagy hitelessége sérül,
- egyéb jogszabállyal védett (pl. üzleti, orvosi) titok bizalmassága vagy hitelessége sérül.

Kár érték szintek

"3": nagy kár

- közvetlen anyagi kár: - 10.000.000,- Ft-ig,
- közvetett anyagi kár **1-10 emberévvel** állítható helyre,
- társadalmi-politikai hatás: bizalomvesztés a tárca felső vezetésében, a középvezetésen belül személyi konzekvenciák,
- több súlyos személyi sérülés vagy tömeges könnyű sérülés,
- szolgálati titok bizalmassága vagy hitelessége sérül,
- szenzitív személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül,
- banktitok, közepes értékű üzleti titok bizalmassága vagy hitelessége sérül.

Kár érték szintek

"4": kiemelkedően nagy kár

- katonai szolgálati titok bizalmassága vagy hitelessége sérül,
- közvetlen anyagi kár: - 100.000.000,- Ft-ig,
- közvetett anyagi kár **10-100 emberévvel** állítható helyre,
- társadalmi-politikai hatás: súlyos bizalomvesztés, a tárca felső vezetésén belül személyi konzekvenciák,
- egy-két személy halála vagy tömeges sérülések,
- államtitok bizalmassága vagy hitelessége sérül.
- nagy tömegű szenzitív személyes adat bizalmassága vagy hitelessége sérül,
- nagy értékű üzleti titok bizalmassága vagy hitelessége sérül.

Kár érték szintek

"4+": katasztrofális kár

- közvetlen anyagi kár: 100.000.000,- Ft felett,
- közvetett anyagi kár több mint 100 emberévvel állítható helyre,
- társadalmi-politikai hatás: súlyos bizalomvesztés, a kormányon belül személyi konzekvenciák,
- tömeges halálesetek,
- különösen fontos (nagy jelentőségű) államtitok bizalmassága vagy hitelessége sérül.

Biztonsági osztályok

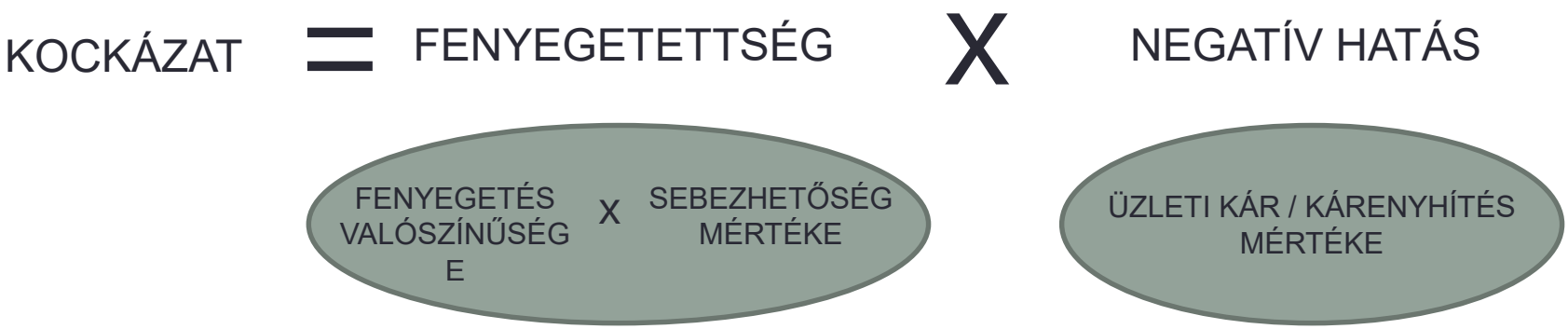
- **alapbiztonsági** követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum "**2**", azaz legfeljebb **közepes kárértékű** esemény bekövetkezése fenyeget;
- **fokozott biztonsági** követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum "**3**", azaz legfeljebb **nagy kárértékű** esemény bekövetkezése fenyeget;
- **kiemelt biztonsági** követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben a "**4+**", azaz a **katasztrofális kárértékig** terjedő esemény bekövetkezése fenyeget.

Informatikai kockázatelemzés

Az informatikai biztonság tervezéséhez, a stratégia kialakításához szükséges, hogy ismerjük a rendszer különböző területeinek kockázatát.

Informatikai kockázatelemzés

Nem védelmi intézkedés, elvégzése önmagában **nem erősíti a védelmet**, de **segít** hogy létrejöjjön a biztonságos informatikai rendszer.



Informatikai kockázatelemzés

- Eszközgazdálkodási audit eredménye.
- Fenyegetések felmérése.
- Informatikai sérülékenység felmérése.

Magyar informatikai biztonsági szabványok

A szabványok négy szintjét szokták megkülönböztetni:

