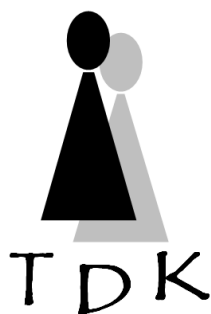


Azúr felhők

– DR site a számítási felhőben

Tudományos Diákköri Dolgozat

Konzulens: Dr. Fehér Péter



Ács Benedek

Gazdálkodástudományi Kar

BSc

Gazdaságinformatikus

II. Évfolyam

2013 március 25.

A BCE Közgáz Campus Tudományos Diákköri Konferenciáját a TÁMOP-4.2.2/B-10/1-2010-0023 azonosítójú “A tudományos képzés műhelyeinek átfogó fejlesztése a Budapesti Corvinus Egyetemen” című projektje támogatja.

Azúr felhők

/DR site a számítási felhőben/

Tartalom

A kutatásom témája és célja	3
Dolgozatom kérdésfelvetése.....	3
A kérdésfelvetés indoklása	4
Kapcsolatom a témával	5
A DR rendszerek bemutatása	6
Miért kellenek?.....	6
DR szintek ismertetése	6
A DR megoldások vállalati elterjedtsége.....	7
A Cloud megoldások bemutatása.....	9
Történelme.....	9
Publikus, privát és hibrid felhő.....	11
A privát felhő	11
A publikus felhő	11
A hibrid felhő	14
A felhő-megoldások negatív, kérdéses tulajdonságai	14
Szolgáltatási szintek.....	15
Jelenlegi piaci helyzet	17
Trendek, előrejelzések a cloud computing jövőjére vonatkozóan.....	17
Az S&T Magyarország bemutatása.....	18
Az S&T és a DR.....	20
Jelenleg használt DR megoldás.....	20
Az S&T igényei egy DR rendszerrel szemben	20
DR megvalósítási alternatívák	23
A Windows Azure bemutatása	24
Az S&T igényeinek megfelelő hagyományos DR megvalósítás	25
A megvalósítás műszaki leírása, paraméterei	25
Megvalósíthatósági problémák	26
Az implementáció időtartama és költsége	26
A hagyományos DR rendszer teljes tulajdonlási költsége	27

A hagyományos megvalósítás üzleti előnyei és kockázatai.....	28
Az S&T igényeinek megfelelő DR site megvalósítása a számítási felhőben	30
A szükséges felhő szolgáltatás konfigurációs beállítások ismertetése, indoklása	30
Megvalósíthatósági problémák	30
A meglévő rendszerrel való integráció időtartama és költsége	31
Az Azure-ban használt erőforrások teljes tulajdonlási költsége	32
Az Azure megvalósítás üzleti előnyei és kockázatai	33
A megvalósítási lehetőségek összehasonlítása	35
Összehasonlítás képességek alapján	35
Összehasonlítás költségek alapján	35
Összehasonlítás rugalmasság alapján	36
Konklúzió: A cloud DR megoldás életképessége vállalati közegben	37
Forrásjegyzék.....	38
Mellékletek.....	41
1. sz. melléklet.....	41
2. sz. melléklet.....	41
3. sz. melléklet.....	42
4. sz. melléklet.....	42

A kutatásom témája és célja

Dolgozatom kérdésfelvetése

Kutatásom célja a hagyományos, fizikai, helyszíni (on-premise) rendszerintegrációs megoldások összehasonlítása a felhő-szolgáltatók nyújtotta lehetőségekkel. Mivel mind az on-premise megoldások, mind a felhőszolgáltatások széles skálán mozognak, így a témát szűkítettem.

Az összehasonlítás nem egyértelmű folyamat, a két megoldás gondolatmenetében gyökeresen eltér egymástól, így az összehasonlítás közben a legnagyobb nehézséget az objektivitás jelentette. A szakszerűség megtartása érdekében kutatásom fókuszába a költségeket helyeztem, így biztosítva az egyértelmű mérhetőséget a megoldások és eredmények elemzése során.

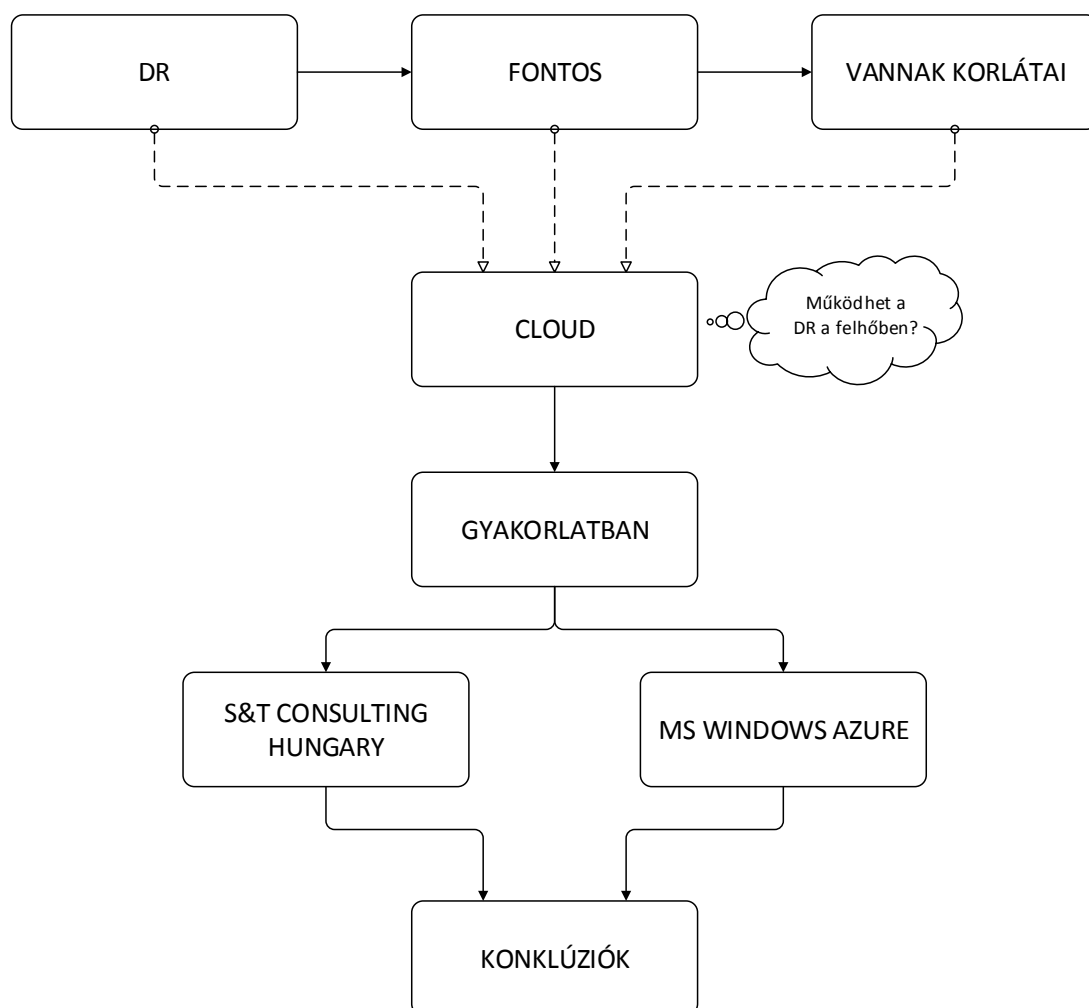
A téma szűkítése és a fókusz figyelembevételével az alábbi kérdésfelvetést fogalmaztam meg:

Van-e lehetőség, egy valós, működő vállalat számára, hogy a hagyományos Disaster Recovery (DR – Katasztrófa helyreállítási) megoldás helyett számítási felhő megoldás használatával valósítsa meg üzleti folytonosságának biztosítását; amennyiben ez így van, akkor melyik megvalósítás jár alacsonyabb költséggel?

A kérdést részletes esettanulmány jellegű feltárás során vizsgáltam.

Dolgozatom logikai szerkezetének megértését az alábbi ábra segíti:

1. ábra - Dolgozatom logikai struktúrája



A kérdésfelvetés indoklása

A vállalat üzleti folytonosságának biztosítása az IT vezetők egyik legnehezebb és legfontosabb mindenkori feladata. Egyszerűen vannak olyan adatok, amelyeket nem lehet pótolni. Erre jó példa lehet a családi képek esete. Egy magánszemély számára a család képei felbecsülhetetlen jelentőséggel bírnak, ráadásul a gyerekek egyszer nőnek fel, nem lehet róluk új képet csinálni arról, hogy babakocsiban milyenek is voltak, mikor már 16 évesek. Az emlékeket nem lehet újra megörökíteni, a házi film-gyűjtemény azonban újra beszerezhető, igaz, adott esetben ez is jelentős költséggel bír. Egy vállalat esetében ez hatványozottan igaz, egy elveszett szerződést, egy jogi nyilatkozatot nehéz ugyan, de nem lehetetlen pótolni. Egy belső elemzés, kutatás, szolgáltatás-tervezet, akcióterv elvesztése azonban sokkal komolyabb probléma, ezeket, amennyiben nem redundánsan tárolják és az elsődleges rendszer használhatatlanná válik, lehetetlen pótolni. Ilyen esetben az sem számít, ha az elsődleges rendszer magas rendelkezésre állású, mert ha jelentős hatású természeti katasztrófa

következik be – árvíz, tűz, meteor -, akkor az épületben is kár keletkezik, nem csak a számítógépes infrastruktúra rendszerben.

Az ilyen jellegű problémák megoldására szolgálnak a DR megoldások, amelyeket akár földrajzilag is jól elkülönülő helyen valósítanak meg, így minimalizálják annak kockázatát, hogy ugyanabban a katasztrófában az elsődleges és a mentési rendszer is sérüljön.

Kapcsolatom a témával

Másodéves gazdaságinformatikus hallgató vagyok, a felhő szolgáltatásokkal először az egyetemen találkoztam. Rögtön felkeltette az érdeklődésemet a téma, mert úgy éreztem, hogy nagy jövő előtt áll a megoldás, amely képes lehet megújítani az IT iparágat, hisz hihetetlenül sokoldalú, gyakorlatilag szinte bármire lehet használni.

Az elmúlt fél évben egy rendszerintegrátor cégnél kezdtem el dolgozni, mint gyakornok, munkaterületem pedig épp a felhő-megoldásokra esett, ezen belül pedig a Microsoft Azure technológiájára.

Ez a háttér indokolja, hogy a téma részletesebb megismerése és feltárása során, dolgozatom témájának is a felhő szolgáltatásokat, illetve annak speciális alkalmazási területét válasszam.

A DR rendszerek bemutatása

A választott témám ismertetése után a DR rendszerek alapos bemutatására térek át, melyben részletezem annak szükségességét és korlátait is.

Miért kellenek?

Egy megfelelő DR (Disaster Recovery) rendszer kiépítése a legtöbb vállalat számára nélkülözhetetlen, hisz vannak olyan adatok, melyeket lehetetlen pótolni, ha egyszer elvesznek. Ez az egyik tanulsága az elmúlt évtized nagy tragédiáinak. A 2001. szeptember 11-ei terrortámadás után sokak figyelmét elkerülte, de az iktortornyokban lévő irodák 50%-a három hónapon belül csődbe jutott (Schopp, 2007), saját elemzésük szerint is azért, mert nem tudták pótolni, helyreállítani az elveszett üzleti adatokat. Nem minden ország küzd azonban a terrorizmussal, nekik ösibb veszély jutott: a természet. Ide tartozik hazánk is, gondoljunk csak az árvizekre vagy a vörösiszap katasztrófára.

