INFORMATIKAI PROJEKTELLENŐR

DR. BEINSCHRÓTH JÓZSEF

IT RENDSZEREK ÜZEMELTETÉSE ÉS BIZTONSÁGA

Tartalom

- **Alapfogalmak**
- **Alapvetések**
- **Veszélyforrások – védelmi módszerek**
  - Fizikai
  - Logikai
  - Szervezeti-szervezési
  - Életciklushoz kapcsolódó
- **Informatikai katasztrófahelyzet**
- **Üzemeltetés - szolgáltatás**
- **Üzemeltetett rendszerelemek**
- **Üzemeltetési tevékenységek**
- **Üzemeltetési dokumentáció**

Alapfogalmak

Informatika: Az informatika a tudomány és technika azon területe, amely az információk keletkezésének, kezelésének és felhasználásának elméletével, gyakorlati megvalósításával és eszközrendszerével foglalkozik.

Informatikai rendszer: Eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására létrehozott rendszere. (Üzemeltetés: felügyelet, karbantartás, hibaelhárítás, fejlesztési javaslatok…) (Az IT üzemeltetés és biztonság átfednek!)

Biztonság: Zavartalan, ártalmas hatástól mentes kedvező állapot, megváltozása nem kizárható, de kis valószínűségű. (Dinamikus állapot (folyamat))

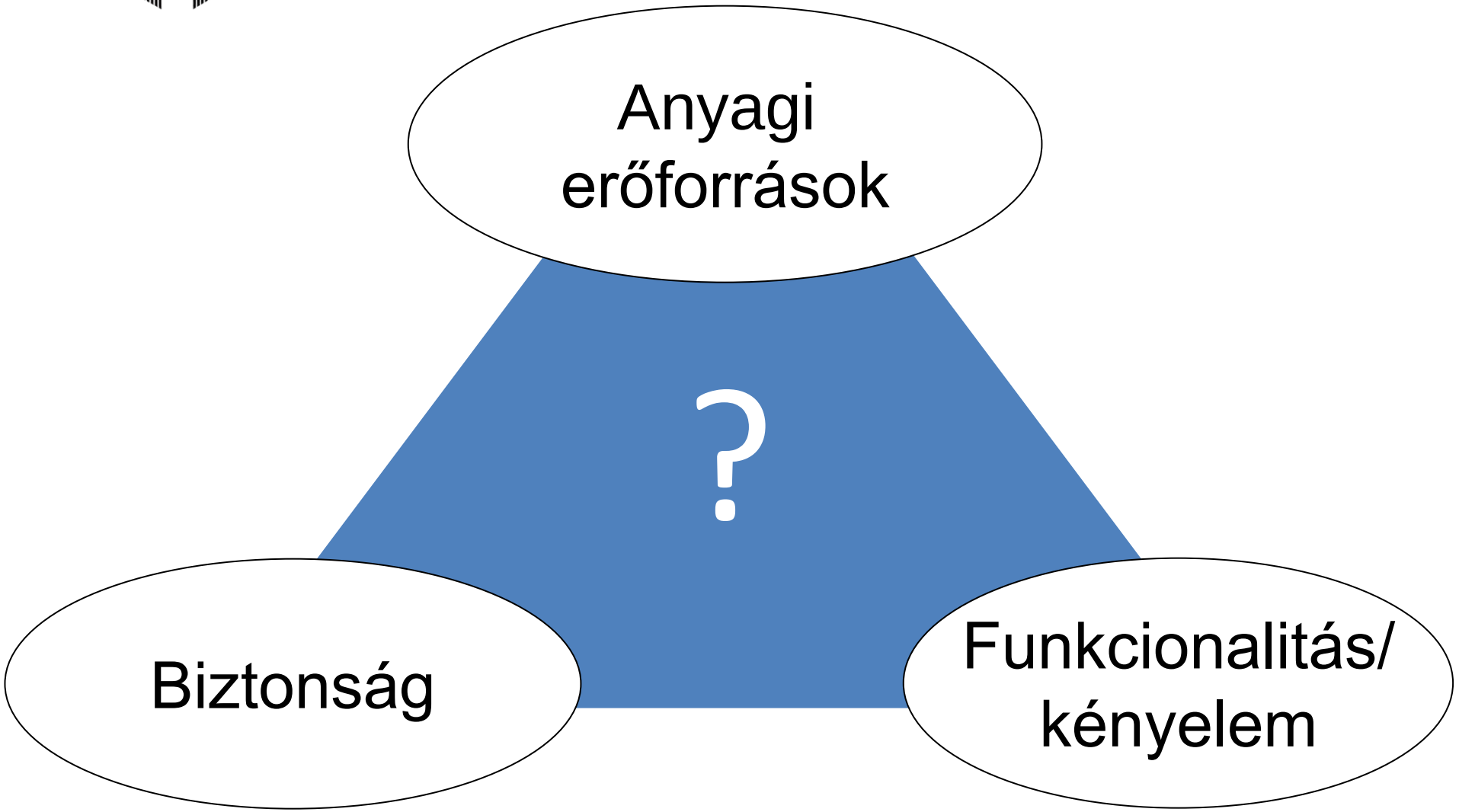
Informatikai biztonság: Az informatikai erőforrások bizalmassága, sértetlensége, rendelkezésre állása minimálisan fenyegetett, azaz a kedvező állapot megváltozásának valószínűsége igen kicsi.