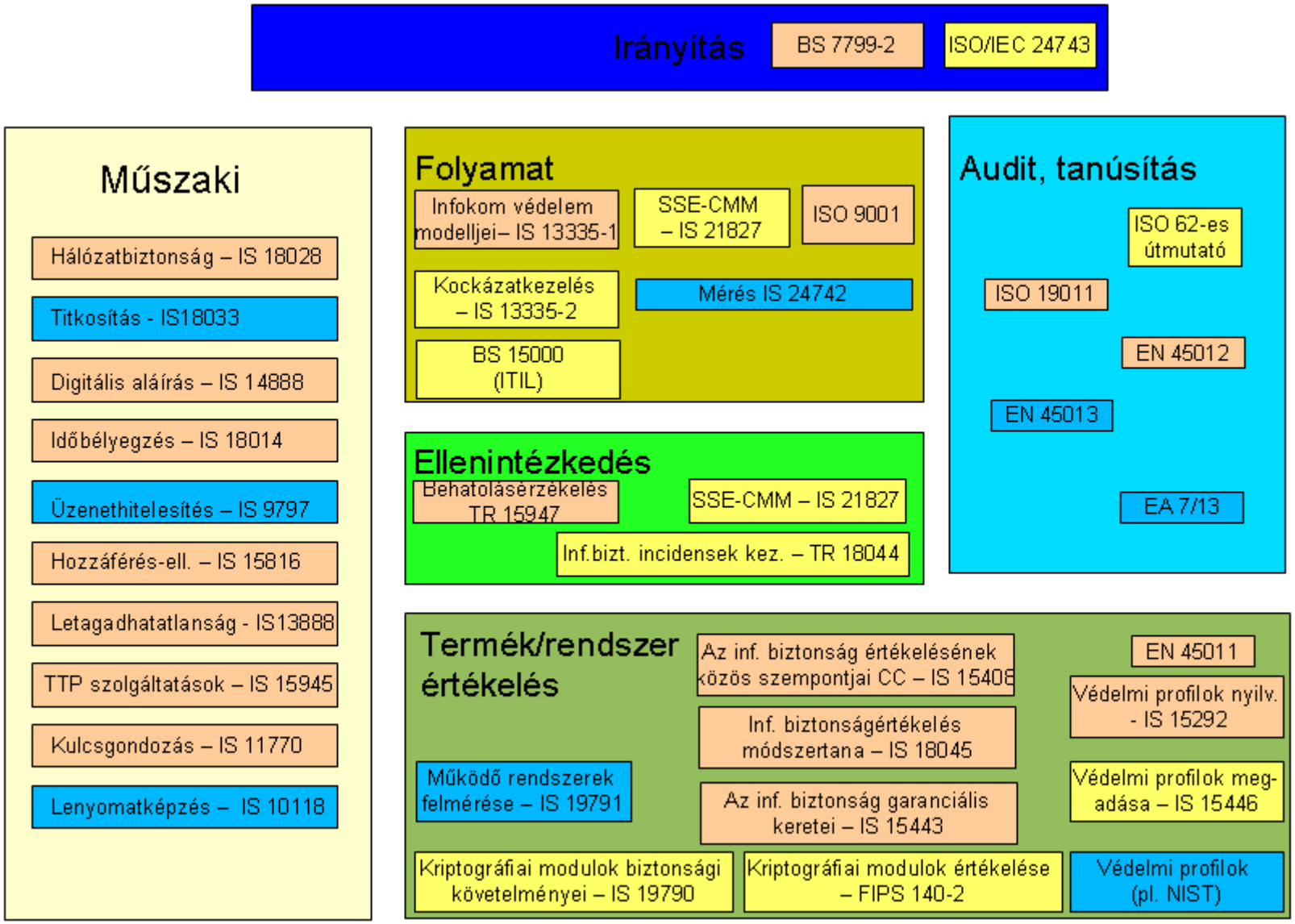
- **hivatalos (de-jure) szabványok:** ide azok a szabványok tartoznak, melyeket a különböző **államok által törvényi szinten** elismert vagy nemzetközi megállapodás keretében létrejött szervezetek adnak ki. A hivatalos szabványokon belül az alábbi szinteken különböztethetjük meg:
  - nemzetközi szintű szabványok (pl.ISO által kiadott szaványok),
  - regionális szintű szabványok,
  - nemzeti szintű szabványok (pl. a Magyar Szabadalmi Hivatal által meghatározott szabványok).
- **ipari (de-facto) szabványok**: az ilyen szabványok egy **adott iparág** konzorciumba tömörült szervezeteinek együttműködése kapcsán jön létre (pl. RFC-k),

Magyar informatikai biztonsági szabványok

- **ad-hoc szabványok:** habár egyik szabványügyi szervezet sem hagyta jóvá, de lényegében szabvánnyá vált. (Általában a de-facto szabványok elődje)
- **saját, védett szabványok:** pl. egy domináns szoftverfejlesztő cég által kiadott előírások, a tulajdonjog a kibocsájtó kezében marad, licenszdíjat szedhetnek érte.

Az informatikai biztonsági szabványok másik csoportosítása tartalmuk szerint történhet:

- az információbiztonság-**irányítási** rendszer követelményei,
- **műszaki** szabványok és leírások,
- **folyamatokra** vonatkozó szabványok (szolgáltatásmenedzsment),
- **ellenintézkedésre** vonatkozó szabványok,
- **auditálás, tanúsításra** vonatkozó szabványok,
- termékek/rendszerek **értékelésére** vonatkozó szabványok


Irányítás
BS 7799-2
ISO/IEC 24743
Műszaki
Hálózatbiztonság – IS 18028
Titkosítás - IS18033
Digitális aláírás – IS 14888
Időbélyegzés – IS 18014
Üzenethitelesítés – IS 9797
Hozzáférés-ell. – IS 15816
Letagadhatatlanság - IS13888
TTP szolgáltatások – IS 15945
Kulcsgondozás – IS 11770
Lenyomatképzés – IS 10118
Folyamat
Infokom védelem modelljei– IS 13335-1
SSE-CMM – IS 21827
ISO 9001
Kockázatkezelés – IS 13335-2
Mérés IS 24742
BS 15000 (ITIL)
Audit, tanúsítás
ISO 62-es útmutató
ISO 19011
EN 45012
EN 45013
EA 7/13
Ellenintézkedés
Behatolásérzékelés TR 15947
SSE-CMM – IS 21827
Inf.bizt. incidensek kez. – TR 18044
Termék/rendszer értékelés
Az inf. biztonság értékelésének közös szempontjai CC – IS 15408
EN 45011
Védelmi profilok nyilv. - IS 15292
Inf. biztonságértékelés módszertana – IS 18045
Működő rendszerek felmérése – IS 19791
Védelmi profilok megadása – IS 15446
Az inf. biztonság garanciális keretei – IS 15443
Kriptográfiai modulok biztonsági követelményei – IS 19790
Kriptográfiai modulok értékelése – FIPS 140-2
Védelmi profilok (pl. NIST)