Katasztrófának számítanak a nem várt hardware meghibásodások, melyek az elsődleges üzleti szolgáltatások kieséséhez, leállításához vezethetnek. Ilyen meghibásodás például, amikor a szerverteremben leáll a légkondicionálás vagy a fűtés, de ide tartoznak a közmű problémák is: egy eltört vízvezeték vagy egy leszakadt elektromos felsővezeték is, mely hosszú időre áramkimaradást okozhat.

DR szintek ismertetése

A DR megoldásokat egy hét szintű skálán szokás értékelni, ezt az alábbiakban ismertetem, Brooks, C. et. al. (2002) alapján:

- 0. szint: „nincs off-site data”, azaz nincs olyan megoldás, mely földrajzilag elkülönülő helyen biztonsági mentéseket tárolna, így elképzelhető az összes üzleti adat elvesztése.
- 1. szint: adatmentés földrajzilag elkülönülő helyen, futtató infrastruktúra nélkül (futtató infrastruktúra: olyan infrastruktúra, mely képes futtatni az üzlet által elsődlegesen használt programokat a felhasználók által megszokott környezetben, illetve képes a munkavégzés alatt keletkező adatok feldolgozására is.) Másnéven PTAM (Pickup Truck Access Method)-nak nevezik, mert a szalagok szállítását a az esetek többségében kisteherautóval oldják meg.

- 2. szint: adatmentés földrajzilag elkülönülő helyen, futtató infrastruktúrával (a kifejezés angol megfelelője: hotsite), mely képes átvenni az elsődleges rendszer összeomlása esetén a terhelést a „recovery time” után, de mikor nincs szükség rá, akkor a rendszer ki van kapcsolva, nem fut.
- 3. szint: a második szinttel megegyező infrastruktúra, annyiban tér el, hogy ezen a szinten a költségek jelentős növekedésével, de a másodlagos futtató infrastruktúra (hotsite) mindig fut, akkor is, ha az elsődleges rendszer hibátlanul működik. Ezáltal elérhető egy rövidebb recovery time, így a „downtime window” hossza csökken. Ez azt jelenti, hogy az az időintervallum csökken le, amelynek kezdetét az elsődleges rendszer meghibásodása jelenti, a végét pedig a másodlagos rendszer éles üzembe állítása.
- 4. szint: megegyezik a harmadik szinttel, a különbség az adattárolás módjában van: az adatokat még mindig egy külön adattárházban tartják, ami nem egyezik meg a másodlagos infrastruktúra földrajzi helyével, ám az elsődleges és másodlagos rendszer állandó összeköttetésben áll egymással egy szélessávú kapcsolat segítségével (lásd: 4. sz. melléklet). Így az üzletileg kritikus rendszerek adatait állandóan szinkronizálják, de a többi rendszert a 3. szint értelmében kell helyreállítani.
- 5. szint: tranzakció integritás szintje, ezt olyan vállalatok használják, amelyeknek kulcsfontosságú, hogy konzisztens legyen az adat az elsődleges rendszer és a DR site adatbázisa között. Ilyen megoldás keretében minimális az adatvesztés mértéke. Az 5. szint magában foglalja a negyediket, azzal a többlettel, hogy itt a teljes IT infrastruktúrát szélessávú hálózaton keresztül szinkronizálják a két (elsődleges és másodlagos) rendszer között.
- 6. szint: ez a szint, a „Disc mirroring” technológián alapszik, azaz a teljes elsődleges üzleti rendszert lemásolják egy földrajzilag távol eső helyen. Az adatok szinkronizálása azonnali és automatikus, azaz bármely módosítás esetén a változtatásokat elvégzi a másodlagos rendszer is, azaz a szinkron megtartásához nem szükséges emberi beavatkozás.

A DR megoldások vállalati elterjedtsége

A DR megoldások látszólag széles körű igényt elégíthetnek ki, ugyanakkor érdemes megvizsgálni, hogy ténylegesen milyen mértékben használják ezeket a vállalatok. A vállalatok 80%-a egy súlyosabb incidens, katasztrófa bekövetkezése után másfél évvel csődbe megy (Gosling, 2008). Ez azért lehetséges, mert csak 20%-uk tevékenykedik olyan téren, ahol az adatok nem jelentenek kulcsszerepet, és így üzletileg nem számítanak kritikus tényezőnek?

Nem, nagyobb részük rendelkezik megfelelő DR megoldással, ezáltal képes újra talpra állni az adatok segítségével, illetve talpon maradni.

Ez az érték elsőre nagyon alacsonynak tűnik. Miért nem alkalmaz minden vállalat DR rendszert? Nincsenek megfelelő műszaki vagy szoftveres megoldások? Vannak, sőt elég erős verseny van az egyes szolgáltatók, fejlesztők között így még azt sem lehet mondani, hogy nincs megfelelő számú alternatíva / nem elég széles a termékskála. A válasz ennél egyszerűbb: azért, mert a DR rendszer a legtöbb cég számára indokolatlanul drága. Azért indokolatlanul, mert a katasztrófa esetén elvesztett adat értékét nem becsülik akkorára, mint amekkora egy biztonsági rendszer kiépítésének és fenntartásának a költsége.

A Cloud megoldások bemutatása

Amint a fentiekből kiderül, léteznek megfelelő DR megoldások és a piac igényli is, ám nem képes megfizetni azokat. Ez a legnagyobb korlátja a disaster recovery rendszereknek: a magas beszerzési ár és fenntartási költségek. A dolgozatomban fő kutatási témája így annak vizsgálata, hogy a magas költségek milyen megoldásokkal mérsékelhetők, illetve kiemelten a felhő szolgáltatások ebben milyen mértékben képesek segíteni.

Történelme

„Computation may someday be organized as a public utility”
[John McCarthy, 1961](#)

A felhőalapú megoldások őseit az 1950-es évek végén megjelenő mainframe-ek, nagyteljesítményű számítógépek között kell keresnünk.

Ezeket a nagy és drága számítógépeket kormányzati intézmények, nagyvállalatok és bankok használták az üzletileg kritikus alkalmazásaik futtatására. Ezen monstrumok szélesebb körben való elterjedését azonban a költségeik és limitált felhasználhatóságuk megghiúsították.

1970-es években fejlődött az elképzelés: kisebb, kevésbé komplex és olcsóbb számítógépek kerültek piacra, és ezek a szerény teljesítményű kisgépek, vagy akkori szóhasználattal „minik” csatlakoztak hozzájuk. Ezres nagyságrendű egyidejű végfelhasználót (minit) szolgáltak ki.

Az olcsó, többfeladatú személyi számítógépek terjedésével azonban ez a kor is letűnt, a megváltozott felhasználói igényekhez egyszerűen jobban alkalmazkodott a személyi számítógépek által nyújtott megoldás, mely költséghatékonyabb és ember közelebb, grafikus felhasználói felülettel rendelkező gépeket nyújtott háztartások számára.

A következő lépést a fejlődésben az internet megjelenése jelentette, mely új igények és új megoldások mellett egy teljesen új világot teremtett mind a magánélet, mind az üzleti élet területén. A szolgáltatások teret nyernek a dobozos szoftverek kárára, a felhasználók adataik egyre nagyobb részét tárolják az interneten (Malik, 2010), mint ahogy szintén az internet vált az egyik legjelentősebb kommunikációs csatornává.

Az elkövetkező évek, évtized nagy váltása pedig az előrejelzések és trendek szerint a szerver-kliens architektúra felváltása lesz a felhő-megoldások által. A felhőalapú szolgáltatások (cloud computing) létrejöttéhez pedig nem is kellett más, a feltételek adottá váltak:

- Nemzetközi sávszélesség megnövekedett, a növekedés üteme gyorsul: 2002 óta 62-szeresére nőtt a nemzetközi sávszélesség szolgáltatók által biztosított kapacitása (Brodkin, 2012).
- A mobil sávszélesség megnövekedett, illetve növekedése állandósult, gyorsult: elemzések szerint 2017-re a havi mobil adatforgalom több mint 12.5-szerese lesz a 2012-es értéknek, azaz 11.2 ExaByte (VNI, 2013).
- Vezeték nélküli hálózatok lefedettsége nőtt: 2010-ben a feltérképezett WiFi hálózatok száma elérte a 20 milliót, ez az érték 2013 januárjára 90 millióra nőtt (Wigle, 2013).
- Adattárolási költségek drasztikusan csökkentek: 2002-ben 1GB adat tárolása \$7.5-ba került, ma ugyanennyi adat tárolási költsége nagyjából \$0.06, ez a 2002-es ár kevesebb, mint egy százada (Davis, 2011)!
- Internet-alapú szolgáltatások köre és minősége is bővült
- Az internet széles körben elterjedt: az elmúlt évtizedben több mint 5.5-szeresére nőtt az internet felhasználók száma (WIU, 2012).

A vállalatok számára időközben egyre fontosabbá váltak az informatikai költségekre vonatkozó megfontolások is, előtérben kerültek a költséghatékonyabb megoldások. Az ebbe az irányba történő fejlesztések egyik állomása a felhő szolgáltatások technológiája.

A cloud szolgáltatások kialakulását egy hasonlattal is kifejezem: az embereknek régebben is szükségük volt vízre, ezért először mindenki elment a folyóhoz. Ezt váltotta fel a kutak megjelenése, amikor is mindenkinek saját erőforrása lett (erőforrás=kút). Ezt pedig a közösségi vízfelhasználás váltotta fel, amikor is a közösen kezelt erőforrásokat (=víztározók) a csatornák (=továbbító közeg) juttatták el a fogyasztókhoz. Ugyanez a folyamat játszódott, illetve játszódik le a számítógépekkel is: a számítógépekből először számítási időt lehetett venni (korsó víz a folyóból), aztán mindenkinek saját számítógépe lett (kutak) és a felhőmegoldások elterjedésével pedig már egy közösen használt, de egyedileg konfigurált (saját csapok) erőforrásokat használhatnak. A hasonlat megértését a következő ábra segíti:

2. ábra - igények és egyéni, illetve közösségi megoldásaik

Igény megnevezése	Egyéni, hagyományos megoldás	Közösségi, hatékonyabb megoldás
Víz	Kutak	Vízszolgáltatás
Csatorna	Derítő	Csatornázás
Hő	Kandalló	Távhő

Igény megnevezése	Egyéni, hagyományos megoldás	Közösségi, hatékonyabb megoldás
Gáz	Palackos	Vezetékes
Internet	Közvetlen csatlakozás BIX-re, NIIF-re	ISP (Internet Service Provider – internetszolgáltatók)
Számítási kapacitás	Saját szerver	Felhő szolgáltatások

Publikus, privát és hibrid felhő

A felhő szolgáltatások megoldásait tekintve, attól függően, hogy kinek a tulajdonában áll az infrastruktúra, a következő kategóriákat lehet megkülönböztetni: publikus, amikor a szolgáltató tulajdona minden; privát, amikor az érintett vállalaté az infrastruktúra; illetve hibrid, amikor mindkét megoldást együttesen használja a vállalat. Ennek szemléltetésére szolgál a 2. sz. *melléklet*. A továbbiakban az egyes megoldásokat fogom röviden áttekinteni:

A privát felhő

Privát felhő alatt a vállalat saját infrastruktúrájának virtualizációját, illetve gyors erőforrás – azaz virtuális gép – allokálást, előállítást értünk. Ez a megoldás nyújtja a lehetőséget a legmélyebb szintű hozzáférés-ellenőrzésre, illetve a legmagasabb szintű biztonság elérésére. A privát felhő megoldások esetében az infrastruktúra beszerzése és fenntartása a vállalat feladata, mely egyben korlátot jelent a méretgazdaságossági előnyök kihasználása során.