Bizalmasság: Az a tulajdonság, amely arra vonatkozik, hogy az információt csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

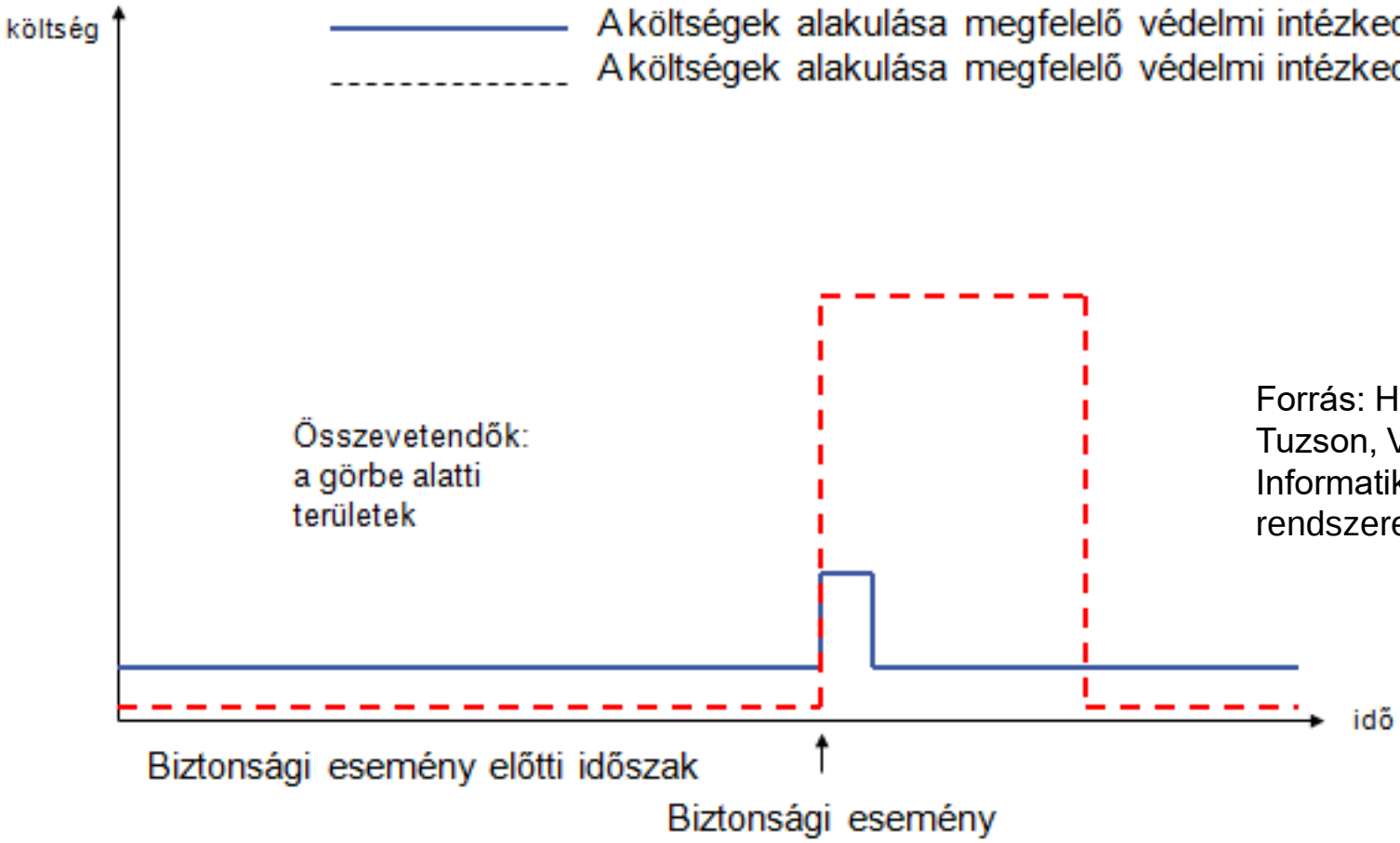
Sértetlenség: Az eredeti állapotnak megfelel, fizikailag és logikailag teljes és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik

Rendelkezésre állás: Az eredeti rendeltetésnek megfelelő szolgáltatások nyújtása, meghatározott helyen és időben, megfelelő performanciával.

Alapvetések (1)



Alapvetések (2)



Forrás: Horváth, Lukács, Tuzson, Vasvári: Informatikai biztonsági rendszerek

Veszélyforrások – védelmi módszerek

Fizikai

Logikai

Szervezeti-szervezési

Életciklushoz Kapcsolódó

Veszélyforrások – védelmi módszerek

Negatív környezeti hatások (természeti jelenségek és technikai katasztrófák, tűz)

Jogosulatlan hozzáférések (aktív és passzív hozzáférések)

Kiesések (bombariadó, nem megfelelő légállapot, nem megbízható eszközök, az energiaellátás és távközlés zavarai)

Hibás dokumentáció (aktualizált, használható, jóváhagyott dokumentáció szükséges)

Veszélyforrások – védelmi módszerek

- Jogosulatlan hozzáférések (jelszavak, PIN kódok, biometria, kriptográfiai kulcsok)
- Kiesések (szoftver hibák, hibás méretezés – túlterhelés, mentések, hátterek)
- Szigetszerű működés (Izolált rendszerek)
- Malware-ek hatása (vírus, baktérium, trójai, keylogger, logikai bomba, phising…)
- Hacker tevékenyég (Inkorrekt kódok, weboldal feltörés…)
- Logikai rombolás (elektromágneses támadás (vezetékes, sugárzásos))
- Hálózati problémák (illetéktelen rácsatlakozás: hozzáférés,módosítás, rombolás)
- Hibás dokumentáció (aktualizált, használható, jóváhagyott dokumentáció szükséges)

Veszélyforrások – védelmi módszerek

„Ad hoc” szervezeti működés (működési folyamatok, szervezeti felépítés, feladatok, felelősségek, hatáskörök és erőforrások, szabályozások)

Gyenge biztonsági szervezet (IT biztonságért felelős szervezet, munkatárs helye a szervezeti hierarchiában; vagyon és adatbiztonság elkülönültsége, ellenőrzések hiánya, oktatások, segregation of duties)

Emberi hibák (rendelkezésre állás, kompetencia, lojalitás, megbízhatóság, végzettség, tapasztalat, biztonsági tudatosság)

Titokvédelmi és iratkezelési hiányosságok (adatok, alkalmazások, eszközök, helyiségek, titkos ügyiratkezelés)

Szerződések gyengeségei (IT biztonsági garanciák a szerződésekben, korlátozott felelősségvállalás)