KÖVETELMÉNYEK AZ INFORMÁCIÓVÉDELEM TERÉN

Védendő adatoknak alapvetően négy csoportját különíthetjük el:

- nyílt, szabályozók által nem védett adat,
- érzékeny (védendő), de nem minősített adat,
- szolgálati titok,
- államtitok.

Érzékeny, de nem minősített adatok

A jogszabályok által védendő adatok:

- személyes, illetve különleges adatok,
- az üzleti titkot,
- a banktitkot képező adatok,
- az orvosi,
- az ügyvédi és
- egyéb szakmai titkok,
- a posta és a távközlési törvény által védett adatok stb. , és
- az egyes szervezetek, intézmények illetékesei által, belső szabályozás alapján védendő adatok.

Információbiztonsági osztályozás az információvédelem szempontjából

- információvédelmi **alapbiztonsági** (**IV-A**) osztály: Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- információvédelmi **fokozott biztonsági** (**IV-F**) osztály: A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.
- információvédelmi **kiemelt biztonsági** (**IV-K**) osztály: Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

Az osztályok követelményei:

- Minimális követelmények
- Infrastruktúra
- Hardver, szoftver
- Adathordozók
- Dokumentumok és dokumentációk
- Adatok
- Kommunikáció, osztott rendszerek
- Személyek

IV-A osztály

Az alapbiztonsági osztály az ITSEC F-C2 osztálynak feleltethető meg logikai védelmi szempontból.

Minimális követelmény

- Az azonosítás és hitelesítés keretében a hozzáférést jelszavakkal kell ellenőrizni. A jelszó menedzselést úgy kell biztosítani, hogy a jelszó ne juthasson illetéktelenek tudomására, ne legyen könnyen megfejthető, megkerülhető.
- A rendszer hozzáférés szempontjából érdekes erőforrásaihoz (processzek, fájlok, tároló területek, berendezések) olyan egyedi azonosítót kell rendelni, amely a hozzáférési jogosultság meghatározásának alapjául szolgál.
- On-line adatmozgás (tranzakció) kezdeményezésének jogosultságát minden esetben ellenőrizni kell.
- Ki kell dolgozni az informatikai rendszerhez történő hozzáférések illetékességi, jogosultsági rendszerét.
- A hozzáférés-jogosultság menedzselésénél az ITSEC F-C2 funkcionális követelményszintnek megfelelően kell eljárni.
- A jogosultsági rendszernek támogatnia kell a jogosultságokhoz kapcsolódó adminisztrátori műveleteket (módosítás, törlés, stb.).
- *Az elszámoltathatóság és auditálhatóság biztosítása* logikai védelmi funkciót az ITSEC F-C2 funkcionális szintnek megfelelően kell biztosítani.
- Intézkedési tervet kell kidolgozni arra vonatkozóan, mi történjék illetéktelen hozzáférések, illetve jogosultságokkal való visszaélések esetén, amely során a lehető legnagyobb mértékben meg kell tudni határozni a felelősséget.
- Egy rendszeren belül a különböző adattípusokat olyan mértékben kell elkülönítetten kezelni, hogy megállapítható legyen a hozzáférések jogossága.
- A hitelesítés és az azonosítás, valamint a hozzáférés szabályozás rendszerét a hálózati alapú osztott rendszerek esetén az ITSEC F-C2 funkcionális szinttel azonos egyenszilárdsággal kell megvalósítani.
- Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.
- Az informatikai rendszer üzemeltetéséről nyilvántartást kell vezetni, amelyet az arra illetékes személynek rendszeresen ellenőriznie kell.

Infrastruktúra

- A **falazatok**, a nyílászárók, a **zárak** biztonsági kialakításánál a vonatkozó építészeti szabványok, a MABISZ és a Rendőrség ajánlásai szerint kell eljárni.
- Az intézmény **őrzés-védelme**, az épület zárása, a beléptetés.
- Ahol számítástechnikai eszközökkel történik a munkavégzés, **biztonsági zárral** kell ellátni és a helyiséget távollét esetén zárva kell tartani.
- A dokumentációk **tűz- és vagyonvédett** tárolása.

Hardver, szoftver

- A számítástechnikai eszközökre a **vagyonvédelem** szempontjából a MABISZ ajánlásait kell alkalmazni.
- A felhasználóhoz kötött **jelszó** használat biztosított legyen.
- A **külső eszközről való rendszerindítás** megakadályoztatása.
- **Vírusvédelem**.
- Az **operációs rendszer** és alkalmazások védelme.
- Össze kell állítani és elérhető helyen kell tartani a számítástechnikai eszközök használatára felhatalmazott **személyek névsorát**, feladataikat körül kell határolni.
- A programok, alkalmazások és eszközök tervezése, fejlesztése, tesztelése és üzemeltetése során a biztonsági funkciókat kiemelten és elkülönítetten kell kezelni.