Egy privát felhő kialakítása jó választás lehet azoknak a cégeknek, melyeknek az adatok biztonsága, illetve a bizalom kiemelt fontosságú, illetve vagy olyan nagy cégeknek, melyek elég nagyok ahhoz, hogy kiépítsenek maguknak egy adatközpontot, majd azt eredményesen és hatékonyan használják is. A Morgan-Stanley globális szinten privát felhő szolgáltatást épített ki, ugyanakkor a cég méretéből adódóan ennek méretgazdaságossági előnyei talán meg is haladják a publikus felhőszolgáltatók (pl. Amazon, Microsoft) által biztosított lehetőségeket (Smulovics, 2011).

A publikus felhő

A publikus felhőszolgáltatásokat nyújtó vállalatok hatalmas befektetéssel adatközpontokat hoznak létre, hogy aztán kiépített kapacitásukat gyakorlatilag bérbe adják ügyfeleiknek, és a

szolgáltatásra (egy SLA – Service Level Agreement keretében) felelősséget vállalnak. Ez egy olyan szerződés, mely megszabja, hogy milyen rendelkezésre állást és biztonságot garantált alkalmazásaink, adataink számára a szolgáltató.

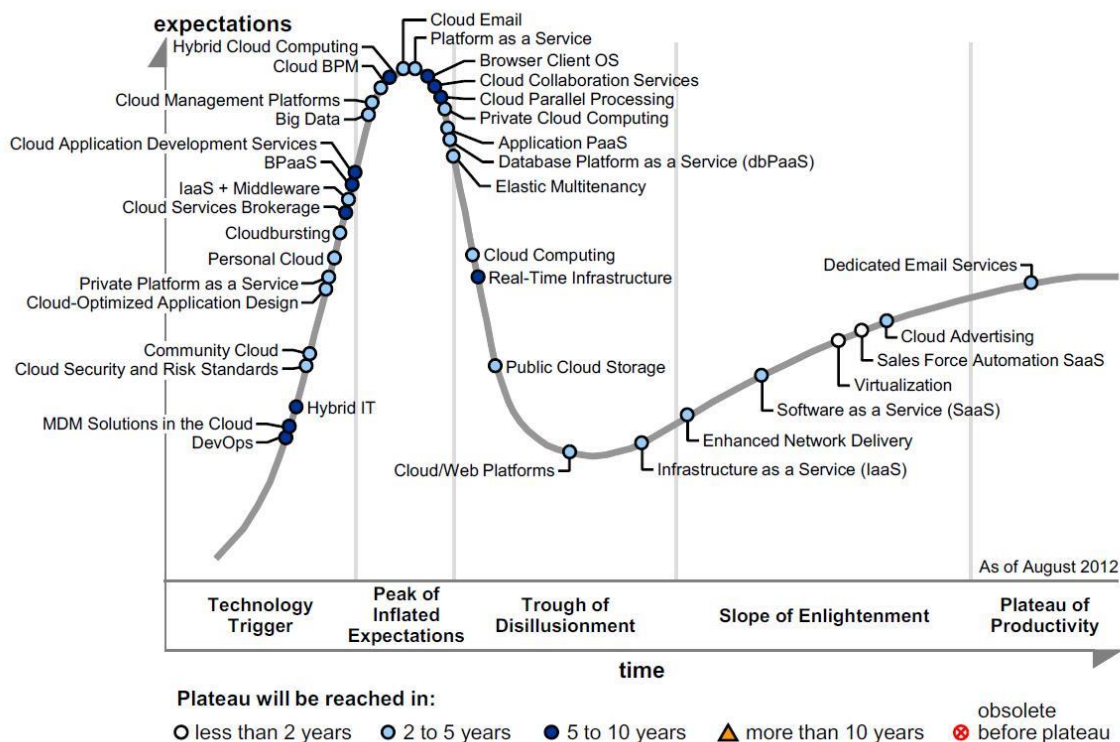
Mindamellet, hogy ez a megoldás garantálja a legnagyobb elérhető költségcsökkenést a központosított erőforrásoknak hála, magában rejt bizonyos kockázatokat is. Egy konkrét példát tekintve: Microsoft Azure szolgáltatási szint vállalása alapértelmezetten magas, 99,95%-os rendelkezésre állást garantál.

Ez az érték 0.05%-al jobb, mint az átlagos IT vállalati rendelkezésre állás (LMWHP, 2013). Az ideillő Gartner tanulmány alapján (Hunter, 2013), amennyiben az ügyfél megfelelően választja meg felhő szolgáltatóját, a rendelkezésre állás többszörös kockázati tényező, mint az, hogy a vállalat számára érzékeny adatokhoz jogosultság nélkül hozzáférjenek a felhőben.

Ez összességében azt jelenti, hogy a felhőszolgáltatásokkal szembeni biztonsági szkepticizmus és ellenséges hozzáállás alaptalan, illetve helytelen. Egyszerűen a technológia itt tart az elfogadási életciklus során.

3. ábra - a számítási felhő életciklusa, forrás: Pettay, Meulen (2012)

Figure 1. Hype Cycle for Cloud Computing, 2012



A publikus felhőre való "előfizetés" jó megoldás lehet olyan vállalatok számára, melyek ki tudják használni a felhőszolgáltatások általános előnyeit:

- Skálázhatóság: gyakorlatilag végtelen számítási kapacitás
- Nincs befektetési költség, így hosszú távú elköteleződés sincs
- Csak az a szolgáltatás, kapacitás jelent költséget a vállalat számára, amit valóban használ is
- Redundáns adattárolás
- Az erőforrások és szolgáltatások azonnal elérhetőek: egy új szerver felállítása kevesebb, mint 5 percet vesz igénybe, szemben az akár több hónappal (beszerzési kérelem, felülvizsgálat, beszerzés, leszállítás, üzembe helyezés, tesztelés, próbaüzem, éles használat)

Ezekre az előnyökre azok a vállalatok támaszkodhatnak főként, melyek:

- Nem tudják megjósolni a szerverekre váró terhelést a jövőben. Jó példa erre egy webshop, aki amellett, hogy nehezen jósolja meg, hogy hány ember fog tőle vásárolni, böngészni kínálatát. Ráadásul a szezonalitást is figyelembe kell vennie, hiszen az év vége felé, decemberben sokkal több ember vásárol ajándékot, mint mondjuk októberben (lásd: 3. sz. melléklet, mely a KFGT (2013)-on alapul). Számukra a skálázhatóság a legfőbb előny, hisz amikor megnő a látogatók száma, akkor csak feljebb kell vinni az igénybe vett kapacitás szintjét és az oldal nagyobb tökebefektetés nélkül is működhet tovább, ezáltal ideális megoldás kisvállalkozások, induló vállalkozások számára.
- Szoftverfejlesztéssel, vagy olyan, egyéb tevékenységgel foglalkoznak, mely tesztelést igényel. A fejlesztői, illetve tesztrendszerekre csak ideiglenesen van szükség: addig, ameddig a fejlesztés tart. Igaz, a fejlesztéssel foglalkozó cégek azzal védekezhetnének ezen állítással szemben, hogy a projekt lezárulta után egy újabb projekt veszi kezdetét, esetleg a meglévő szoftvert akarják javítani, javítócsomagokat kidolgozni, ehhez pedig továbbra is kell az infrastruktúra, amivel eredetileg is dolgoztak. Ám ez nincs teljesen így, hisz csak az éles üzemhez, illetve a kész rendszer teszteléséhez kell a teljes kapacitása a szervereknek, a fejlesztés kezdeti szakaszában, illetve a modultesztok alatt csak a töredék kapacitásra van szükség, ez pedig hatalmas költségcsökkentési lehetőség azok számára, akik felhőszolgáltatást választanak a hagyományos, on-premise rendszerek helyett.
- Azon vállalatok, melyek számára az üzleti sikerességhez nélkülözhetetlen az állandó rendelkezésre állás, illetve az adatbiztonság. Számukra a legvonzóbb a redundáns tárolás, illetve a felhő-szolgáltatók legnagyobb részénél opcionálisan választható geo-redundancia. Így gyors elérési időt és többszörösen biztosított tárolást érhetnek el a biztonság megtartása mellett.
- A kis és középvállalkozások, valamint a KKV-k számára a publikus felhő szolgáltatások előnyt jelentenek abban, hogy jelentős IT beruházás nélkül biztosíthatják az üzletvitelhez szükséges kapacitásokat.

A hibrid felhő

A hibrid felhő szolgáltatások ötvözik a privát és a publikus felhő-megoldásokat. Ez azt jelenti, hogy az ügyfél eldöntheti, mely alkalmazásait, rendszereit vagy szolgáltatásait akarja a privát felhőben működtetni, és melyiket egy publikus szolgáltatónál. A megoldás szépséghibája abban keresendő, hogy így megnő az ellenőrzés alá vonandó terület, a biztonság csökken, mivel a védendő terület nő, és több vállalatnál kívüli cégekben kell megbízni, ellenőrizni.

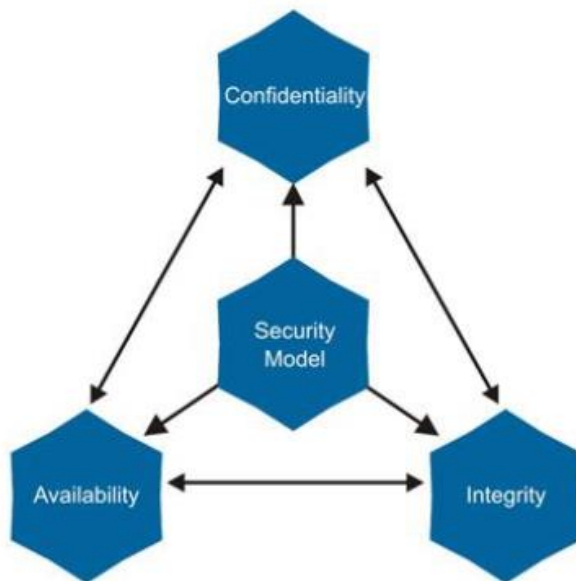
Mindemellett a közeljövőben ez jelenti a potenciális költségcsökkentés és a lehetséges alternatívák miatt: a felhasználó – ez esetben a felhasználó a vállalat vezetősége – dönti el, hogy mi hol fusson.

A felhő-megoldások negatív, kérdéses tulajdonságai

Az alábbiakban azokat a hátrányokat, vagy még inkább félelmeket sorolom fel, amelyek miatt a cloud megoldások még nem váltották fel teljesen a lokális (on-premise) rendszereket:

- EDoS (Economic Denial of Service) támadások kockázata: azok az internetes oldalak, szolgáltatások, melyek futásához felhőszolgáltató biztosítja az infrastruktúrát, védve vannak a DDoS (Distributed Denial of Service) támadásokkal szemben, hisz a rendszer a terhelés növekedésével automatikusan növeli a szükséges erőforrásokat. Az oldal működési költségei azonban akár az eredeti százszorosát is elérhetik, így a támadás mégis sikeresnek tekinthető, hisz a támadott vállalat költségeit annyira megemelték, hogy az könnyen csődbe is juthat.
- Adatok elfogásának kockázata az átvitel ideje alatt: bár az adattárolás biztonságát a szolgáltatók meg tudják oldani, a legsebezhetőbb pontot azonban az átvitel jelenti, az adatok átvitelére mindig ajánlatos VPN hálózatot kiépíteni a rendszerek között.
- Szolgáltató alkalmazottja általi támadás: az ügyfelek nem tudják, hogy konkrétan mely alkalmazottak érik el az ő személyes adataikat, így e téren meg kell elégedniük a szolgáltató által biztosított SLA-ban foglaltakkal.
- Jogi körülmények, nehéz eldönteni, hogy a felhő melyik ország jogrendszeré alá tartozik: ahol az adat van, ahol a szolgáltató, vagy ahol igénybe veszik?
- Bizalmi kérdések:
 - A felhasználók nem tudják, hogy fizikailag hol vannak az adataik
 - Az adatok esetleg a konkurenciával azonos tároló rendszerbe kerülnek
 - Adataik elveszhetnek, vagy épp nem biztonságosan törlik őket
 - Nincs ellenőrzési joguk a hozzáférések felett

4. ábra - biztonsági elvárások a felhő megoldásokkal szemben, forrás: Szommer, Balogh (2012)



A felhő szolgáltatások biztonsági modellje is a más területeken már jól ismert és használt elvárásokat tükrözi (CIA):

Confidentiality: Bizalmasság, azaz az adatokhoz csak azon felhasználók férhetnek hozzá, akiknek megvan a megfelelő jogosultságuk.

