Bevezetés a kiberbiztonságba - Biztonságtudatosság

Üzletmenet-folytonosság tervezése

Bonifert Tamás

2023. 05. 18.

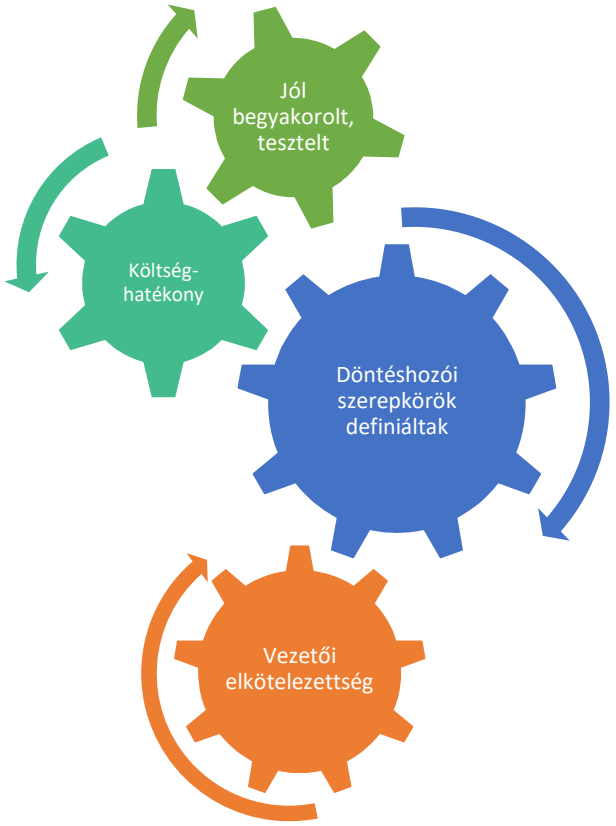
Mi az üzletmenet-folytonosság tervezés?

Forrás: ISO 22301, Stay in Business

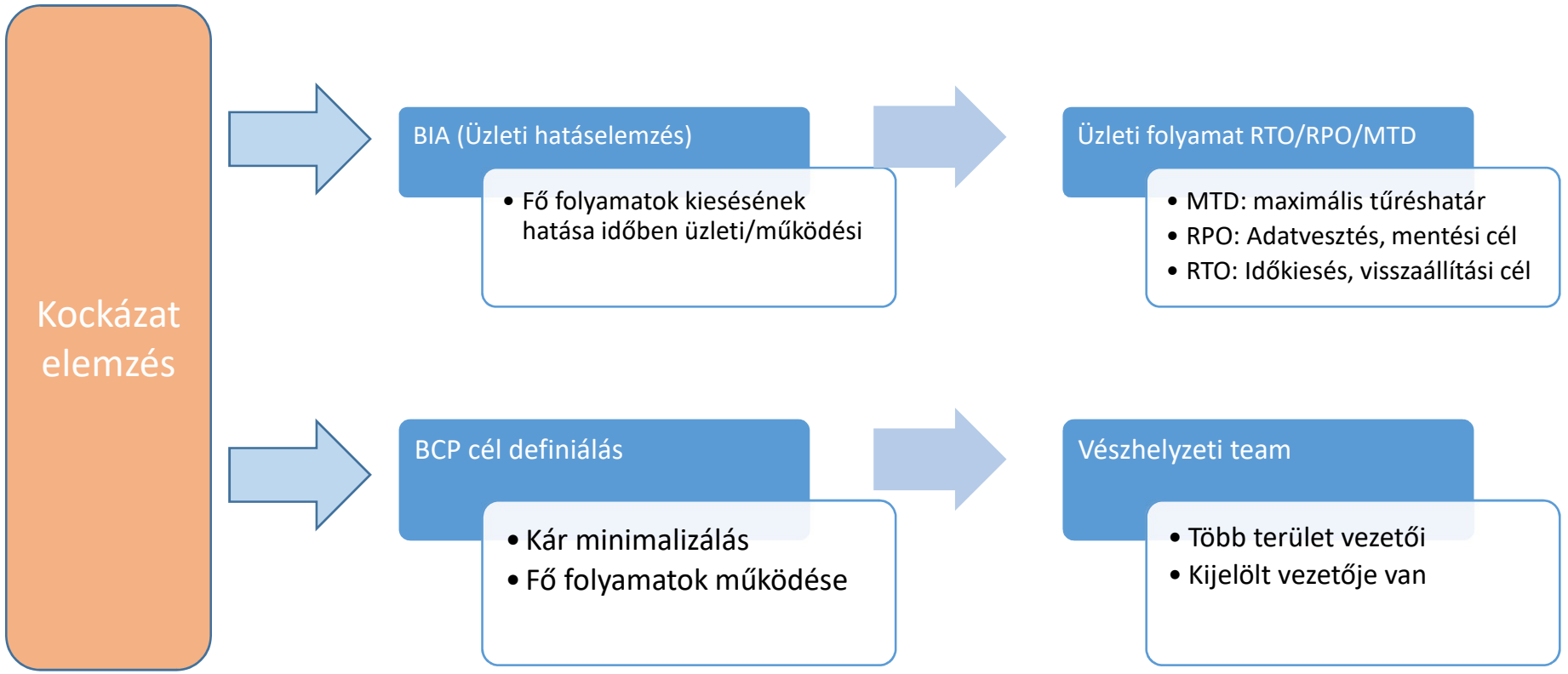
- Az a folyamat, melynek során a szervezet felkészül az üzleti folyamatok kiesés utáni visszaállítására, kár minimalizálással
- Kockázat menedzsment képezi az alapját: mire kell felkészülni?
- Az üzleti területek bevonása alapvető: az üzleti terület határozza meg a kiesések hatását, és az elfogadható kiesési időt: BIA
- Tartalmaz alternatív üzleti folyamatokat, illetve a támogató IT rendszer előkészítését, és visszaállítási lépéseit
- Folyamatos működtetést, tesztelést, karbantartást, és képzést igényel
- BCDR: a rendszer leállás utáni visszaállítása (DRP), és az üzleti folyamatok folyamatossága (BCP) egy egységet képez