Adathordozók

- Az adathordozó eszközök elhelyezésére szolgáló **helyiségeket** illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen védeni kell
- Adat-átviel, **adathordozók** tarolása, mentése, megbízhatóan zárt helyen történhet
- Az adathordozók beszerzését, tárolását, felhasználását és hozzáférését szabályozni, nyilvántartani, rendszeresen és dokumentáltan **ellenőrizni kell**
- Az adathordozók **nyilvántartása**
- **Leltárba** vett adathordozók használata
- Külső adathordozók **vírusirtás** után használhatóak
- **Adatmegsemmisítés**

Dokumentumok és dokumentációk

- A nyomtatott anyagok kezelését az iratkezelési szabályzat szerint kell elvégezni.
- Az informatikai rendszer biztonságával kapcsolatos dokumentációt az informatikai rendszer biztonsági fokozatának megfelelően kell kezelni.
- Az informatikai rendszer dokumentációját mindig aktualizálni kell.

Adatok

- Hozzáférési kulcsokat (azonosító kártya, jelszó), a jogosultságokat és más, a biztonsággal kapcsolatos paramétereket **titkosítva kell továbbítani**.
- A rendszer biztonságát érintő adatok (pl. jelszavak, jogosultságok, naplók) védelméről a hozzáférési jogosultságok kiosztásánál kell gondoskodni.
- Külső személy - pl. karbantartás, javítás, fejlesztés céljából - a számítástechnikai eszközökhöz úgy férhet hozzá, hogy a kezelt **adatokat ne ismerhesse** meg.
- Az adatbevitel során a **bevitt adatok helyességét** az alkalmazási követelményeknek megfelelően ellenőrizni kell.
- Programfejlesztés vagy próba céljára **valódi adatok felhasználását el kell kerülni**.
- Gondoskodni kell arról, hogy a számítógépen feldolgozott minden adatállomány az adattípust jelölő **biztonsági címkével** legyen ellátva.

Kommunikáció, osztott rendszerek

- Az elektronikus úton továbbított **üzenetek** védelme.
- **Hitelesítési** eljárás.
- Az adott hálózati alrendszer hitelesítési mechanizmusa nem érintheti a hálózat többi alrendszerének hitelesítési rendszerét.
- **Alhálózat** közötti importált adatok.
- A hálózati erőforrások használata.
- A **forgalom monitorozására** és rögzítésére alkalmas erőforrást illetéktelenül ne használjanak.
- Egy alhálózatban definiált azonosító hozzáférési joga delegálható egy másik alhálózatba és ez alapján kell érvényesíteni az eredeti azonosítóhoz rendelt jogokat.
- A szabad belátás szerint kialakított hozzáférés-vezérlést (DAC) ki kell terjeszteni a teljes osztott rendszerre.
- **Központi** hozzáférés-menedzsment .
- A biztonságos **adatcsere** .
- Az **adatvesztés és sérülés** elkerülése céljából hibadetektáló és javító eljárásokat kell alkalmazni.
- Az osztott rendszerben a jelszavak, a jogosultságok és a biztonsággal kapcsolatos más paraméterek, adatok csak **titkosítva továbbíthatók**.

Személyek

- Kitűzők viselete.
- A belépés rendjét a hozzáférési jogosultságokkal összhangban kell szabályozni.
- A magasabb jogosultságú személyeknél el kell kerülni a jogok túlzott koncentrációját.
- Informatikai oktatás továbbképzést a munkaerő számára.
- Az IT biztonságát meghatározó munkakörökben dolgozó munkatársak **helyettesítési** rendjét ki kell alakítani.
- A fontosabb alkalmazásokhoz **rendszergazdákat** kell kinevezni, akiknek feladatkörét pontosan meg kell határozni.
- A **fejlesztői** környezetet el kell választani az **alkalmazói** környezettől, szét kell választani a fejlesztői, működtetői és adminisztrációs hozzáférési jogköröket.
- **Külső partnerekkel** kötött fejlesztési, karbantartási szerződések biztonsággal kapcsolatos részeinek kialakítására pontos szabályozást kell adni.

IV-F osztály

A fokozott biztonsági osztály az ITSEC F-B1 osztálynak feleltethető meg.

Minimális követelmény

- Az **azonosítás és hitelesítés** (ITSEC F-B1)
- A **hozzáférés-szabályozás** (ITSEC F-B1)
- Az adatok minősítését és a feljogosítás műveletét a **vonatkozó és hatályos törvények** szerint kell elvégezni, illetve engedélyezni.
- Az elszámoltathatóság és az **auditálhatóság** (ITSEC F-B1)
- Minősített adatokat kezelő **alhálózatok** összekapcsolási szabályai.

Infrastruktúra

- 12 órás áthidalást biztosító szünetmentesség az elektronikai jelzőrendszerek számára (biztosítható a teljes felület és a részleges térvédelem)
- A személyzet és a külső személyek **belépési** és azonosítási rendjét szabályozott formában kell megvalósítani.
- Az őr- és a biztonsági személyzet létszámát úgy kell kialakítani és olyan eszközzel kell ellátni, hogy eseményt esetén az érintett személy **jelezni tudjon**.

Hardver, szoftver

- A beépített adathordozókon tárolt adatokkal **azonos szinten védendő** minden számítástechnikai eszköz.
- A minősített adatot előállító, feldolgozó, tároló és lekérdező programok, valamint ezek dokumentációi (adat független elemek) minősítéséről az **adatot minősítőnek** kell gondoskodnia.

Adathordozók

- Az adathordozók tárolása csak megbízhatóan zárt helyiségben, minimum 30 perces **tűz-állóságú tároló** szekrényben történhet.
- A fokozott biztonsági osztályba tartozó minősített adatokat tároló **adathordozók** kezelését **törvény** írja elő.
- Az adattípus (minősítés) **felismerhető jelölését** a számítástechnikai berendezéssel előállított adattároló és megjelenítő eszközökön biztosítani kell.
- Az adatok **sértetlen és hiteles** állapotának megőrzését biztosítani kell.