Integrity: Sértetlenség, azaz az adatok nem változnak a felhőben, egy adott lekérdezésre mindig ugyanazt a választ kell adnia a rendszernek.

Availability: Rendelkezésre állás, az SLA-ban (Service Level Agreement) foglaltak szerint. Ez határozza meg, hogy a szolgáltatás az idő hány %-ban aktív biztosan.

Szolgáltatási szintek

Nagyon fontos tisztázni, hogy a cloud computing nem egy bizonyos termék, szolgáltatás, hanem egy modell:

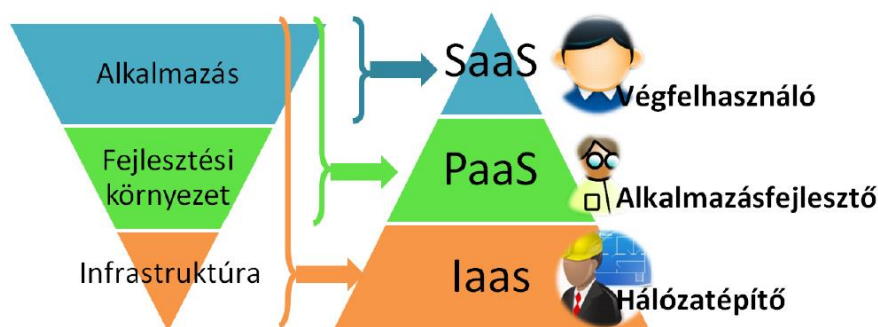
Egyedileg konfigurálható, de közösen felhasznált erőforrások.

A leggyakoribb erőforrások:

- Számítási kapacitás
- Szerver használat joga / lehetősége
- Bármikor és bárhol elérhető tárhely
- Hálózati kapacitás, infrastrukturális lehetőségek
- Bármikor és bárhol elérhető alkalmazások és szolgáltatások

Az erőforrások rendelkezésre állását, azaz azt, hogy milyen mélységig, milyen rétegekig vesszük igénybe a szolgáltató erőforrásait, a szolgáltatási szint határozza meg.

5. ábra - szolgáltatási szintek, forrás: Szommer, Balogh (2012)



IaaS – Infrastructure as a Service: a felhasználó **az infrastrukturális lehetőséget**, a számítási, tárolási és hálózati kapacitást veszi igénybe SaaS módon. Az ügyfél feladata a szükséges licencek, szoftverek beszerzése, telepítése, a szolgáltató csak az erőforrásokat biztosítja.

PaaS – Platform as a Service: a felhasználó a felhő alkalmazások **fejlesztő környezetét** is SaaS módon veszi igénybe. Egy olyan keretrendszert kap, amelyen saját maga alakíthatja ki az ön maga, vagy egy harmadik fél általi felhasználásra szánt szolgáltatást.

SaaS – Software as a Service: a felhasználó a szolgáltató felhő infrastruktúráján levő **alkalmazások szolgáltatását** veszi igénybe. Tehát az ügyfélnek nem kell beszereznie sem az infrastruktúrát, sem a szoftvereket, vagy licenceket, csak előfizet a mindezekre alapuló szolgáltatásra, amelyet bárhol és bármikor elérhet.

A szolgáltatási szintek további megvilágítását az alábbi ábra segíti, mely a felelősségi köröket mutatja be (az ábrát a Roberto Brunetti: Windows Azure: Step by step c. könyv alapján készítettem, 2011, O'Reilly Media Inc.):

6. ábra - felelősségi körök

Helyi megvalósítás	IaaS	PaaS	SaaS
Alkalmazás	Alkalmazás	Alkalmazás	Alkalmazás
Adat	Adat	Adat	Adat
Futási idő	Futási idő	Futási idő	Futási idő
Futtató környezet	Futtató környezet	Futtató környezet	Futtató környezet
Operációs rendszer	Operációs rendszer	Operációs rendszer	Operációs rendszer
Szerver	Szerver	Szerver	Szerver
Háttértár	Háttértár	Háttértár	Háttértár
Hálózat	Hálózat	Hálózat	Hálózat
	= a felhasználó felelőssége		
	= a szolgáltató felelőssége		

Jelenlegi piaci helyzet

A cloud megoldások csoportosítása a széles körben elfogadott rendszerezési elvekkel megegyezően a McAfee, Brynjolfsson (2011) alapján történt, mely elkülönülő piacok jelenlegi állapotát az alábbiakban közlöm:

IaaS: a verseny talán ebben a szegmensben a legerősebb a szolgáltatók között, ez annak tudható be, hogy egyrészt heterogén, tehát több szolgáltató van, másrészt pedig az elemzők szerint itt várható a legnagyobb növekedés, ez a szektor fog a legmagasabb növekedési ütemmel bírni (Anderson, et al, 2012). Az eddigi növekedési ütem is nagyon magas volt, két év alatt 25%-al nőtt az IT felhőszolgáltatások száma. A szolgáltatók között van a Microsoft (Azure), az Amazon (Amazon Web Services), a Google (Google Cloud) és hazai előnye, jelenléte miatt ide sorolandó még a Cloud.hu -is.

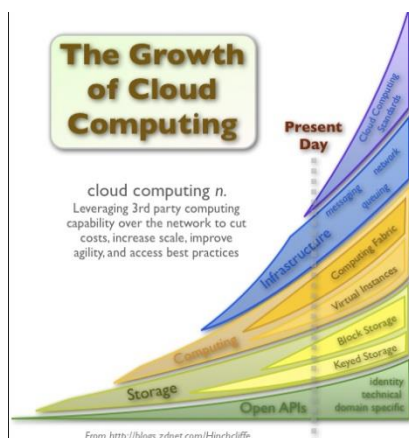
PaaS: az egyértelmű piacvezető itt a Google az AppEngine termékével, mely biztos alapot nyújt a fejlesztők számára a szoftverfejlesztéshez. 2010-es indulása után azonban komoly konkurencia lett a Microsoft Windows Azure: AppFabric is, melynek előnye, hogy habár .net alkalmazások fejlesztésére specializált, ám nem korlátozták erre az egyetlen platformra.

SaaS: már sok nagy cég használ cloud megoldásokat: Salesforce, Blizzard, a legtöbb bank (Netbank szolgáltatások), Gmail, Dropbox, OnLive. Ahogy az internet elterjedésével szinte kötelező lett a cégek számára a jelenlét az interneten (saját weboldal, adott esetben web shop), úgy a trendek azt mutatják, hogy a felhő szolgáltatások is utat nyernek maguknak, hisz ezáltal csökkenthetők a költségek, az eddig nagy kihívásnak tartott geológiai problémák (távolság) pedig megoldódnak. A felmérések szerint 2012-ben az internet használók 56%-a használ cloud alapú e-mail szolgáltatást, mint Gmail, Hotmail vagy Yahoo! Mail, ez az érték pedig a következő évben 60%-ra fog nőni (Malik, 2010).

Trendek, előrejelzések a cloud computing jövőjére vonatkozóan

Most, hogy már megismerkedtünk az IT felhők múltjával és jelenével, foglalkozzunk a jövőjükkel is, az elkövetkező évek IT trend előrejelzései segítségével.

7. ábra - a felhő szolgáltatások növekedése, forrás Hinchcliffe (2010)



A cloud szolgáltatások jövője egyértelműen biztosított, ez nem lehet kérdés, ha olyan sikeres termékeket és szolgáltatásokat lehetett rájuk építeni, mint a fent említettek. A jövő „befelhősödését” jelzi előre a legtöbb nagy elemző, illetve IT cég, szakember (lásd: 7. ábra).

Azonban meg kell jegyeznünk, hogy a jelenlegi hozzáállások mellett – az IT szakembereknek, CIO-knak nincs pozitív véleményük a számítási felhőkről, sokan a munkájuk jövőjének végét látják bennük – jelenleg egy publikus felhő megoldás, mint az Amazoné vagy a Microsofté, az üzleti élet számára vállalhatatlan.

Ám a hibrid felhők ideje már most eljött, ezt támasztja alá a Gartner prioritás mátrixa is, mely szerint a hibrid-IT eljövetele, azaz a technológia teljes elfogadása a szakma által 5-10 éven belül várható:

8. ábra - prioritás mátrix a számítási felhőre, forrás: Hunter (2011)

Figure 2. Priority Matrix for Cloud Computing, 2012

benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational	Virtualization	Big Data Cloud Advertising Cloud Computing Community Cloud Platform as a Service	DevOps Hybrid Cloud Computing Real-Time Infrastructure	
high		Application PaaS Cloud BPM Cloud Management Platforms Cloud Security and Risk Standards Cloud/Web Platforms Cloudbursting Cloud-Optimized Application Design Elastic Multitenancy Enhanced Network Delivery Infrastructure as a Service (IaaS) Personal Cloud Private Cloud Computing	Cloud Application Development Services Cloud Parallel Processing Cloud Services Brokerage Hybrid IT	
moderate	Sales Force Automation SaaS	Cloud Email Database Platform as a Service (dbPaaS) IaaS + Middleware Private Platform as a Service Public Cloud Storage Software as a Service (SaaS)	BPaaS Cloud Collaboration Services MDM Solutions in the Cloud	
low		Dedicated Email Services	Browser Client OS	

As of August 2012

Source: Gartner (August 2012)

Az S&T Magyarország bemutatása

Az 1993-ban alapított S&T Csoport az egyetlen olyan termék-független vállalat az IT rendszerintegráció és tanácsadás területén, melynek 17 országra kiterjedő földrajzi lefedettsége, helyi jelenléte van a közép- és kelet-európai régióban, illetve Ázsiában.

Az S&T fő tevékenységi területei az informatikai tanácsadás és rendszerbevezetés, valamint az egyedi IT megoldások és rendszerek tervezése, építése és üzemeltetésének támogatása. Az S&T a teljes informatikai értéklánc mentén nyújt szolgáltatásokat a közép- és nagyvállalatoknak. A csoport szakemberei átfogó szakmai ismeretekkel és szerteágazó

tapasztalatokkal rendelkeznek a következő iparágakban: gyártás, kereskedelem, telekommunikáció, államigazgatás, pénzügyintézetek, közművállalatok, autópálya, légi- és védelemipar.

9. ábra - S&T cégek Európában, forrás: www.snt.hu



Az S&T Consulting Hungary Kft. hálózati, IT-biztonsági és adattárolási rendszerektől, az integrált vállalatirányítási megoldásokon át, egészen a mérnöki tervező szoftverekig, testreszabott standard megoldásokat és egyedi fejlesztéseket készít közép- és nagyvállalatok, állami intézmények részére. A vállalat – elődcégeivel együtt – több mint tizenöt éve működik sikerrel a hazai és nemzetközi informatikai szolgáltató piacon.

Az S&T Consulting Hungary Kft. Managed Services - ügyféltámogatás, konzultáció, tanácsadás, termékfejlesztés - szolgáltatási területének keretében is nyitott az új technológiák és megoldások iránt, illetve stratégiai partnerségben áll a Microsoft Magyarország Kft.-vel.

