**BCP-DRP felfogás a gyakorlatban – gyakorlati BCP-DRP felfogás**

*(Business Continuity Plan – üzletmenet-folytonossági terv*

*Disaster Recovery Plan – katasztrófa helyreállítási terv)*

**I. BCP-DRP felfogás a gyakorlatban**

**Mi található az interneten? (négy, kiragadott példa)**

1.)

<http://www.ant.hu/termek/uzletmenet-folytonossag-tervezes-bcp-drp>

ANT (Advanced Network Technologies) Kft.

jell.:

Példásan tudományos honlapszöveg.

Csak IT-ra koncentrál (a cég is IT szolgáltató).

2.)

<https://www.humansoft.hu/Uzleti_megoldasok/Informatikai_tanacsadas/Uzletmenet_folytonossagi_tervezes.html>

Humansoft Kft.

jell.:

IT (szolgáltató) cég.

DE! Lehet, hogy már láttak gyakorlatot?

*„Előfordult már Önöknél, hogy a mindennapi munkát*

*nem tervezett rendszerleállás,*

*be nem jelentett áramszünet,*

*távközlési hálózat hibája,*

*áradás, heves vihar,*

*tűzeset, csőtörés,*

*a beszállító, külső szolgáltató késlekedése,*

*a dolgozók tömeges késése, megbetegedése zavarta meg?”*

3.)

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwio5cvCn5PgAhWJblAKHWP9CQgQFjADegQIBxAC&url=http%3A%2F%2Fiig.elte.hu%2Ffile%2Felte_bia_drp_bcp_szabalyzat_v5.doc&usg=AOvVaw2LwhGRa4qPQiNTb4IaFS1g>

ELTE Gazdasági és Műszaki Főigazgatóság Informatikai Igazgatóság

jell.:

Szépen, szisztematikusan összeállított keretszabályozás (a konkrétumok a továbbiakban - hivatkozva).

4.)

<https://www.tmsi.hu/uzletfolytonossagi-bcp-terv/>

Tőzsér és Máriás Szoftver Iroda (TMSI) Kft.

jell.:

IT szolgáltató, IT biztonságot szolgáltató cég.

Szimpatikus a gyakorlat szerinti megközelítés.

*„A gyakorlat, szakkönyvek, nemzetközi keretrendszerek alapján az informatikai üzletfolytonossági és katasztrófalehárítási terveket alapvetően a lehetséges kockázatok (és még sok más szempont, pl. az adatvagyon) alapján kell kialakítani. Ez a gyakorlatban a villámcsapás-, tűz-, árvíz- és hasonló kockázatok mérlegelésével történik. Ahol egyáltalán foglalkoznak ilyennel, ott a terveket a szabványok alapján elkészítik, “polcra teszik” a feladatot kipipálják.*

*És ha nem az árvíz okozza a fennakadást? Mert például lehet hatósági ellenőrzés, ami akár a számítógépek/szerverek lefoglalásával is járhat. Vagy például olyan nyári hőség, ahol kiderül hogy a szerverszoba klímája rosszul van bekötve és a szerverek felforrnak.”*

**Ami látszik (az interneten tovább keresve).**

Ami nem jó:

1. A fenti (jobbára) pozitív megközelítésnek tekinthető kiragadott példákra nagyon sok olyan találat esik, ahol csak szép (divatos) szavak sorakoznak egymás után, információtartalom nélkül.

2. Az előzőből is következően a BCP-DRP csak egy kipipálandó papír („polcra teszik”) minden értelem és gyakorlati haszon nélkül.

3. Nincs egységes, a gyakorlatban használható értelmezése a BCP-DRP-nek. Pontosabban! A „közvélekedésben” nincs, és ezáltal elfogadott respektje sincs.

4. Mindenki túlsúlyban IT környezetben (hálózatok, eszközök, stb.), IT katasztrófákra értelmezi BCP-DRP-t.

(Más megközelítésben. Ha egy szervezetnél egy darab számítógép sincs, akkor ott a BCP-DRP nem is értelmezhető?)

Ami jó:

5. Pozitívnak tartom a „tudományos” megközelítést is, ha nem merül ki fölösleges agyalgásban, hanem párosul – a tudományos megközelítésből levezetett – a szervezetre szabott gyakorlati intézkedésekkel.

A tudományos szó azért került idézőjelbe, mert:

- Ha csak a felhasználó elvarázslása a cél (mert pl. áltudományos, sok idegen szó egymásután, logikai kapcsolat nélkül), akkor az a vevő becsapása és látszatbiztonságot eredményez.