Dokumentumok és dokumentációk

- A felhasználók részére **Biztonsági Kézikönyv** biztosítandó.
- Gondoskodni kell a **változás-menedzsmentről** és a biztonságot érintő változások naplózásáról.
- A rendszerben feldolgozásra kerülő, a fokozott biztonsági osztályba sorolt adatok és a hozzájuk kapcsolódó **jogosultságok nyilvántartását** elkülönítetten kell kezelni.

Kommunikáció, osztott rendszerek

- A **kisugárzással,** illetve a zavartatással kapcsolatos EN 55022 és EN 55024 szabványok a mérvadók.
- A kommunikációs csatornákra vonatkozóan az ITSEC F-B1funkcionális osztálynak az egy, illetve többszintű csatornákon átvitt adatok biztonsági kezelésére vonatkozó követelményei mérvadók.
- A **kötelező hozzáférés-vezérlést** (MAC) ki kell terjeszteni a teljes rendszerre.
- Központi hozzáférés menedzsment esetén az alanyok biztonsági paramétereit biztonságos úton kell az osztott rendszer többi feldolgozó egységéhez eljuttatni.
- A fokozott biztonsági osztályba sorolt adatok forgalmazásával kapcsolatba kerülő valamennyi **hálózati elemre** ki kell terjeszteni a fokozott biztonsági szintnek megfelelő védelmet.
- A hálózaton megvalósítandó a **végpont-végpont szintű jogosultság** ellenőrzés, az elszámoltathatóság és auditálhatóság biztosítása védelmi funkciók.
- Központi auditálás esetén védetten kell továbbítani az **auditálási információkat** a többi alhálózatból.
- A hálózaton történő adatátvitelnél az X/Open ajánlás elosztott rendszerekre vonatkozó ajánlását (X-DIST) kell figyelembe venni a vezérlő és a hasznos adatok, a le nem tagadhatóság, valamint a szolgáltatások rendelkezésre állásának biztosítása szempontjából.
- Az adattovábbításra használt hálózat esetében a biztonsági osztálynak megfelelő szinten biztosítani kell az **illegális rácsatlakozás** és a **lehallgatás** akadályozását.
- A minősített adatok **rejtjelzése** során a 43/1994. (III. 29.) Korm. Rendelet előírásai kötelezőek.

Személyek

- A felhasználók tevékenységének **szelektív szétválasztását** az ellenőrzés céljából biztosítani kell.

- A minősített adatok kezelésében a titokbirtokos és az informatikai rendszert üzemeltető közötti feladat és **felelősség megosztást** szabályozni kell.

IV-K osztály

A kiemelt biztonsági osztály az ITSEC F-B2 osztálynak feleltethető meg.

Minimális követelmény

- Az *azonosítás és hitelesítés* logikai védelmi funkció kialakításánál az ITSEC F-B2 funkcionális követelményeknek megfelelően kell eljárni.
- A *hozzáférés-szabályozás* logikai védelmi funkció kialakításánál az ITSEC F-B2 funkcionális követelményeknek megfelelően kell eljárni.
- Az adatok minősítését és a feljogosítás műveletét a vonatkozó és hatályos a törvények szerint kell elvégezni, illetve engedélyezni.
- A hozzáférési jogok egyedi vagy csoport szinten történő megkülönböztetésénél az ITSEC F-B3 osztály biztonsági követelményeinek a rendszeradminisztrátor, az operátor és a biztonsági felügyelő szerepkörére, valamint a felhasználói jogok odaítélésére, módosítására és visszavonására vonatkozó része veendő figyelembe.
- A biztonsági napló adatait heti rendszerességgel kell ellenőrizni és archiválni.

Infrastruktúra

- A mechanikai védelem **közforgalmú területről** történő betekintés ellen is védjen.
- Az **elektronikai védelem** terjedjen ki a számítástechnikai eszközökre, a felügyelet nélküli helyiségekre.
- A személyzet és a külső személyek belépési és azonosítási rendjét szabályozott formában, **intelligens beléptető-rendszerrel** kell megvalósítani, amely a mindkét irányú áthaladásokat **naplózza** és biztosítja az azonosító eszköz azonos irányban történő többszöri felhasználásának tilalmát.
- A helyiségbe (épületbe) belépni szándékozókat **hitelesíteni** és azokról **nyilvántartást** vezetni kell.

Hardver, szoftver

- Kiemelt biztonsággal védett adathordozókkal azonos szinten védendő fizikailag minden számítástechnikai eszköz, amellyel az ebbe az osztályba tartozó adatokat kezelnek.
- Az informatikai rendszerben moduláris felépítésű, strukturált és védett alrendszerként valósuljon meg a logikai védelem.
- Az *azonosítás és hitelesítés* logikai védelmi funkció kialakításánál az ITSEC F-B2 funkcionális követelményeknek megfelelően kell eljárni.
- A *hozzáférés-szabályozás* logikai védelmi funkció kialakításánál az ITSEC F-B2 funkcionális követelményeknek megfelelően kell eljárni. Strukturált adatállományoknál mező szinten kell kialakítani a hozzáférés szabályozást.
- Az indításvédelmet logikai úton csak aránytalanul nagy ráfordítással lehessen megkerülni.
- A *biztonságos kezelési funkciókat* az X/Open privilegizált jogokat biztosító osztály követelményeinek megfelelően kell kialakítani.
- A biztonságot érintő vagy a fellépési gyakoriságuk miatt biztonsági szempontból kritikus veszélyt jelentő események figyelését az ITSEC F-B3 osztály funkcionális követelményeinek megfelelően kell megvalósítani.