BCDR sikerkritériumok

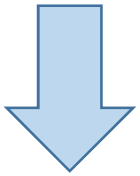
- Minden érintett tudja, hogy mi a dolga leállás esetén: jól begyakorolt, letesztelt BCP/DRP tervek
- Költséghatékony: minél gyorsabban kell visszaállítani egy folyamatot, annál drágább a DRP stratégia –> üzleti hatáselemzés
- Definiált döntéshozói szerepkörök: katasztrófahelyzet esetén létfontosságú a fejetlenség elkerülése. Világos döntésekre van szükség, melyhez dedikált szerepkörökre van szükség.
- Vezetői elkötelezettség és jóváhagyás



BCDR folyamata



BCDR folyamata



Támogató erőforrások
- A kritikus folyamatokat támogató erőforrások (IT, humán, stb.)

Alternatív folyamatok
- Helyettesítő folyamat a normál működés helyreállásáig

Visszaállítási stratégiák
- Alternatív site
- Alternatív szolgáltatás
- Mentés
- Redundancia

Tesztelés, tudatosság
- Tervek éves tesztelése
- Érintettek oktatása, BCP/DRP tervek begyakoroltatása

Üzleti hatáselemzés (BIA) és a BCDR kapcsolata

1. Az üzleti terület meghatározza a kritikus folyamatokat és kiesésük hatását
2. Az üzleti terület meghatározza a kritikus adatköröket és az adatvesztési toleranciát
3. Az IT terület a kritikus folyamatokhoz meghatározza a támogató IT erőforrásokat
4. A BIA eredménye
   - a kritikus folyamatok MTD értékei
   - Erőforrások, IT rendszerek felé támasztott RTO értékek
   - a kritikus adatok RPO értékei, mentési stratégia