Jogszabálysértés (IT biztonsági és ágazati törvények)

Veszélyforrások – védelmi módszerek

Fejlesztés, beszerzés (követelmények, elkülönült fejlesztő rendszer, biztonsági garanciák, elterjedt, szabványos szoftverek)

Átadás-átvétel (biztonsági követelményrendszer ellenőrzése, az átvételi teszt a biztonsági követelmények ellenőrzésére, speciális hozzáférések (programozók spec. jogosultságai), hátsó ajtók, a dokumentáció hiánya

Üzemeltetés (Fizikai, logikai, szervezeti-szervezési…)

Kivezetés, selejtezés (adathordozók, selejtezési rend)

ACTIVITY – Esettanulmány

Adott egy kerületi rádió, amely az interneten keresztül szolgáltat műsort elsősorban a kerület lakói számára, naponta 6-22 óráig. Költségeit önkormányzati támogatásból és reklámbevételekből fedezi. Fő erőforrásai: stúdió, média szerver, internet kapcsolat, technikai személyzet és műsorvezetők és az önkormányzat alkalmazásában álló rendszergazda.

Az erőforrások csak a szükséges mennyiségben állnak rendelkezésre, tartalékok nincsenek, a média szerverről éjszakánként szalagos mentés készül. A mentéseket az önkormányzat egy tűzbiztos páncélszekrényében tárolják.

A műsorok jellemzően a médiaszerveren tárolt felvételek és élő közvetítések a stúdióból. Külső helyszíni közvetítések csak kivételesen fordulnak elő.

A rádióstúdió a kerületi művelődési központ épületében található, a helyszíni szünetmentes tápláláson túlmenően helyszíni villamos energia nem áll rendelkezésre. Az internet kapcsolat redundancia nélküli, vezetékes kapcsolat. A rádió műsora egy hétre előre az önkormányzat web szerverén elérhető.

FELADAT:

Azonosítsunk az esethez tartozó veszélyforrásokat és alkalmazható védelmi intézkedéseket!

A preventív megközelítés nem elegendő – katasztrófa terv

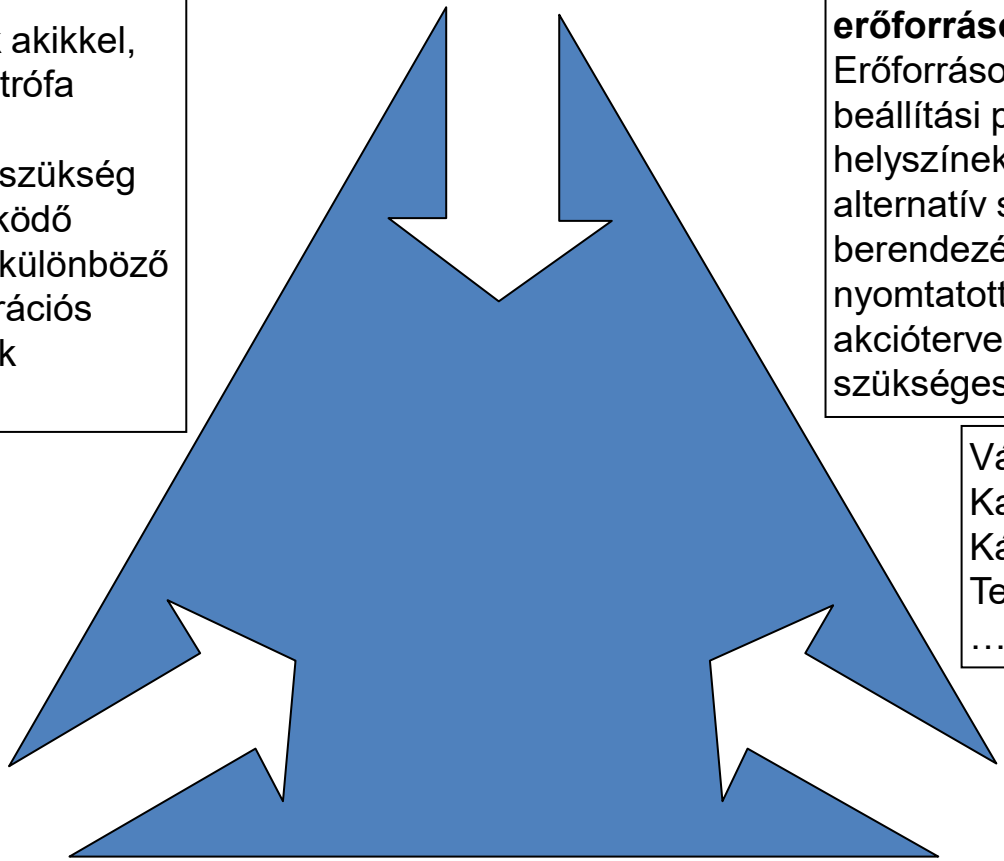
Konkrét tények és adatok, amelyek egy esetleges folyamat kiesés (katasztrófa helyzet) esetén azonnal szükségesek.