- Ha valóban tudományos a megközelítés, de megreked az elvi szinten, abból a felhasználó még nem tudja, hogy konkrét esetben mit is kéne csinálnia. Tehát jó, de gyakorlati haszon nélküli, így szintén látszatbiztonság lesz a végeredmény.

6. Mindenképpen előremutató, hogy egyre többen kezelik haszontalan kérdés helyett (mint kipipálandó szabványpont) gyakorlati haszonnal bíró eljárássorként. Ellentmondás, hogy reménykedünk, hogy ezt az eljárássort soha nem kell alkalmaznunk. Ebből azért adódnak olyan tényezők, hogy „lazábban” tervezünk és nem tesztelünk (a bekövetkezés potenciális volta miatt, vagy mert nincs tesztelő eszközünk, stb.).

7. Viszont! A „jobbaknál” sem egységes, hogy hol kezdjük a katasztrófákkal, BCP-DRP-vel való foglalkozást.

**Nézzük a „közvélekedést”**

A felhasználók mondták:

A katasztrófa: valamilyen működési anomália. Bekövetkezésével több-kevesebb valószínűséggel számolhatunk (ebben benne van a nulla is, tehát potenciális). Hatásának elkerülésére (minimalizálására) intézkedéseket hozunk – ennek a logikai sornak lesz a BCP-DRP a végső eleme.

Egy szervezetnél minden lehetséges katasztrófát vegyünk fel, értékeljünk, súlyozzuk (kockázatértékelés) és intézkedjünk rá (BCP-DRP-ban).

**Mit mond egy szabvány**

A 27001 szerint követelmény:

- A11.1.4. Külső és környezeti fenyegetésekkel szembeni védelem:

A természeti katasztrófák, a rosszindulatú támadás vagy a balesetek elleni fizikai védelmet meg kell tervezni, és azt alkalmazni kell.

- A17.1.1. Az információbiztonság folytonosságának tervezése:

A szervezetnek meg kell határoznia az információbiztonsági követelményeit, valamint az információbiztonság irányításának folytonossági követelményeit olyan kedvezőtlen helyzetekben, mint pl. egy válság vagy katasztrófa során.

(A szabvány több követelményt határoz meg, de a „vezérgondolathoz” ez a kettő elég lesz.)

Ezek szerint a tanácsadóknak nem sikerült egészen pontosan sem a katasztrófa, sem a BCP-DRP kérdést tisztázni a felhasználókkal.

**Pontosítsunk tovább**

A katasztrófák fogalmát szűkítsük, kategorizáljuk (a bármiféle működési anomáliákról).

A katasztrófák körébe értendőek:

**- elemi károk,**

**- természeti csapások,**

**- társadalmi katasztrófák**

A szűkítéssel nem veszítettünk, mert pl.…

- a felhasználó képzetlen (nem ismeri a szabályokat),

- a felhasználó nem akarja tartani a szabályokat,

- a vincseszter tönkrement,

- a bejárati ajtó nyitva maradt,

- stb.

…ezeket a „hétköznapi” problémákat áttoltuk az incidensek témakörébe és ott szabályozhatjuk (hogy ne következzen be – megelőzés; ha bekövetkezett - incidenskezelés).

*A katasztrófák és kategóriáik részletes kifejtése nem ennek az írásnak a tárgya.*

A további rendezéshez vegyünk figyelembe olyan tényezőket, mint pl.:

- a bekövetkezés gyakorisága (potenciális lehetőség, vagy volt is rá példa),

- az okozott/okozható kár mértéke (anyagi, presztízs, stb.),

- el lehet kerülni, vagy a bekövetkezés a szervezettől független (csőtörés, árvíz).

**II. Gyakorlati BCP-DRP felfogás**

**Minek, hol a helye?**

A felhasználónak nem az a fő tevékenysége, hogy ISO rendszereket üzemeltessen. A felkészítő (tanácsadó) segítsége rendkívül hasznos. Feltételezzük, hogy mindkettő a saját szakmai területén otthon van. A felkészítő felelősége olyan megoldások kialakítása, ami a szakmaterületek hatékony együttműködését eredményezi.

Következik egy olyan lehetséges „értelmezési sor”, amit a nem túl hozzáértő felhasználó képes megérteni, megvalósítani és – akár külső segítség nélkül – kézbentartani.

Továbbá, rendkívül fontos, hogy mindezek közben a felhasználóban alakuljon ki meggyőződöttség a tevékenység gyakorlati hasznosságáról.

*(Nem elfogadható az a mondat, hogy: majd jön a tanácsadó, rendbe teszi az ISO-nkat, az auditor kicsit morgolódik, de a nap végén hazamegy, mi a papírokat feltesszük a polcra és egy évig békén hagynak.)*

1. Összegyűjtjük (átgondoljuk) az összes, a normál tevékenységünket (negatívan) befolyásoló tényezőt, tapasztalatot.