Dokumentumok és dokumentációk

- A referencia hitelesítési mechanizmus dokumentáció struktúrájának és szintjének meg kell felelnie az ITSEC E3 étékelési követelményeknek.
- A változás-menedzsmentet számítástechnikai úton kell megvalósítani.
- Az Informatikai Biztonsági Kézikönyvnek tartalmaznia kell a referencia monitor működésével kapcsolatos ellenőrzési és üzemeltetési eljárások leírását.

Kommunikáció, osztott rendszerek

- Az egy, illetve többszintű kommunikációs csatornák azonosításával kapcsolatos követelményei tekintetében az ITSEC F-B2 osztály funkcionális követelményei a mérvadóak.
- A rejtett kommunikációs csatornák ellenőrzésére és detektálására vonatkozó követelmények tekintetében az ITSEC F-B2 osztály funkcionális követelményeinek A. 52 pontja mérvadó.
- Az adatáramlás bizalmasságának megőrzése céljából ajánlott **szelektív útvezérlés** (selective routing) alkalmazása.
- A **kábelezésre** vonatkozóan az EIA/TIA-568 Kereskedelmi Épületkábelezési Szabvány, valamint a kisugárzással, illetve a zavartatással kapcsolatos EN 55022 és EN 55024 szabványok a mérvadók.

Személyek

- **Új** jogosultság kiosztásával, a jogosultság **törlésével**, átmeneti **felfüggesztésével**, valamint az informatikai rendszer használata közben más módon beállt biztonsági szint változásokkal kapcsolatban az ITSEC F-B2 funkcionális követelményei A.50 és A.51 pontjai mérvadók. (ITSEC B3-ból)
- A Biztonsági Kézikönyv felhasználásával rendszeres **oktatást** és **vizsgáztatást** kell rendszeresíteni.
- A biztonsági személyzet feladatát "**vállalkozás keretében**" nem láthatja el.

ITB 15 ajánlás

MEGBÍZHATÓ MŰKÖDÉS

RENDELKEZÉSRE ÁLLÁS

Megbízható működés

Az informatikai rendszerek megbízható működését úgy értelmezzük, hogy az **alkalmazói rendszernek** (felhasználói programok és adatok) a tervezés és megvalósítás során kialakított **funkcionalitását** egy megbízható informatikai alaprendszer (hardver és alapszoftver) az adott biztonsági osztálynak megfelelő követelményeknek megfelelő szintű rendelkezésre állással biztosítja a **felhasználó részére**.

Rendelkezésre állás

- Rendelkezésre álláson azt a valószínűséget értjük, amellyel egy definiált **időintervallumon belül** az alkalmazás a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható.

- **Rendelkezésre áll** egy alkalmazás vagy erőforrás, mikor a működésének képes eleget tenni, képes feladatokat fogadni, működni. Értékét százalékban adják meg.

- **Szerverek** esetén ez az az idő, amikor képesek kiszolgálni a klienseket.

Rendelkezésre állás

$$\text{Rendelkezésre állás (R)} = \frac{T_{üz} - \sum_{üz} T_{ki}}{T_{üz}} \times 100(\%)$$

ahol $T_{üz}$ az üzemidő periódus, amelyre a rendelkezésre állást értelmezzük és T_{ki} a kiesési idő egy alkalomra.

$T_{üz}$ = 1 hónap	Rendelkezésre állás (R)	Megengedett kiesési idő $(S T_{ki})$	Megengedett legnagyobb kiesési idő egy alkalomra $(max T_{ki})$
A megbízható működési alapbiztonsági (MM-A) osztály	95,5 %	23,8 óra	-
A megbízható működési fokozott biztonsági (MM-F) osztály	99,5 %	2,6 óra	30 perc
A megbízható működési kiemelt biztonsági (MM-K) osztály	99,95 %	16 perc	1 perc

A kiesési időt befolyásolják:

- az újraindítási képesség megvalósítása,
- a hibaáthidalás folyamatának kialakítása,
- a rendszerkonfiguráció hatékony menedzselése.

Rendelkezésre-állás menedzsment

- **Megbízhatóság (reliability)**: egy információtechnológiai összetevő azon képessége, hogy ellásson egy megkívánt funkciót meghatározott körülmények között, egy meghatározott időtartamra.
- **Karbantarthatóság (maintainability)**: egy számítógépes komponens vagy szolgáltatás azon képessége, hogy meg lehet tartani egy olyan állapotban, vagy vissza lehet állítani egy olyan állapotba, amelyben képes ellátni a megkívánt funkciót.
- **Szolgáltatási képesség (serviceability)**: szerződéses kikötés, amely meghatározza az informatikai komponens rendelkezésre-állását az adott összetevőket szolgáltató és karbantartó külső szervezettel való megegyezés szerint.
- **Biztonság (security)**: lehetővé teszi a számítógépes komponensek vagy informatikai szolgáltatások elérését biztonságos körülmények között.

Rendelkezésre-állás menedzsment

Az informatikai rendszereket és szolgáltatásokat úgy kell tervezni, hogy

- megbízhatóak,
- hibatűrők és
- karbantarthatók

legyenek **teljes életciklusuk** során, a tervezéstől, a megszüntetésükig.

Rendelkezésre-állás menedzsment

- a **kézi rendszerekre** való visszaállás gyakorlatilag **lehetetlen**,
- a **felhasználók hatékonysága** és eredményessége erősen függ az informatikai szolgáltatások rendelkezésre-állásától és megbízhatóságától,
- a szervezeti felhasználók tevékenysége az **informatikán alapul**, amely nélkül a szervezet működésképtelen.