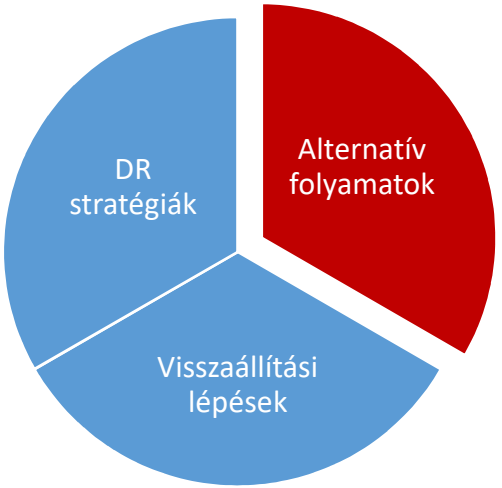
Üzleti hatáselemzés (BIA)

- Tisztán üzleti elemzés, nem műszaki
- Célja, hogy meghatározza a leállás által okozott kárt
- Minden üzleti folyamathoz meghatározza az MTD értéket
- Meghatározza, hogy az MTD-n túli leállás naponta, hetente mekkora kárt okoz
- A hatás lehet kvalitatív (hírnév), vagy kvantitatív (anyagi)
- Interjús módszerrel végezzük egy területi vezető és egy szakértő dolgozó bevonásával
- Tartsuk szem előtt, hogy minél kisebb az MTD, annál drágább lesz a DRP stratégia

NEM ELEMZI A LEÁLLÁS OKÁT, CSAK AZ OKOZOTT KÁRT AZ IDŐ FÜGGVÉNYÉBEN

Alternatív folyamatok (BCP)

- Üzletmenet-folytonossági tervezés része
- Proaktívabb megközelítés, mint a DRP
- Alternatív folyamatokat fejleszt ki arra az esetre, ha az IT rendszer leáll
- Biztosítja, hogy a kritikus folyamatok a leállás alatt is működjenek (pl. papíros könyvelés)
- Holisztikusabb megközelítés, vállalat fókuszú
- Rendszeres tesztelése, gyakorlása szükséges, hogy jól begyakorolt legyen, és naprakészen illeszkedjen az eredeti folyamathoz



Visszaállítási lépések (DRP)

- Katasztrófa-elhárítási tervezés része
- Reaktív megközelítés, az incidens megtörténtére indulnak a lépések
- Célja, hogy az IT rendszert a meghatározott idő alatt vissza lehessen állítani eredeti működési szintre.
- Technológiai fókuszú megközelítés
- Rendszeres tesztelése, gyakorlása szükséges, hogy előjöjjenek az IT rendszerek hibái, a DRP előkészületek hiányosságai