Elérhetőségek:

Személyek, szervezetek akikkel, illetve amelyekkel katasztrófa helyzetben gyors kapcsolatfelvételre lehet szükség (pl. közvetlenül közreműködő operatív munkatársak, a különböző beszállítók, hardver, operációs rendszer ill. alkalmazások forgalmazói).

Alternatív helyszínek, erőforrások:

Erőforrások jellemzői, esetleges beállítási paraméterei. Gyülekezési helyszínek. Tartalék helyszínek (pl. alternatív szerverszoba).Tartalék berendezések. Az akciótervek nyomtatott példányai.Az akciótervek végrehajtásához szükséges erőforrások.…



Válságtanács
Katasztrófa menedzser
Kárfelmérő team
Technikai visszaállító team
…

A folyamatok kiesése esetén alkalmazható **szükséghelyzeti tervek** és **akciótervek** valamint **helyettesítő tevékenységek**.

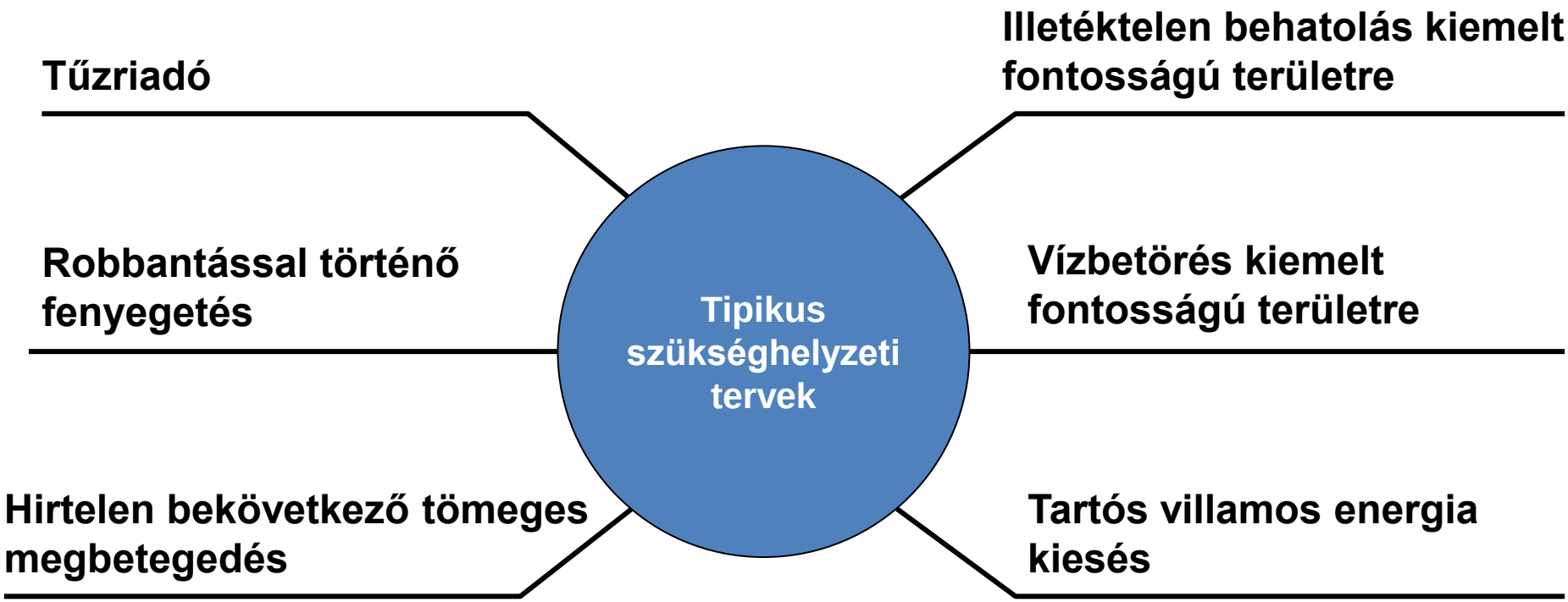
A folyamatok kiesése esetére kialakított szervezeti egység definiálása (katasztrófahelyzet kezelő szervezet).