Rendelkezésre-állás menedzsment

Az informatikai szolgáltatásokat nyújtó rendszerek megbízhatóságát a következők **befolyásolják**:

- az informatikai infrastruktúra összetevők megbízhatósága és karbantarthatósága, ill. a környezet, amelyen e rendszerek alapulnak,
- a szállítók és külső partnerek, akik a karbantartást végzik,
- az informatikai szolgáltató szervezet által használt eljárások és eszközök,
- az informatikai szolgáltatásokat nyújtó informatikai infrastruktúra konfigurációja.

Rendelkezésre-állás menedzsment

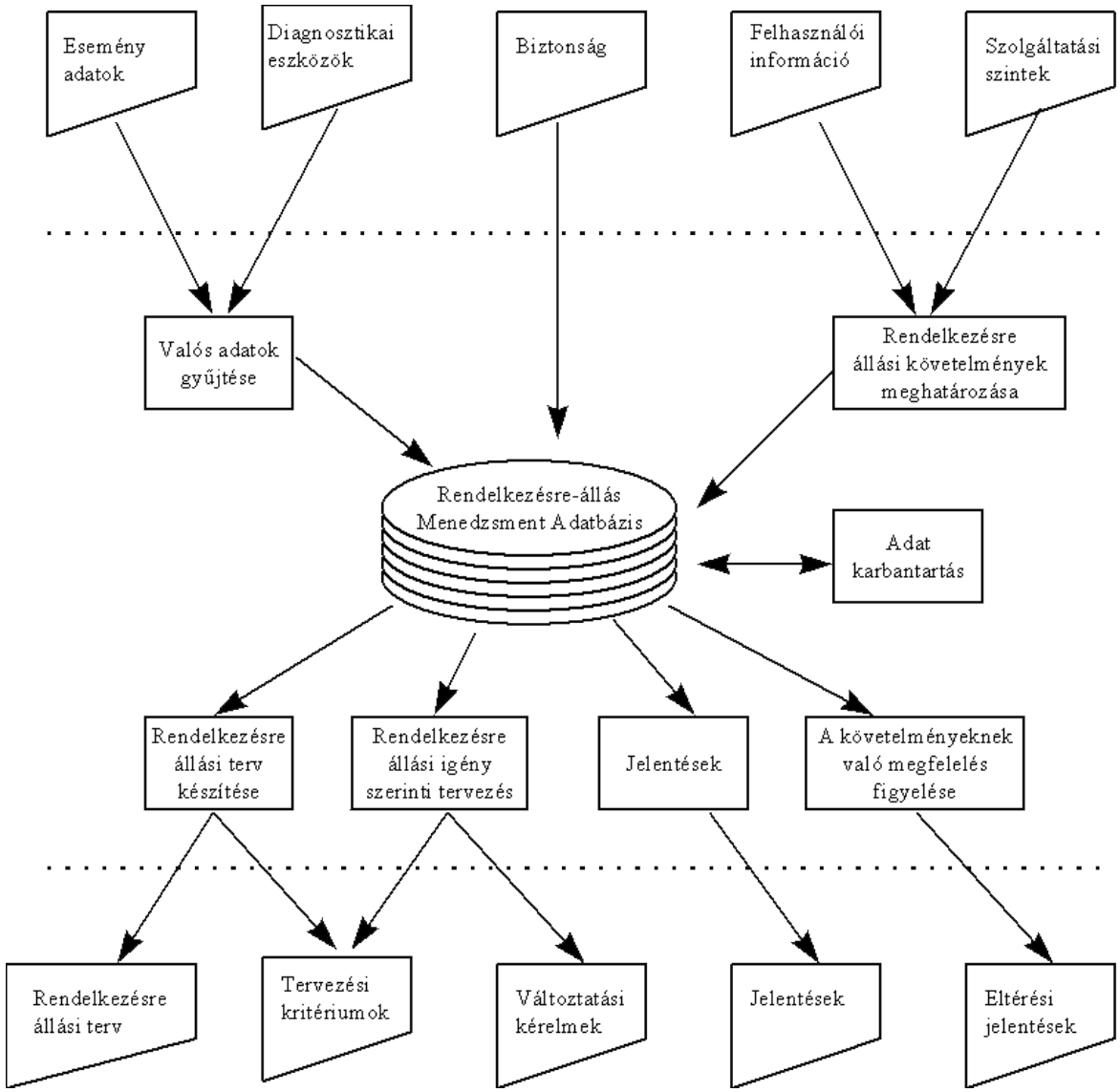
A hatékony és eredményes rendelkezésre-állás menedzsment a következő **hasznokat** eredményezi:

- az informatikai szolgáltatások **javuló minőségét**,
- az új és meglévő informatikai szolgáltatások **költség-hatékony** nyújtását,
- az informatikai infrastruktúra **javuló menedzselhetőségét**,
- **jobb tervezési** képességét,
- az informatikai szolgáltatások **biztonságosabb** nyújtását