2013-ra az S&T Consulting Hungary Kft a világon elsőként lett Microsoft Managed Service Provider. Ennek keretében jogosult arra, hogy az Azure szolgáltatásokat illesszen be saját infrastruktúra építő és integráló portfóliójába.

Az S&T és a DR

A következő fejezetben bemutatom a vállalat és a DR rendszerek kapcsolatát azáltal, hogy elemzem igényeit egy DR rendszerrel szemben, ennek okait, tehát azt, hogy miért kell a vállalatnak üzletmenet folytonosságot biztosító megoldás.

Jelenleg használt DR megoldás

Jelenleg az S&T Consulting Hungary Kft. 1. szintű DR megoldást alkalmaz. Ezt a képet árnyalja, hogy egyes rendszerei magas rendelkezésre állásúak, illetve rendszeresen végez biztonsági mentéseket adatairól.

Mindazonáltal mindkét tényező figyelembe vétele esetén sem beszélhetünk magasabb szintű DR megoldásról, például egy természeti katasztrófa esetén rendszerek egész csoportja állhat le, illetve adatok veszhetnek el. (A fenti kijelentésemet belső felmérésemre és a BCPHB 2007-re alapozom).

Azonban a vállalatnak szüksége van DR megoldásra, ugyanis az elsődleges rendszerek elvesztése esetén elvesztené a kapcsolatot az ügyfeleivel, mint az IT megoldások szolgáltatója: az ügyfelei nem tudnák bejelenteni a hibákat, nem tudna az S&T árajánlatot adni. Ezek összessége pedig súlyos presztízsveszteséget okozna a cégnél, mely a jövőbeni üzletmenetet nehezítené meg, illetve ügyfélvesztéssel eredményezhetne.

Az S&T igényei egy DR rendszerrel szemben

Az S&T vezetőségével való interjúm után egyértelművé váltak az igények egy megvalósítandó DR rendszerrel szemben, amelynek: **a BCP (Business Continuity Planning – Üzleti Folytonosság Terv) -vel összhangban és a költséghatékonyságot kiemelt szempontként tartva az üzletileg kritikus szolgáltatások állandó működését kell biztosítani, méghozzá a dolgozat során bemutatott 4. DR szint követelményei szerint.**

A fenti döntés meghozatala előtt elemeztem az üzletileg kritikus szolgáltatásokra veszélyt jelentő vészhelyzeteket, katasztrófákat, ezek bekövetkezésének valószínűségét és a bekövetkezésük esetén létrejövő pénzügyi, jogi, illetve a vállalat presztízisére gyakorolt hatását. Annak eldöntését, hogy mely szolgáltatás üzletileg kritikus, BIA (Business Impact Analysis) segítségével határoztam meg (Ramesh, 2002). Ezen adatokat az S&T kérésére nem közlöm, csak az alábbi táblázatot, melyben bemutatom a cég által jelenleg használt szolgáltatásokat, alkalmazásokat:

10. ábra - Szolgáltatások üzleti kritikussága

Szolgáltatás megnevezése	Szolgáltatás leírása	Üzletileg kritikus az adott szolgáltatás?
SAP	ERP (Enterprise resource Planning), azaz vállalatirányítási rendszer, a vállalat minden részlegére kiterjedő erőforráskezelő	IGEN
COGNOS	Az IBM által fejlesztett, integrált BI (Business Intelligence), azaz üzleti intelligencia rendszer, amely az üzleti tervezést segíti	NEM
CRM	Customer Relationship Management rendszer, az ügyfelekkel való bizalmi kapcsolatot, illetve az ügyfélszegmentálást segítő rendszer, mely saját adatbázissal rendelkezik (Winer, 2001).	NEM
OCS	Microsoft Office Communication Server, a szervezeten belüli kommunikáció könnyítése érdekében	NEM
NETSEC	Check Point biztonsági szolgáltatás az jogosulatlan hozzáférések megakadályozása érdekében.	IGEN
Active Directory	A Microsoft hálózati szolgáltatásainak gyűjtőneve, a szolgáltatás segítségével ellenőrizhetők és kezelhetők az alkalmazottak Windows profiljai.	IGEN
SolveDirekt & RcG	SolveDirect központi, illetve RcG lokális hibajegy-kezelő rendszerek.	IGEN
SharedPoint portal	Központi intranet portál szolgáltatás a bizalmas információk biztonságos elérésének garantálására.	NEM
EMC archiválás	Adatarchiválást biztosító szolgáltatás laptopok, pc-k, szerverek és e-mail tartalmak számára.	NEM

Szolgáltatás megnevezése	Szolgáltatás leírása	Üzletileg kritikus az adott szolgáltatás?
--------------------------	----------------------	---

ForeFront antivirus	A Microsoft biztonsági programcsomagja vállalati adatok védelme és a hálózati hozzáférés szabályozásának biztosítása érdekében.	NEM
MS SCCM	Microsoft System Center Configuration Manager a windows alapú vállalati infrastruktúra kezelésére.	NEM
MS Exchange.	A Microsoft vállalatok számára fejlesztett e-mail rendszere.	IGEN

Üzletmenet folytonosság szempontjából a vállalat az üzletileg kritikus szolgáltatásokra koncentrált, így ezeknek a szolgáltatásoknak DR site-on való biztosítása mellett döntött.

Az egyes szolgáltatások üzleti kritikusságának sorrendjét a *1. sz. melléklet* mutatja (magasabb érték = üzletileg kritikusabb szolgáltatás). Ez alapján pedig már megszülethetett a végső döntés, hogy mely konkrét szolgáltatásokat kell DR-ben is biztosítani. Ezek pedig az alábbiak:

Active Directory, RCG – SolveDirect, E-mail, NETSEC, SAP.

Az üzletileg kritikus szolgáltatások kiesésére a cég a következő kockázatelemzést végezte el (melyet jelen dolgozat keretei között adottságnak fogadunk el):

11. ábra - szolgáltatások kiesésének pénzügyi kockázatelemzése

Szolgáltatás megnevezése	Szolgáltatás kiesésének valószínűsége a vizsgált három évben	Kiesés esetén a veszteség becsült mértéke	Kockázati tényezővel súlyozott várható veszteség
SAP	5%	3 000 000.-	150 000.-
NETSEC	5%	15 120 000.-	756 000.-
Active Directory	5%	1 300 000.-	65 000.-

Szolgáltatás megnevezése	Szolgáltatás kiesésének valószínűsége a vizsgált három évben	Kiesés esetén a veszteség becsült mértéke	Kockázati tényezővel súlyozott várható veszteség
SolveDirekt & RcG	5%	135 000 000.-	6 750 000.-
MS Exchange.	5%	1 000 000.-	50 000.-
Kockázati tényezővel súlyozott várható veszteség összesen:			10 891 000.-

Az eddigiek rövid összegzése: bemutattam, hogy mik azok a DR rendszerek, hogy miért fontosak és mik a korlátaik, amiért nem terjedtek el jobban. Ezután ismertettem a cloud megoldásokat, mint lehetséges alternatívát a hagyományos DR megoldásokra, az elkövetkezőkben pedig a gyakorlatban nézem meg, hogy melyik megoldás a költséghatékonyabb, illetve először azt, hogy megvalósítható-e egyáltalán mind a kettő?

DR megvalósítási alternatívák

Egy megfelelő DR rendszer megvalósítására két potenciális alternatíva is kínálkozik az S&T számára:

- A hagyományos megoldás, mely értelmében CAPEX-ként (Capital Expenditure, azaz befektetési költségként) beruháznak egy bizonyos nagyságú infrastruktúra-állományba, majd azt egy megfelelő helyen beüzemelik, beszerzik a szükséges szoftvereket, és megkezdik a DR rendszer telepítését, az adatok szinkronizálását.
- Felhő szolgáltatás igénybe vétele, mely esetében befektetési költségek nélkül, tisztán működtetési költségként (OPEX – Operating Expenditure) alakíthatják ki igényeiknek megfelelő DR rendszerüket.

Módszertanát tekintve mindkét alternatívára TCO számítást végzek. TCO számítás esetében az adott időszakra vonatkozó összes beruházási, illetve fenntartási költséget figyelembe veszem. Meg kell jegyeznem, hogy felhőszolgáltatások kapcsán nem beszélünk beruházásról, így a beruházás arányos mutatók csak korlátozottan alkalmazhatóak.

A TCO számítások esetében nem a számviteli, hanem pénzügyi értelemben vett költségeket, azaz a cash-flow szemléletet vesszük figyelembe. Magyar nyelven a legjobban a költség szóval lehetne megragadni, ugyanakkor ennek a kifejezésnek a használata nem gyökerezett

még meg. Éppen ezért a TCO számítások során használt költség fogalom alatt minden esetben a költség tartalmát (cash-flow szemlélet) értjük.

A Windows Azure bemutatása

Figyelembe véve, hogy az S&T a Microsoft Magyarország Kft. stratégiai partnere és azt, hogy a nagy szolgáltatók között nincs jelentős árkülönbség, egyértelmű volt, hogy az S&T a Windows Azure-t vizsgálja meg első helyen a felhő szolgáltatások között. Jelen fejezetben ezt a technológiát mutatom be részletesen.

A Windows Azure a Microsoft 2010. február 1.-én indult felhőszolgáltatása. Nagyon fiatal szolgáltatásnak számít a többi felhőhöz képest - hisz az Amazon Web Services már 2006-ban debütált, a Google App Engine szolgáltatása pedig 2008-ban – ám ezt bőségesen ellensúlyozza többoldalúságával: nem csak IaaS, hanem PaaS és SaaS szolgáltatásokat is integráltak egyetlen felületre: ugyanazon az oldalon lehet beállítani egy új weboldalt, indítani egy virtuális szervert és új fejlesztői környezetet létrehozni. Ez a multifunkcionalitás egyedülálló, egyetlen olyan másik szolgáltató sincs, aki egy interfészen keresztül adna lehetőséget a három szolgáltatási szint egyidejű használatára. Ennek illusztrálására szolgál a következő ábra:

12. ábra - az Azure szolgáltatások struktúrája, forrás: Farkas et al (2013)



Az SLA-ban 99,95%-os rendelkezésre állást garantál a szolgáltató, melyet saját, helyi rendszerrel csak indokolatlanul nagy költségekkel lehetne biztosítani (Racsó 2012).

Az S&T igényeinek megfelelő hagyományos DR megvalósítás

Az alábbiakban bemutatom az eddig ismertetett igényeknek eleget tevő hagyományos DR megoldást, annak pontos paramétereivel, problémáival, üzleti előnyeivel és hátrányaival, illetve költség számításokkal.

A megvalósítás műszaki leírása, paramétere

A hagyományos megvalósítás műszaki paramétereinek meghatározását az S&T-vel közösen végeztem, miután ismertettem azokat a szolgáltatásokat, melyek futtatását a másodlagos rendszernek biztosítani kell (Active Directory, RCG – SolveDirect, E-mail, NETSEC, SAP). Így az alábbi konfiguráció lett megállapítva:

13. ábra – hagyományos megvalósítás műszaki paramétere

Megnevezés	Specifikáció	Szükséges darabszám
Processzor	4 magos	4
Memória	64 GB	4
Háttértár	6 TB	1

A fenti hardware erőforrásokon, virtualizált környezetben futna az összes szolgáltatás, amennyiben az elsődleges rendszer összeomlik.

További információk a megvalósításról:

- A megvalósítás helyszínének Tolna megye lett kiválasztva természeti biztonsága (Magyarországon ez a leg földrengés-biztosabb megye) miatt.
- Jelen alternatíva esetén a szerverek dedikált szervertermekben kerültek volna elhelyezésre . Ennek költsége a „A hagyományos DR rendszer fenntartási költsége” című fejezetben mutatom be.