Az akciótervek számos paramétert tartalmaznak

Az akciótervek leírása folyamatként történhet

#	„Átadó”	Input Objektum	Tevékenység	Tevékenységért felelős	Output Objektum	„Átvevő”	Megjegyzés
1	Bármely munkatárs	Az informatikai hálózat állapota	A vírusfertőzés kiterjedtségének előzetes meghatározása, a fertőzött rész leválasztása.	Rendszer-gazda	Szegmentált hálózat	Rendszer-gazda	Egy-egy kliens gép vírusfertőződése nem indokolja az akcióterv végrehajtását.
2	Rendszer-gazda	A vírusfertőzés ténye	A személyzet tájékoztatása	Rendszer-gazda	Értesítés	Személyzet	
3	Rendszer-gazda	Fertőzött hálózat	A fertőzés okának felderítése, tájékozódás az adott vírusról	Rendszer-gazda	A fertőzés bekövetkezésének ismert oka	Rendszer-gazda	Pl. frissítés elmaradása
	…	…	…	…	…	…	…

A szükséghelyzeti tervek a kisebb jelentőségű eseteket fedik le



A folyamatok átmeneti működtetése informatikai rendszer nélkül

Helyettesítő tevékenységek

- **Tipikusan csak korlátozott ideig folytathatók.**
- **Nem garantálják a hatékony működést, nem feltétlenül költségoptimálisak**
- **Korlátozott kapacitást tudnak biztosítani**
- **Alkalmazásuknak speciális feltételei vannak**

Példa:

Az ERP rendszer kiesése esetén a rendszer által támogatott folyamatok egy része átmenetileg papír alapon, manuálisan végzett tevékenységekkel fenntartható lehet.

A katasztrófa tervhez kapcsolódó tevékenységek (1)

Karbantartás

- A naprakészség biztosítása szükséges
- Teljes körű karbantartás meghatározott időnként (tipikusan évente) ill. új kritikus folyamat esetén szükséges
- Részleges karbantartás (erőforrások rendelkezésre állása, módosulása, naprakészség)

Tesztelés

- A tesztelés módja (éles?, szimulációs vagy szóbeli)
- A tesztelési tervnek tartalmaznia kell az elvárt eredményeket. A tesztelési jegyzőkönyvet a katasztrófa menedzser köteles kiértékelni. Abban az esetben, ha a tesztelt akcióterv végrehajtása során elért eredmények elmaradnak az elvárttól, meg kell határozni az eltérés okát és el kell végezni a szükséges korrekciókat.
- A tesztelését minden évben, a kötelezően előírt karbantartást követően célszerű végrehajtani, törekedve arra, hogy a felülvizsgálat során bekövetkezett módosulások tesztelésre kerüljenek.