Ezek nem mindegyike tekintendő potenciális katasztrófának. Az egyszerűbb, napi, általános kérdéseket a Rendszer kézikönyvben, Utasításokban szabályozzuk.

Pl.

- a felhasználó a monitorán kiragasztva tárolja a jelszavait,

- a biztonsági zóna ajtaját mindig nyitva hagyják,

- a számzáras ajtó billentyűzete olyan koszos, hogy 1-2 találgatással ki lehet találni a kódot,

- a biztonsági területek dolgozói - „csak egy kávéra” – átjárnak egymáshoz,

- az irattár – törött – ablakán bejön a madár, az egér,

- a kitöltött nyomtatványok hátsó oldala jó lesz a gyereknek rajzolni.

Jellemző, hogy utasításban, oktatással – egyszeri alkalommal – rendezhetőek.

Kapcsolódó kérdések:

- az ellenőrzés fontossága,

- mi az a szabályszegési szint, amit már incidensnek nevezek, és van-e incidenskezelési elképzelésem, a retorziókkal együtt

- egyáltalán, jó-e a szabályozásom (betartható-e?).

2. A megmaradt működési anomáliákat jelenítsük meg a kockázatértékelési rendszerünkben.

Ezekre egyre inkább jellemző lesz, hogy a bekövetkezésük esetleges (potenciális).

Kockázatértékelésre bármelyik módszer megfelelő, amelyik tudja kezelni a „bekövetkezés valószínűsége” és az „okozott kár nagysága” kérdéseket (legalább).

A kockázatértékelés végén három eredményre juthatunk:

- Visszacsatolunk a szabályozáshoz.

Jó példa:

Szabályoztam (és oktattam) a titoktartás fontosságát, de a szervezetemnél – a konkurenciaharc kiélezettsége miatt – fontos a dolgozók alaposabb és rendszeres felkészítése. Ez lehet pl. social engineering képzés.

Rossz példa:

Internet felhasználásával szolgáltatok. Társadalmi katasztrófa bekövetkezését valószínűsítem (pl. országos sztrájk). Jelmondatom: Mert mi minden időpillanatban szolgáltatunk!

Intézkedés. UPS minden géphez, legalább 2 hálózati betáplálás, aggregátor a telephely sarkában. Élelmiszer- és vízkészlet felhalmozása. Dolgozók vészhelyzeti bejuttatásának és elszállásolásának megszervezése. Mert mi minden időpillanatban szolgáltatunk!

(De kinek? Ill. minek?)

Egyszerűbb a szerződésben kitérni, hogy „vis maior” esetén milyen kieséssel vagy korlátozással.

- Felvállalom (de nem csak a kockázatot, hanem a hatásait is!).

Kockázatos az ide tartozó kockázatokkal nem – helyesen – foglalkozni.

Lehetőségek

a. Tudok róla, de jelenleg nincs lehetőségem a megoldásra (jelenleg!).

b. Tudok róla, elenyésző az előfordulása és a kárértéke (több a védelem ára, mint a kár).

A veszélye annak van, ha szerencsejátéknak tekintjük.

c. Tudok róla, a kár is nagy (lehet), de mi az esélye, hogy pont velünk történik?

- További tervezést igényel. (Ezek lesznek a BCP-DRP hatókörébe tartozók.)

Azokban az esetekben, amikor a bekövetkezés esélye nem egyértelmű, viszont az okozott kár jelentős.

Hozok egy példát, ami élő, de pont az aktuális jellege miatt mára már kikerült a BCP-DRP hatóköréből és átkerült a napi szabályozásba:

10 évvel ezelőtt nem volt napi probléma (nyáron), hogy a hőmérséklet eléri a 40 fokot és „megfőnek” a dolgozók és a szerverek.

**BCP-DRP tervezés**

Az ide tartozókra jellemző, hogy nem egyértelműen behatárolható a bekövetkezés esélye, viszont a kárérték jelentős.

Elvi megközelítés szerint az előzőekben tárgyalt működési anomáliák, incidensek, katasztrófák hatásait van esélyünk megelőzni.

pl. Megnőtt a szeles, viharos időjárás gyakorisága. Intézkedés: a biztonsági szolgálatnak legyen feladata az ablakok, ajtók zártságának ellenőrzése.

A BCP-DRP témakörébe tartozó katasztrófákat tekinthetjük bekövetkezettnek. Valójában még nem azok, de megelőzni sem tudjuk.

Amit viszont tudunk: gondos tervezéssel előre felkészülni, hogy bekövetkezés esetén hogyan minimalizáljuk a hatásokat.