Megvalósíthatósági problémák

Az elsődleges problémákat és nehézségeket az alábbiak jelentik egy hagyományos DR site megvalósítása esetén:

- Szélessávú kapcsolat kiépítése a két rendszer (elsődleges és másodlagos) között: a szélessávú kapcsolatban biztosnak kell lennie bármilyen időjárási viszony esetén, illetve alternatív útvonalakat is ki kell alakítani az adatsomagok számára. Ezen okok miatt külön SLA-t érdemes kötni a hálózat szolgáltatóval.
- Szélessávú kapcsolat titkosítása: az adatok elfogásának lehetőségét ki kell zárni, ennek leghatékonyabb módja VPN kapcsolat felállítása, illetve valamilyen titkosítási algoritmus használata (pl.: RSA, AES 256).
- A DR rendszer által igényelt szoftverek: ezeket integrálni kell az összes olyan elsődleges rendszerbe, amelyből a mentéseket, illetve adat szinkronizációt végezni kívánjuk.
- Vállalati tűzfal: engedélyezni kell a DR szoftver számára a szinkronizációt, ám meg kell akadályozni minden egyéb jogosulatlan hozzáférést. Az új szoftver bevezetése egy újabb támadási felületet jelent, amit védeni kell.

Az implementáció időtartama és költsége

Az implementáció időtartama egy olyan tényező, mely egyes cégek számára kritikus: az igény megszületése után minél hamarabb éles üzembe kell állítani, mert a katasztrófa bekövetkezésére az idő elteltével egyre nagyobb lesz az esély. Hagyományos beszerzés esetén az alábbi folyamatok, alfolyamatok mennek végbe a beszerzés és beüzemelés során:

14. ábra - hagyományos megvalósítás implementációjának költsége

Folyamatlépés/alfolyamat megnevezése	Folyamatlépés/alfolyamat leírása
Igény új erőforrásokra	Döntés születik arról, hogy DR rendszert kell kiépíteni, majd elemzik, hogy mely rendszerek működését kell biztosítani és megállapításra kerül, hogy milyen infrastruktúra beszerzése indokolt.
Árajánlatok kérése	A kívánt infrastruktúra specifikációja ezután a beszerzési munkatárshoz kerül, aki eldönti, hogy kitől, mely beszállítótól érdemes árajánlatot kérni.

Ajánlatok elbírálása	A visszakapott árajánlatokat a vállalat egyéni értékrendje szerint elbírálják, majd kiválasztják a nyertes beszállítót.
Szerződéskötés a beszállítóval	A kiválasztott beszállítóval megkötöttetik a szerződés.
Hardware leszállítása	A beszállító leszállítja a megrendelt hardvert, amit az átvétel során a megrendelő ellenőriz.
Hardware beüzemelése	A megérkezett hardvert üzembe állítják, azaz elhelyezik, elvégzik a szükséges konfigurációs beállításokat, áram alá helyezik.
DR szoftver implementálása	Szoftver kompatibilitásának és megfelelő működésének tesztelése.
Próbaüzem	A próbaüzem során ellenőrzik, hogy megfelel-e az egyedi igények kielégítésére és minden megfelelően működik-e.
Éles üzem	Az infrastruktúra készen áll az éles üzembe helyezésre. A folyamat elején kialakult vállalati igény teljesítetté válik.

Ez a folyamat akár fél évig is eltarthat, ami jelentősen megnövelheti az üzleti kockázatokat, adott esetben ugyanis a vállalat vezetése számára ismert tény, hogy valami katasztrófa fog bekövetkezni, ami ellen nem tehetnek mást, mint egy DR rendszer kiépítését. (Ilyen eset lehet az is, amikor ismert tény, hogy egy folyó ki fog önteni, és nincs idő vagy lehetőség az elsődleges rendszer elköltöztetésére.)

A hagyományos DR rendszer teljes tulajdonlási költsége

A fentebb ismertetett megvalósítás becsült teljes tulajdonlási költségei 3 évre a következő táblázat szerint alakul. A táblázatban nem elég csak az infrastruktúra beszerzési és integrációs költségeit elemezni, a fenntartási kiadásokat is figyelembe kell venni. Ezek az összegek gyakran nagyobbak, mint azt a felhasználók, vagy az üzleti vezetők hiszik. Egy adatközpont áramfogyasztása akár a TCO – azaz a tulajdonlás teljes költségének – 15-20%-a is lehet (Farkas, et al, 2013).

Információk a táblázathoz:

- A költségcsatások 235-ös USD/HUF árfolyamon lettek elvégezve.
- Karbantartási költségeket, fűtési / hűtési költségeket, bérleti költségeket a jelenlegi, átlagos piaci ár alapján határoztam meg.
- Az áramfogyasztás az S&T saját mérési eredményei és a gyártói adatok alapján lett számolva.
- Biztonsági rendszer alatt videokamerát és biometrikus beléptetést értek.
- Hardware tekintetében az S&T a HP ProLiant Gen8 szervercsaládot választotta.
- Software tekintetében az S&T a CA ARCserve D2D backup megoldást választotta. (<http://www.arcserve.com/us/products/d2d/features-overview.aspx>)
- A számításokat a széles körben elfogadott és bevett módszer szerint három évre számoltam.

15. ábra - hagyományos megvalósítás teljes tulajdonlasi mutatója

Évek száma	0	1	2	3	
Beruházási költségek					
Alkalmazás szerver	20 000				
Adattároló szerver	8 000				
Integrációs és beüzemelési költségek	2 000				
Szoftver beszerzési költsége	564				
Fenntartási költségek					
Hardver karbantartási költsége		1 700	2 100	2 500	
Szoftver követési díj		113	113	113	
DR site bérlet		140	140	140	
Helyszín biztosítás		60	60	60	
Védelem és egyéb költségek	120	100	100	100	
Áram		257	257	257	
Fűtés - hűtés		105	105	105	
Költség összesen	30 684	2 475	2 875	3 275	39 308
NPV	30 684	2 281	2 442	2 564	37 971
r (konzervatív) =	8,50%				
Mértékegység =	eFt				

= Folyó költség

= NPV költség

Hagyományos megvalósítás esetén a teljes tulajdonlasi költség nettó jelenértéke tehát 37 971 000 Ft.

A hagyományos megvalósítás üzleti előnyei és kockázatai

A hagyományos megvalósítás üzleti előnyei közé az alábbiak tartoznak:

- Az adott vállalat tisztában van az általuk használt hardware állapotával, elhelyezkedésével, illetve a biztonsági és üzemeltetési részletekkel.
- A megbízhatóság megegyezik a vállalati infrastruktúra többi elemével. Az eddigiekhez képest nem kell új megoldásokat alkalmazni.

- Könnyebben beleilleszkedik a megszokott „gondolatmenetbe”, kevésbé radikális megoldás. Éppen ezért könnyebben elfogadja a szervezet, nem jelent változást.
- A költségek állandó jellegűek, jelentős változásuk nem várható (Jelentős változás alatt +-30%-os árcsökkenést, illetve árnövekedést értek).

Ezzel megegyezően természetesen hátrányai is vannak ennek a megvalósítási alternatívának:

- Az ára nagyon magas a veszélyeztetett adatok elvesztése esetén létrejövő üzleti hátrányokhoz képest (lásd: „Az S&T igényei egy DR rendszerrel szemben” fejezet, üzletileg kritikus szolgáltatások kiesésének kockázatát és az ezáltal létrejövő pénzügyi veszteséget bemutató táblázat).
- Egy újabb rendszer, melyet integrálni kell a meglévő vállalati infrastruktúrába, ezzel párhuzamosan pedig újabb támadási felületet jelent, ami nehezíti a cég informatikai biztonságának megtartását.
- Az S&T felelőssége az infrastruktúra fenntartása, karbantartása.
- Az on-premise megoldás rugalmatlan, azaz nem lehet könnyen sem DR szintet, sem technológiát váltani abban az esetben, ha a vállalat igényei megváltoznak a megoldással szemben.

Az S&T igényeinek megfelelő DR site megvalósítása a számítási felhőben

A hagyományos DR megvalósítás részletes ismertetése után bemutatom a felhő szolgáltatást felhasználó megoldást is annak érdekében, hogy a konklúziók levonása előtt objektív összehasonlítást lehessen végrehajtani.

A szükséges felhő szolgáltatás konfigurációs beállítások ismertetése, indoklása

Az S&T igényeinek megfelelő kapacitás biztosítását a Windows Azure Management portálján állítottam be az alábbi értékekre:

16. ábra - Azure megvalósítás műszaki paraméterei

Megnevezés	Specifikáció	Szükséges darabszám
Large VM (Virtual Machine)	4 magos	4
Memória	64 GB	4
Háttértár	6 TB	1

A fenti értékek teljes egészében megegyeznek az on-premise megvalósítással, azonban ez a háttértár valójában többnek felel meg, két okból is. Elsősorban a hardware gyártók terminológiája szerint 1TB = 1 000 000 MB, valójában azonban 1 048 576 MB. Másodsorban pedig az operációs rendszer és a file-rendszer által elfoglalt terület jelentékeny nagyságú, ezzel pedig csökken a valóban, szabadon rendelkezésre álló tárterület. Azure megvalósítás során azonban az igénybe vett tárterületbe nem számít bele sem az operációs rendszer, sem a file-rendszer által lefoglalt terület.

Megvalósíthatósági problémák

A megvalósíthatósági problémák az Azure esetében kompatibilitási problémákat jelentenek. Nem minden program költöztethető ugyanis a felhőbe. Ilyenek alkalmazások az alábbiak:

- Olyan ellenőrző programok, melyek azt az adott gépet (laptop, munkaállomás, PC, szerver) figyelik, monitorozzák, hogy megfelelően működnek-e, amin futnak (Betts, et al, 2012).
- Nagy erőforrás-igényű alkalmazások (például ERP rendszerek, Active Directory). Ezen programok erőforrásigénye egyenesen arányos az általuk menedzselt modulok és felhasználói profilok számával. A megvalósíthatósági problémát az jelenti, hogy az Azure-ban van egy korlát, mely szerint nem lehet 20 processzormagnál többet használatba venni egy felhasználói profil alatt. Ezáltal ennél nagyobb erőforrást igénylő alkalmazások felhőbe költöztetése nem lehetséges (megjegyzés: kevés felhasználót menedzselő, tehát csekély erőforrás-igényű rendszerek, Active directory Azure-ban való futtatása lehetséges).

A meglévő rendszerrel való integráció időtartama és költsége

Ezen megvalósítás esetében nincs értelme beszerzési időtartamról beszélni, hiszen épp az a megoldás lényege, hogy nem kell beruházni infrastruktúrára. Így az integráció időtartamát fogom ismertetni az alábbiakban:

17. ábra - Azure integráció folyamatlépései és időtartama

Folyamatlépés/alfolyamat megnevezése	Folyamatlépés/alfolyamat leírása	Becsült időtartam
Igény új erőforrásokra	Döntés születik arról, hogy DR rendszert kell kiépíteni, majd elemzik, hogy mely rendszerek működését kell biztosítani.	Kevesebb, mint két munkanap. Ennél rövidebb idő alatt – akár órák alatt – is végrehajtható ez a folyamat, ám vezetőségi döntést igényel a folyamat megkezdése, így a két nap realisabb, biztosabban teljesülő érték.
Erőforrásigények meghatározása	A kiválasztott rendszerek és igények alapján meghatározásra kerülnek az Azure-ban használni kívánt erőforrások.	Kevesebb, mint egy nap. Amennyiben nem megfelelően lettek kiválasztva az erőforrások, akkor azok pár perces beállítás-módosítás segítségével bármikor változtathatóak

MS Windows Azure Account létrehozása	Amennyiben nincs a vállalatnak Windows Azure account-ja megfelelően hitelesítve – valós telefonszám, bankszámlaszám, számlázási adatok és cím –, akkor létre kell hozni egyet.	Egy új account regisztrálásának feldolgozására a Microsoft 24 órás felső határt ad meg, maximum egy nap, amíg kialakítják használtára készre a vállalati profilt.
Alkalmazások telepítése és konfigurálása	Az operációs rendszer, szükséges keretrendszerek és a DR site-on futtatni kívánt szolgáltatások telepítése, konfigurálása.	3 nap, ebből a legtöbb időt a konfigurációs beállítások töltik ki.