Rendelkezésre-állás menedzsment

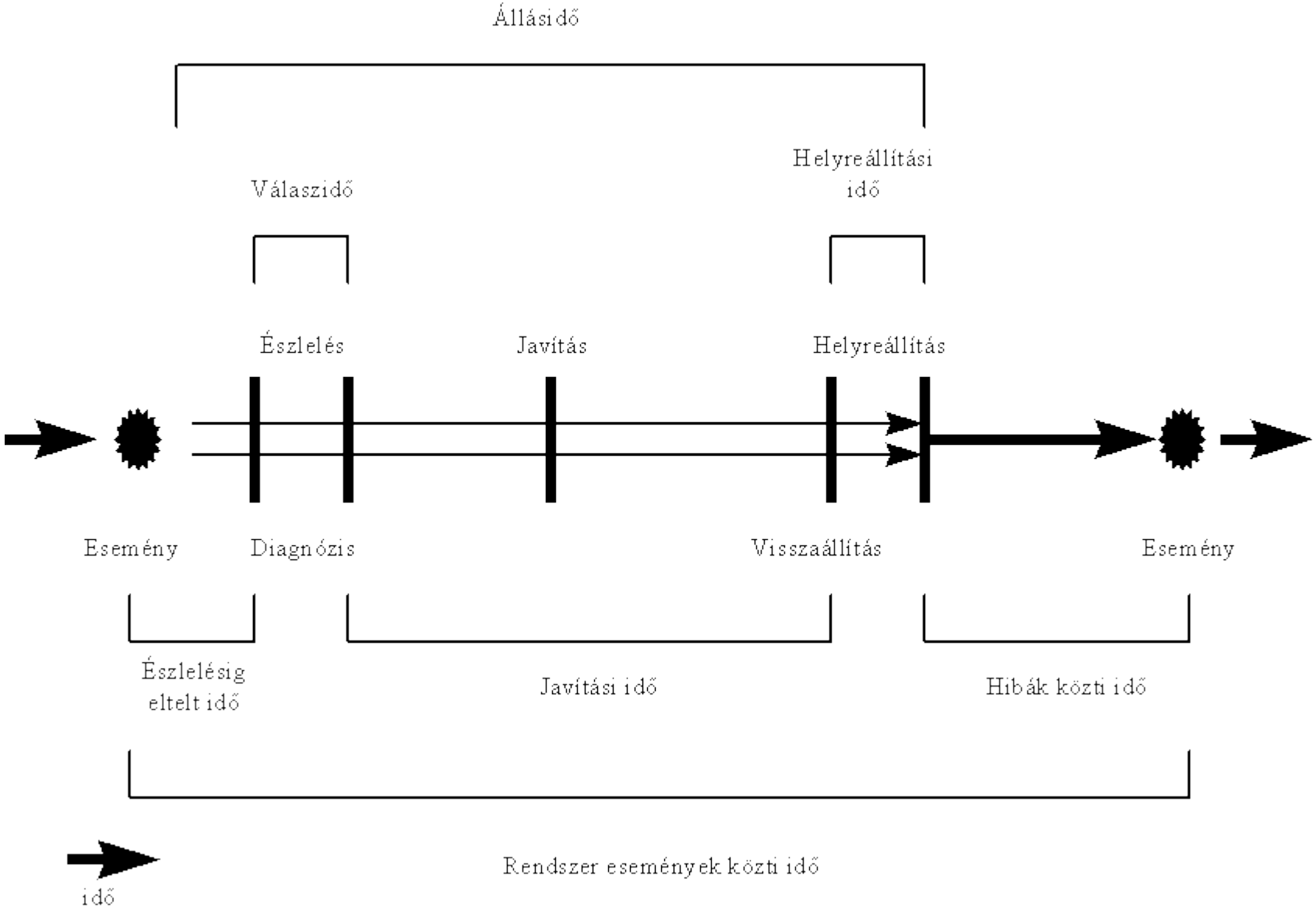
A rendelkezésre-állás menedzsment funkciónak két fő **felelősségi területe** van:

- **Tervezési feladatkör**; azaz a rendelkezésre-állás fenntartása az informatikai infrastruktúra változásai és a felhasználói követelmények változásai közepette.
- **Üzemeltetési feladatkör**; azaz valós adatok gyűjtése és a követelményeknek való megfelelés figyelemmel kísérése.


Esemény adatok
Diagnosztikai eszközök
Biztonság
Felhasználói információ
Szolgáltatási szintek
Valós adatok gyűjtése
Rendelkezésre állási követelmények meghatározása
Rendelkezésre-állás Menedzsment Adatbázis
Adat karbantartás
Rendelkezésre állási terv készítése
Rendelkezésre állási igény szerinti tervezés
Jelentések
A követelményeknek való megfelelés figyelése
Rendelkezésre állási terv
Tervezési kritériumok
Változtatási kérelmek
Jelentések
Eltérési jelentések

A rendelkezésre-állás javítására két fő lehetőség van:

- csökkenteni kell a hibánkénti **állásidőt**,
- csökkenteni kell az adott időtartamon belüli **hibák számát**.


Állásidő
Válaszidő
Helyreállítási idő
Észlelés
Javítás
Helyreállítás
Esemény
Diagnózis
Visszaállítás
Esemény
Észlelésig eltelt idő
Javítási idő
Hibák közti idő
Rendszer események közti idő
idő

A következő adatelemeket kell összegyűjteni:

- dátum és idő, amikor a komponens **nem működik**, pl. egy hiba (bekövetkezési) ideje,

- dátum és idő, amikor a komponens **üzemelni kezd**, azaz a komponens sikeres helyreállításának ideje.

A külső szervezettel való kapcsolat

- Annak időpontja, amikor a külső szervezetet **értesítették** (call-out time).
- Annak időpontja, amikor a külső szervezet átadta a komponenst az informatikai szervezet számára üzemi körülmények között (**üzemeltethető állapotban**).
- Azon időadatok, amelyek egyéb **szerződéses feltételekhez** kötődnek, mint pl. a szolgáltató mérnök a helyszínre kell érjen az értesítést követő két órán belül - ezeket szintén gyűjteni kell.