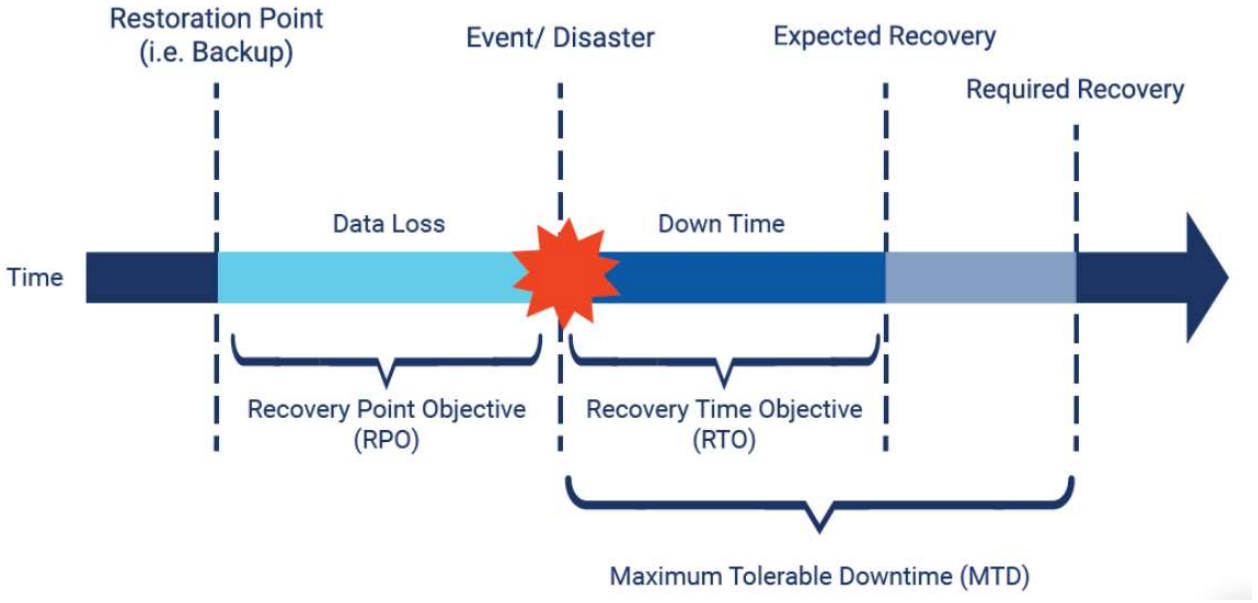
DR stratégiák

- Alternatív site: minél jobban előkészített, annál drágább
  - Tükör site: minden rendszer és tranzakciós teljesen azonos az eredeti telephellyel
  - Hot site: Azonos hardver és szoftver környezet az eredeti telephellyel
  - Warm site: Speciális hardverek nem állnak rendelkezésre, csak minimális
  - Cold site: Csak a kábelezés, és a hely áll rendelkezésre
- Alternatív szolgáltatói szerződés: ilyen például egy másodlagos internet szolgáltató
- Alternatív adatközpont: a szervezet saját maga üzemeltet georedundáns szervertermet
- Redundáns szerverek: A szerverek cluster párokban dolgoznak, és az egyik kiesése esetén a másik átveszi a feladatát

DR stratégiák

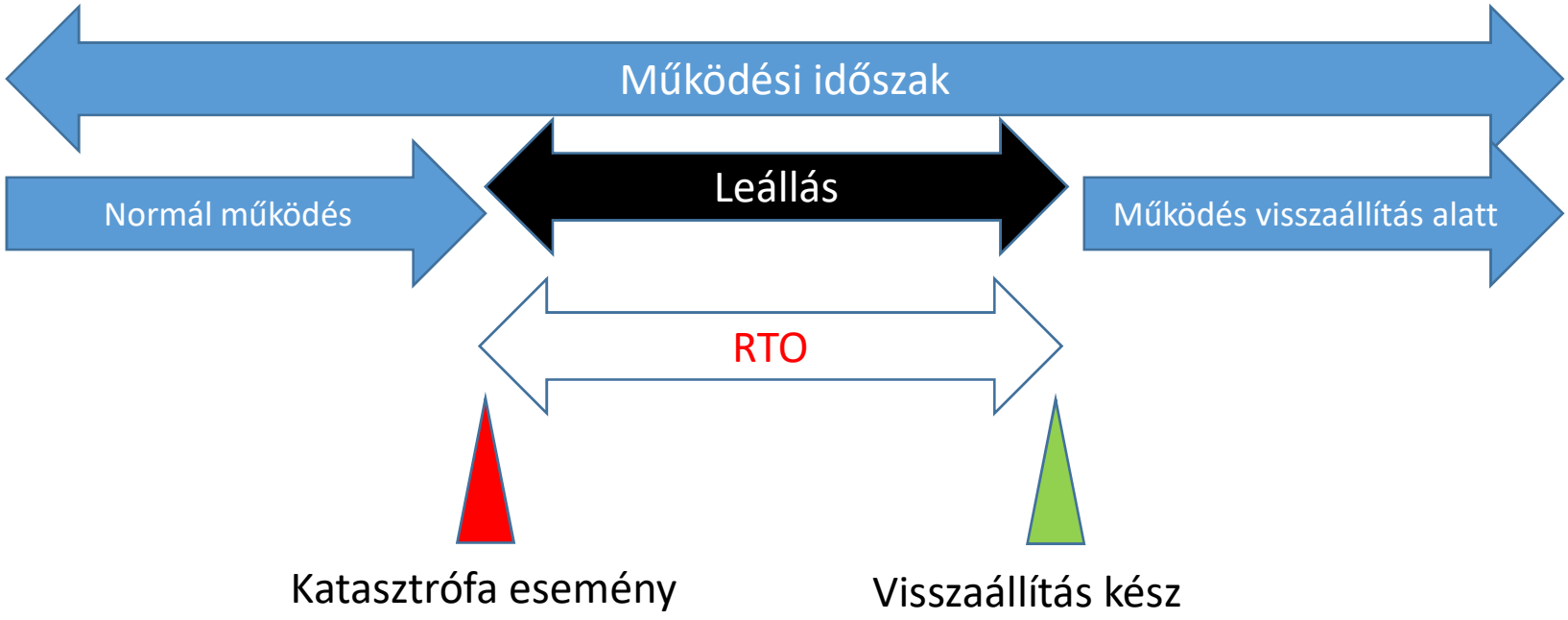
- Mentés: az adatokat menteni kell, és a mentéseket célszerű földrajzilag elkülönített helyen tárolni, védeni. Típusai:
  - Teljes mentés: mindig mindent mentünk. Leginkább tárhely igényes
  - Inkrementális mentés: mindig az előző mentés óta megváltozott fájlokat mentjük. A visszaállításhoz az utolsó teljes, és az összes inkrementális mentés kell.
  - Differenciális mentés: mindig az előző teljes mentés óta megváltozott fájlokat mentjük. A visszaállításhoz az utolsó teljes, és az utolsó differenciális mentés kell.
  - Folyamatos mentés: minden adatváltozást azonnal lementünk.