Az integráció költségét azok az emberi munkaórák jelentik, amelyek a szükséges konfigurációs beállítások végrehajtásához, illetve az adatmigráció, adatszinkronizáció elindításához, automatizáláshoz kellenek. Ennek becsült értéke a következő – „Az Azure-ban használt erőforrások költsége című” – fejezet táblázatában található.

Az Azure-ban használt erőforrások teljes tulajdonlási költsége

Az alábbi táblázat értelemszerűen nem egyezik meg a hagyományos megvalósításnál használt táblázattal, ugyanis Azure megoldás esetében más költségtelekkel kell számolnunk: az első esetben a VPN kapcsolatnak nincs külön költsége, míg az Azure megvalósítás esetén a beszerzési költségek vesztik értelmüket.

További információk a táblázathoz:

- Az SQL lekérdezések költsége a lekérdezések havi számától függ. A táblázatban szereplő értékek az S&T Consulting Hungary Kt.-nél 2013. február 3-tól 2013. március 4-ig tartó mérési eredmények alapján lettek meghatározva.
- Az adatforgalom költségében csak az Azure-ról való letöltés szerepel, a feltöltés nem jelent költséget a vállalat számára.
- A költségszámítások 235-ös USD/HUF árfolyamon lettek elvégezve.
- Amennyiben a cég féléves vagy éves hűségsszerződést köt, úgy a három évre vetített költségek 3 384 000 Ft-tal csökkennek. Azért nem a csökkentett érték szerepel a táblázatban, mert így a variabilitás, mint üzleti előny elveszne.
- Az Azure szolgáltatásokhoz tartozik egy lista, hogy milyen hálózati eszközökkel érhetőek el. Valójában lényegesen több eszközzel létrehozható a kapcsolat, ám a Microsoft csak a listában szereplő eszközök használata esetén biztosítja a támogatást (supportot). A listára mutató link a kutatásom forrásai között található (VPN, 2013).

- A táblázatban szereplő költségek drasztikusan csökkenthetők, amennyiben alacsonyabb DR szint lesz az elvárt a cég felől.

18. ábra - Azure mevalósítás teljes tulajdonlási mutatója

Évek száma	0	1	2	3	
Beruházási költségek					
Azure kompatibilis hálózati eszközök	90				
Integrációra és konfigurációra fordított emberi munkaórák költsége	100				
Szoftver beszerzési költsége	564				
Fenntartási költségek					
Számítási kapacitás		2 431	2 431	2 431	
Tárolási kapacitás		1 044	1 044	1 044	
VPN kapcsolat költsége		106	106	106	
Active Directory		-	-	-	
SQL lekérdezések költsége	120	396	396	396	
Adatforgalom költsége		314	314	314	
Költség összesen	874	4 292	4 292	4 292	13 749 = Folyó költség
NPV	874	3 955	3 646	3 360	11 835 = NPV költség
r (konzervatív) =	8,50%				
Mértékegység =	eFt				

Az Azure megvalósítás üzleti előnyei és kockázatai

Az Azure megvalósítás üzleti előnyeit az alábbiakban mutatom be:

- Elsődleges előny lehet a legtöbb vállalat számára az ára ennek az alternatívának. Befektetési költség nélkül, alacsony működési költségek mellett biztosít magas szintű disaster recovery megoldást.
- Skálázhatóságot biztosít, azaz amennyiben a cég igényei saját DR rendszere felé megváltoznak, úgy gyorsan és könnyen lehet a meglévő DR rendszert az új igényekre szabni.
- Egy másik nagyon fontos előnye az Azure megoldásnak az, hogy out-of-the-box, azaz azonnal használható, és alapesetben (default) bekapcsolt biztonsági beállításokat tartalmaz. Ezek egy része szoftveres – például tűzfal – másik része pedig hardveres – például állandó biztonsági szolgálat, telephely infrastruktúrájának biztonsága – alapokon nyugszik. Így összességében egy mélységi védekezéssel ellátott rendszer áll a rendelkezésünkre (Kaufman, Venkatapathy, 2010).
- Az adatok tárolásának módja általunk választott tulajdonság, így akár magas szintű – AES 256 – titkosítással is elláthatjuk üzletileg kritikus adatainkat (CSDS,2013).
- Ezen megvalósítás esetében nem kell elköteleznie magát a megrendelőnek három évre egy szolgáltató felé, így amennyiben az évek során egy másik szolgáltató ajánlata kedvezőbb lesz, a vállalat minimális költséggel válthat át.

Ahogy a megvalósítás előnyei, úgy a hátrányai is a felhő-megoldás természetéből származtathatóak:

- A cég nem fér hozzá fizikailag az általa használt erőforrásokhoz. Így amennyiben valami probléma adódik az infrastruktúrával, akkor nem teheti meg a szükséges lépéseket a hiba elhárítására, csak várhat, amíg a szolgáltató kijavítja az üzemzavar forrását.
- A racionális üzleti döntésen kívül itt egy szintén üzleti, de bizalmi döntést is kell hoznia a vállalatnak. Meg kell bíznia a választott szolgáltatójában ahhoz, hogy érzékeny üzleti adatokat helyezzen saját fizikai rendszereinek hatókörén kívülre.
- A cég könyvelésében kizárólag üzemeltetési költségek fognak megjelenni ebben a témában, ami eltér az eddig megszokott költségektől. A felhő szolgáltatások igénybe vétele a hagyományos tervezéstől eltérő logikát képvisel, melynek a szervezet kultúrájába bele kell épülnie.
- A cégnek alaposan tanulmányoznia kell a szolgáltató által nyújtott SLA-t, ugyanis annak ki kell térnie az adatok jogi birtoklására és a szétválás feltételeire is. Ezek nagyon fontos információk, meglétük nélkül a vállalat kiszolgáltatottá válik szolgáltatója felé.

A megvalósítási lehetőségek összehasonlítása

Az eddigiekben bemutattam, hogy mik azok a DR rendszerek, hogy miért fontosak, és azt is, hogy komoly korlátaik vannak. Ezután ismertetésre kerültek a felhő megoldások, és az az elképzelés, hogy a DR rendszerek korlátaikat az új megoldással lehetne ledönteni.

A továbbiakban összehasonlítom a két megvalósítási alternatívát annak érdekében, hogy kutatásom kérdésfelvetésére a válaszem – azaz dolgozatom konklúziója – megfelelően alátámasztott legyen.

Összehasonlítás képességek alapján

A két alternatíva összehasonlításának első lépéseként a képességeket elemzem. Alapvetően mindkét rendszer ugyanazt a célt szolgálja: az elsődleges üzleti rendszerek és adatok biztosítása egy DR site által, mely abban az esetben, ha az elsődleges rendszerekben kár keletkezik, akkor átveszi annak szerepkörét, feladatait. Ez a gyakorlatban azt jelenti, hogy noha a megvalósítások logikailag is alapvetően eltérnek egymástól, a cég valójában nem érzékel működésbeli, illetve minőségi különbséget a kettő között.

Az Azure által nyújtott szolgáltatás független a vállalat on-premise infrastruktúrájának elavulásától, így, míg a hagyományos megoldás esetében a harmadik év végére már – az amortizáció miatt – egy, az életciklusa végéhez közeledő rendszert lesz kénytelen használni a vállalat, addig a felhő szolgáltatás esetében nem kell ilyen elavulással és korlátokkal számolnia.

Összehasonlítás költségek alapján

Kutatásom gerincét a megvalósítások pénzügyi összehasonlítása, elemzése adja, ennek oka, hogy a hagyományos DR rendszerek korlátját épp a magas költségek jelentik. A két megvalósítás 3 évre kalkulált tulajdonlás teljes költsége (TCO) az alábbiak szerint alakul:

19. ábra - megvalósítások költségei

Hagyományos, on-premise megoldás	Windows Azure felhő-megoldás
37 971 000.-	11 835 000.-

Amint a táblázatban is látható, hatalmas költség-különbség jelentkezik a két megvalósítás között, pedig az előző fejezetben – „Összehasonlítás képességek alapján” – leírtak alapján képességeik lényegében megegyeznek. Ez egyértelmű előny a felhő-megvalósítások számára, hisz nem csak azok a vállalatok térhetnek át cloud alapú DR site-ok használatára, akiknek ezelőtt is volt tőkéjük arra, hogy on-premise DR rendszert építsenek ki, hanem olyan vállalatok is alkalmazhatnak DR megoldásokat, akiknek ezen szolgáltatások bevezetése és használata azok magas költségei miatt eddig indokolatlanoknak lettek minősítve.

Más szavakkal megfogalmazva a felhő DR megoldások számára a KKV-k, induló vállalkozások, illetve középvállalkozások ún. „kék óceánnak”¹ tekinthetők, tehát egy olyan piacnak, ahol nincs a megoldásnak versenytársa a piacon.

Tehát a felhő-megoldások költséghatékonyabbak a vizsgált esetben, ugyanakkor ez az eset is jól érzékelteti a két alternatíva közötti pénzügyi strukturális különbségeket és ebből az ügyfelek számára elérhető árelőny lehetőségét.

Összehasonlítás rugalmasság alapján

A rugalmasság elvárásának biztosítása a felhő szolgáltatások sajátosságát és egyben kiemelt előnyét jelenti. Ezáltal az informatikai infrastruktúra megfelelően tud alkalmazkodni a gyorsan változó üzleti igényekhez. Konkrét esetünkben ez azt jelenti, hogy amennyiben az S&T igényei megváltoznak saját DR rendszere irányában, akkor az Azure szolgáltatáson alapuló infrastruktúrát gyorsan és egyszerűen, implementációs költségek nélkül lehet az új igényekre optimalizálni. Egy on-premise rendszer esetében azonban a hardverbe való beruházás kötöttséget, elkötelezettséget jelent.

A rugalmasságnak azonban pszichológiai ára van, a vállalat számára akár kellemetlen, ellenérzéseket válthat ki, hogy az általa használt erőforrások nem az ő fizikai, illetve jogi tulajdonában állnak, nem az ő kezében van az irányítás. Az ellenérzéseken túl ez komoly kihívást is jelent, mert egyrészt bizalmat feltételez a cég részéről a szolgáltató felé, másrészt egy esetleges meghibásodás esetén várakozáson kívül mást nem tehet az ügyfél.

¹ . A kék óceán fogalmát és jelentését a Kék óceán stratégia című könyvből értelmeztem.

Konklúzió: A cloud DR megoldás életképessége vállalati közegben

Ugyan egy nagyon speciális helyzetet láttunk, de ez az eset kiváló példa arra, hogy részletesen végiggondoljuk a cloud szolgáltatások üzleti használhatóságát, életképességét. Az eddigiekben elméletben és gyakorlatban is megvizsgáltam a hagyományos megvalósítást és a felhő-alapút is, majd objektív összehasonlításnak vetettem alá a kettőt, mely alapján most már egyértelmű következtetések vonhatók le.