A katasztrófa tervhez kapcsolódó tevékenységek (2)

Oktatás

- Ismertető és gyakorlati rész
- Általános, biztonsági tudatot növelő oktatás
- A konkrét tervek oktatása a felelősök számára (az érintett munkatársaknak pontosan tudniuk kell, hogy mi a szerepük a katasztrófát követő munkában, milyen felelősséggel és hatáskörrel rendelkeznek (ez eltérhet a normál munka során betöltött szerepektől), és konkrét feladataikat végre is tudják hajtani
- Az oktatásra gyakoriságának meghatározása (Gyakorlat: legalább évente – a tesztelésekkel összhangban)
- Az új belépő munkatársak oktatása is szükséges.
- Az oktatás megtehető az egyébként szükséges munka, tűzvédelmi stb. oktatásokkal együtt

Tárolás

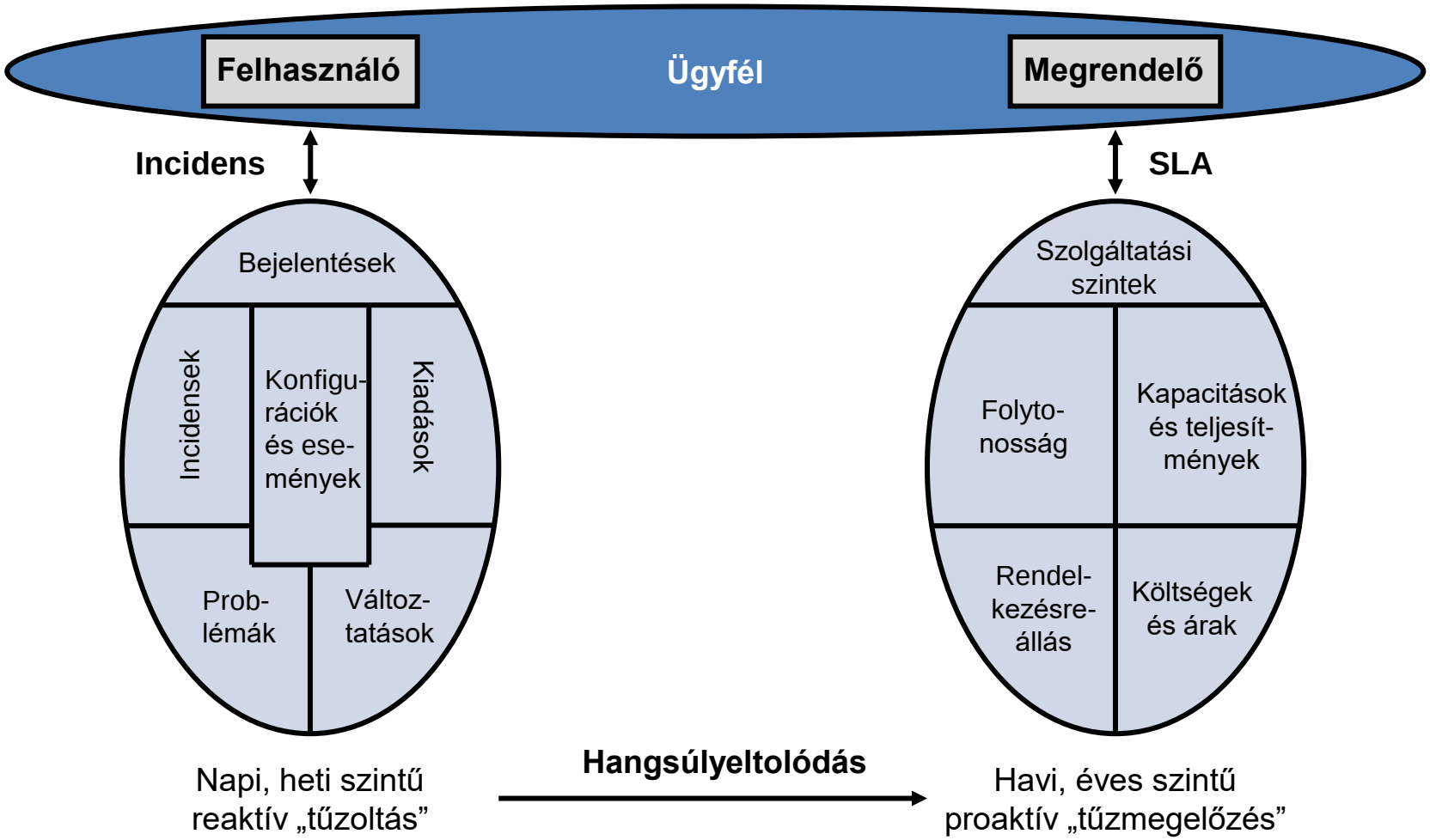
- Alternatív, de könnyen elérhető helyszínen, csak az utolsó (érvényes) változat létezzen
- A katasztrófa terv bizalmas dokumentum!