DRP mérőszámok



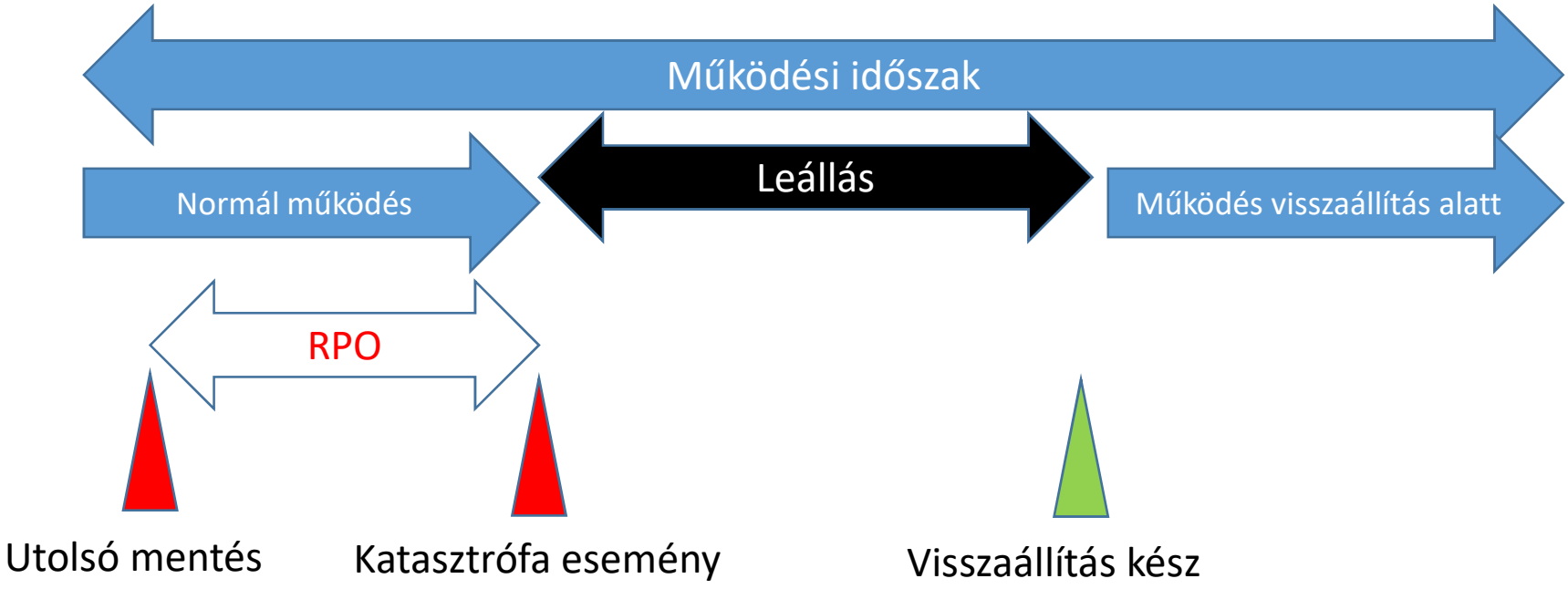
- **Recovery Point Objective (RPO)**: Adatvesztés tolerancia. A katasztrófától visszafelé a maximum időtartam, mely adatainak elvesztése visszafordíthatatlan kárt okoz.
- **Recovery Time Objective (RTO)**: A rendszer tervezett visszaállítási időtartama, hogy ne érje el az MTD-t, azaz a maximális elviselhető leállást.
- **Maximum Tolerable Downtime (MTD)**: Maximum leállási idő, amit a folyamat képes tolerálni