A hagyományos DR megvalósítás az elemzett vállalat számára egyértelműen nem optimális, és nem is indokolt alternatíva, hisz az üzletileg kritikus szolgáltatások kiesése esetén a kockázati tényezővel súlyozott várható veszteség összesen kevesebb, mint 11 millió forint, míg a DR site teljes tulajdonlási költsége több mint 37 millió forint.

A felhő-alapú megvalósítás olcsóbb ugyan jóval, de még mindig nem mindenható, ezért a cloud-ról szóló döntések esetében is szükséges, hogy lássuk az üzleti elvárásokat és azokhoz mérjük a megoldás minőségét és pénzügyi következményeit. Ezeket tekintve pedig a felhő-alapú DR megoldás életképes alternatíva, hisz a teljes tulajdonlás költsége nagyjából 12 millió forint, ez az érték egymillió forinttal több, mint az üzletileg kritikus szolgáltatások kiesése esetén a vállalat pénzügyi vesztesége. A közvetett előnyök azonban a felhő-alapú megoldás felé billentik a mérleget, hisz olyan tulajdonságok, melyek egy vállalat vezetősége számára komoly értékkel bírhatnak. Ilyen közvetett előnyök az alábbiak:

- Rugalmasság, skálázhatóság
- Biztonság és redundancia
- Gyors alkalmazkodóképesség az üzleti igényekhez

Közvetett hátrányként mindenképpen szeretném megemlíteni a bizalom kérdését. A privát felhő használata kétségtelenül költséghatékony megoldás, de a vállalati, bizalmas adatok és szolgáltatások egy részének áthelyezése a számítási felhőbe egy bizalmi döntés is, melyet a vezetőségnek mérlegelnie kell a pénzügyi döntés meghozatala előtt.

Összességében a felhő-megoldások a vállalatok számára egy új lehetőséget jelentenek, melyek megnyithatják a lehetőséget DR site létrehozása felé olyan cégeknek, melyek eddig nem teheték meg ezt a magas költségek miatt. De hasonló megoldások lehetőséget biztosítanak a fejlesztői és tesztrendszerek kialakítása és egyéb, ad-hoc, illetve ideiglenes igények az IT felé, melyek hagyományos informatikai megoldások segítségével nem biztosíthatóak.

Forrásjegyzék

1. Ed Anderson, Chad Eschinger, Laurie F. Wurster, Federico De Silva, Ruggero Contu, Venecia K Liu, Fabrizio Biscotti, Gregor Petri, Jie Zhang, Morgan Yeates, Warren Bell, Jeffrey Roster, Susan Cournoyer, Tom Eid, Joanne M. Correia, Yanna Dharmasthira, Hai Hong Swinehart, TJ Singh, Cathy Tornbohm, Robert H. Brown, Dan Sommer, Chris Pang (2012) Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 2Q12 Update in: Gartner G00234817
2. BCPHB (2007) Business Continuity Preparadness Handbook, AT&T
3. Dominic Betts, Alex Homer, Alejandro Jezierski, Masashi Narumoto, Hanz Zhang (2012) Getting to the Cloud, in: Moving Applications to the Cloud on Microsoft Windows Azure, 3rd. edition, Microsoft, pp 15-45.
4. Jon Brodtkin (2012) Bandwidth explosion: As Internet use soars, can bottlenecks be averted? in: ArsTechnika, <http://arstechnica.com/business/2012/05/bandwidth-explosion-as-internet-use-soars-can-bottlenecks-be-averted/> (letöltés ideje: 2013 március 3.)
5. Brooks, C. – Bedernjak, M. – Juran, I. – Merryman, J. (2002) Chapter 2: The tiers of Disaster Recovery, in: Disaster Recovery Strategies with Tivoli Storage Management, Red Book Series, IBM, pp 21-36.
6. W. Chan Kim, Renée Mauborgne (2008) Kék óceán stratégia, a verseny nélküli piaci tér, Park kiadó, Budapest
7. CSDS (2013) Crypto Services and Data Security in Windows Azure in: <http://msdn.microsoft.com/en-us/magazine/ee291586.aspx> (letöltés ideje: 2013. január 22.)
8. Ashleigh Davis (2011) Decade of Storage: From USB to Cloud Storage (infographic) in: RackSpace Blog <http://www.rackspace.com/blog/decade-of-storage-from-usb-to-cloud/> (letöltés ideje: 2013. március 10.)
9. Farkas Bálint, Kovács Gábor, Király István, Turóczy Attila, König Tibor, Érsek Attila, Safranka Mátyás, Fülöp Dávid, Pellek Krisztián, Kiss Balázs (2013) Windows Azure lépésről lépésre, Jedlik Oktatási Stúdió, Budapest, 16-17. és 27. oldal.
10. Richard Hunter (2011) The CIO's View of Cloud Collaboration: Choose Candidates Wisely in: Gartner cloud collection

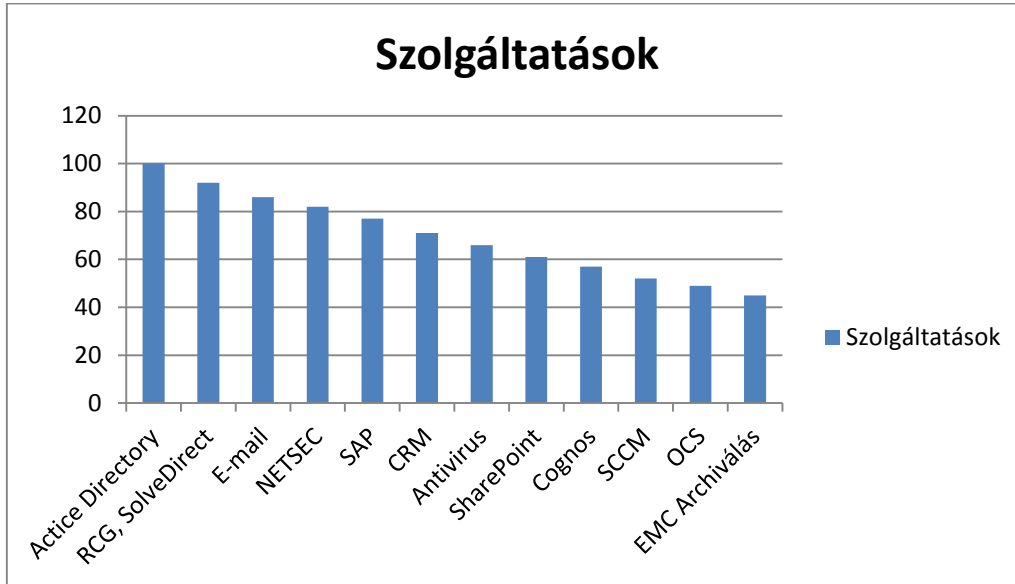
11. Charlie Kaufman, Ramanathan Venkatapathy (2010) Cloud Security Design, in: Windows Azure Security Overview, Microsoft
12. KFGT (2013) 1.8: Kiskereskedelmi forgalom, megjelent: A KSH jelenti: Gazdaság és társadalom, 2012. január–december, Központi Statisztikai Hivatal
13. LMWHP (2013) List of monitored web hosting providers by overall uptime descending in:
<http://uptime.besthostratings.com/webhosts-uptime.php?order=uptime&page=1&sort=desc>, Best Host Ratings (letöltés ideje: 2013 március 18.)
14. Andrew McAfee, Erik Brynjolfsson 2011 What Every CEO Needs to Know About the Cloud, in: Harvard Business Review
15. Mel Gosling (2008) The 80 percent myth, in: Continuity Central,
<http://www.continuitycentral.com/feature0440.htm> (letöltés ideje: 2013. március 18.)
16. Om Malik (2010) Stats on Cloud Computing in: Cloud Hypermarket
<http://gigaom.com/2010/12/07/infographic-cloud-computing-by-the-numbers/>
(letöltés ideje: 2013. március 6.)
17. Christy Pettey, Rob van der Meulen (2012) Hype Cycle for Cloud computing in: Hype Cycle for Emerging Technologies
18. Padmavathy Ramesh (2002) Elements Of Business Continuity Planning, in: Business Continuity Planning, Technology Review 2002/4, TATA Consultancy Services, pp: 5-15.
19. Schopp Attila (2007) Okosan félni, megjelent: ITBusiness, 2007 október 2, 17. oldal
20. Smulovics Péter (2011) Morgan Stanley Desktop, elhangzott: Adecco IT Academy
21. Szommer Károly, Balogh Zoltán (2012) L07: Cloud, elhangzott: 2012. október 15. , Budapesti Corvinus Egyetem
22. Vital Records: How Do You Protect And Store Vital Records? (2009) in: Records Management, University of Washington
<http://f2.washington.edu/fm/recmgt/managing/vitalrecords/store> (letöltés ideje: 2013. március 10.)
23. VNI (2013) Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017 in: Cisco Visual Networking Index

24. VPN (2013) About VPN Devices for Virtual Network, in:
<http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx> (letöltés ideje: 2013. március 2.)
25. Wigle (2013) Statistics on WiFi networks in: Active graph
<http://wgle.net/graph-large.html> (letöltés ideje: 2013. február 16.)
26. Winer R. S. (2001) Introduction in: Customer Relationship Management: A Framework, Research Directions, and the Future, Haas School of Business, University of California at Berkeley, pp 2.
27. WIU (2012) World Internet Usage And Population Statistics in: Internet World Stats, Miniwatts Marketing Group
<http://www.internetworldstats.com/stats.htm> (letöltés ideje: 2013. február 9)

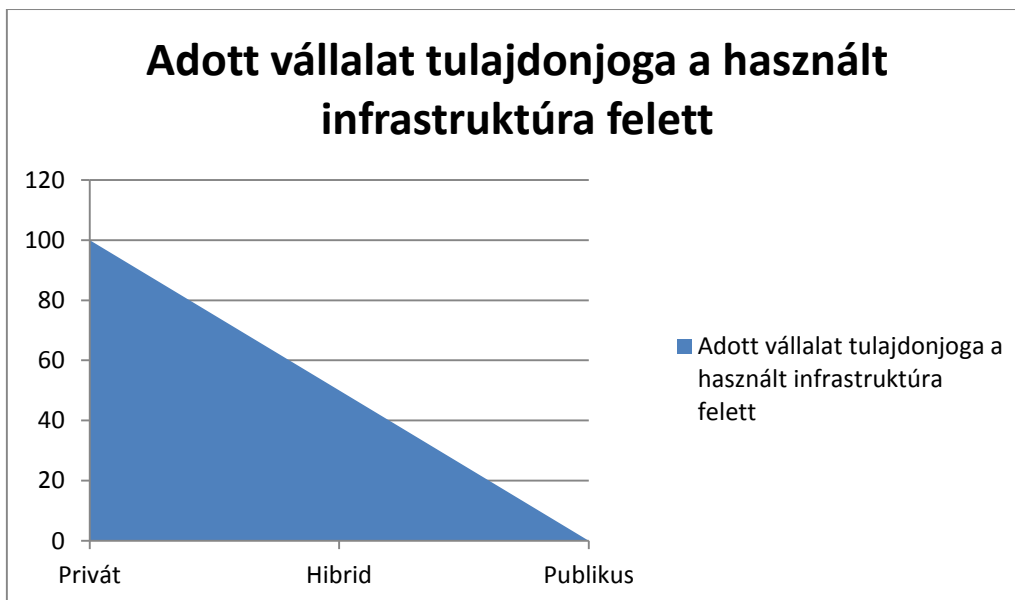
Mellékletek

Megjegyzés: Az összes mellékletet a szerző készítette az adatok közötti kapcsolatok, illetve gondolatmenete követésének megkönnyítése céljából!

1. sz. melléklet



2. sz. melléklet



3. sz. melléklet



4. sz. melléklet