ACTIVITY - akcióterv

Készítsünk akciótervet a kerületi rádió esetén azonosított veszélyforrások valamelyikének kezelésére!

#	„Átadó”	Input Objektum	Tevékenység	Tevékenységért felelős	Output Objektum	„Átvevő”	Megjegyzés
1							
2							
3							

Üzemeltetés - szolgáltatás



forrás: IQSOFT – John Bryce oktatóközpont: ITIL Foundation Certification

Üzemeltetett rendszerelemek

- Alkalmazások (kliens és szerver oldal)
- Adatbázisok
- Felügyeleti rendszerek
- Virtuális rendszerek
- Operációs és virtuális rendszerek (kliens és szerver rendszerek)
- Hálózat (aktív és passzív elemek)
- Hardver (szerverek és munkaállomások)
- Kiszolgáló infrastruktúra (klíma, UPS, szerver szoba stb.)

Üzemeltetési tevékenységek

Rendszeres és eseti tevékenységek

Tipikus hibák kezelése (incidens és problémakezelés)

Mentés (mit, mikor, teljes/inkrementális, mivel, milyen gyakran, mennyi ideig őrizzük, hol tároljuk?)

Naplózás (elérhetőség, megőrzési idő, selejtezés)

Emberi tényező (Az üzemeltetési tevékenységek fontos feltétele!)

Üzemeltetési dokumentáció

Az informatikai rendszerek üzemeltetési dokumentációjának célja, hogy számba vegye és rögzítse az üzemeltetés során felmerülő rendszeres és eseti tevékenységeket és ezzel egyúttal támogassa a rendszer üzemeltetéséhez szükséges képesítéssel és gyakorlattal rendelkező üzemeltető személyzetet.

Egy teljes informatikai rendszer üzemeltetési dokumentációja általában számos, tipikusan hierarchiát alkotó dokumentumrendszer, amelyek tartalma kiterjed a kiszolgáló infrastruktúrától (klíma, UPS stb.) a konkrét alkalmazásokig. Ezeket ki kell, hogy egészítsék az igazoló jellegű dokumentumok (riportok, teszt jegyzőkönyvek stb.), amelyek elsősorban a bekövetkezett események visszakövethetőségét teszik lehetővé.

Üzemeltetési dokumentáció - szerkezet

- Dokumentum azonosítás
- A rendszer(ek) üzemeltetése során érvényesítendő üzleti követelmények
- A rendszer(ek) leírása (tipikusan hivatkozás más dokumentumra)
- Felügyeleti eszközök és felületek
  - Saját
  - Külső
- Tevékenységek
  - Rendszeres
    - Heti
    - Havi
    - Évi
  - Eseti (ITIL szerint)
    - Incidenskezelés
    - Eseménykezelés
    - Változáskezelés
    - Kiadáskezelés
    - Konfiguráció kezelés
    - Igények kezelése
    - Hozzáférés kezelés
  - Tipikus hibák kezelése

- Mentések- visszaállítások
- Naplózás
  - Elérhetőség
  - Megőrzési idő
  - Selejtezés
- Emberi tényezők
  - Az üzemeltetéshez szükséges kompetenciák
  - A felhasználáshoz szükséges kompetenciák
  - Szerepkörök, privilégizált felhasználók és felelősségi köreik
- Sablonok (riportok, tesztek stb.)

Köszönöm a figyelmet!