Recovery Time Objective



- RTO: az az időtartam, melyet az üzlet az IT szolgáltatás teljes elérhetetlensége esetén elvisel. Ez az idő áll rendelkezésre ahhoz, hogy a DRP megoldás visszaállítsa a működést.
- Az üzlet határozza meg, nem pedig a DRP megoldás.
- Úgy kell meghatározni, hogy a DRP megoldás ne legyen költségesebb, mint a kiesés

Recovery Point Objective



- RPO: A katasztrófától visszafelé a maximum időtartam, mely adatainak elvesztése visszafordíthatatlan kárt okoz. Gyakorlatilag az utolsó mentés időpontját adja meg.
- Az üzlet határozza meg, nem pedig a DRP megoldás.
- Úgy kell meghatározni, hogy a DRP megoldás ne legyen költségesebb, mint a kiesés (pl. tárhely költség)

BCDR tesztelés

Miért teszteljük a BCP terveket?

- Elérhetők-e a BCP dokumentumok?
- Ismerik-e az érintettek a terveket?
- Valóban működnek-e az alternatív folyamatok?
- Az érintettek gyakorlatot szerezzenek

Miért teszteljük a DRP terveket?

- Elérhetők-e a DRP dokumentumok?
- Ismerik-e az érintettek a terveket?
- Tartalék szoftver és hardver működési hibák felderítése
- A tartalék rendszer megfelel-e az élesnek?
- Az érintettek gyakorlatot szerezzenek

BCDR tesztelés típusai

Asztali gyakorlat	•Az asztali gyakorlat (tabletop testing) egy elméleti teszt, melynek során brainstorming jelleggel a résztvevők végig beszélik, hogy kinek mi a szerepe és feladata egy leállás esetén.
BCP/DRP terv átvizsgálás	•A terv átvizsgálás során szintén elméleti síkon a résztvevők részletesen átnézik a terv lépéseit, és végig gondolják annak megvalósíthatóságát.
Checklist teszt	•A checklist alapú teszt a legegyszerűbb. Ennek során az érintettek kapnak egy listát a felkészülési feladatokról, a kontaktokról, szerepkörökről. A teszt során ezt a listát kell ellenőrizni.
Szimulációs teszt	•Akár BCP, akár DRP tesztről van szó, a szimulációs teszt során egy rész folyamat/rendszer leállását szimulálják, és erre hajtják végre a tervet. A leállás kontrollált és behatárolt.
Párhuzamos teszt	•A párhuzamos teszt során kipróbálják, hogy a tartalék rendszerek teljes kapacitással ki tudják-e szolgálni a folyamatokat. A teszt során az éles rendszerek párhuzamosan üzemelnek.
Real/teljes teszt	•A real, vagy teljes teszt során az éles rendszert valóban leállítják, és kipróbálják, hogy a tartalék rendszer el tudja-e látni a feladatát.

KÖSZÖNÖM A FIGYELMET!

Kérdések?