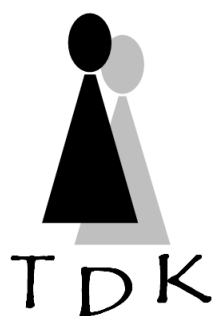


A Cloud szolgáltatás biztonsági kérdései

– avagy mit kínálnak a szolgáltatók és mit várnak a vállalatok?

Tudományos Diákköri Dolgozat

Konzulens: Dr. Fehér Péter



Balogh Turul
Gazdálkodástudományi kar
BSc
Gazdaságinformatika
II. Évfolyam

2014.03.24.

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.

Tartalom

1.	Bevezetés és a téma jelentősége	3
2.	Motiváció és a kérdésfelvetés	3
3.	A dolgozatom felépítése	4
4.	Történelmi felvezetés	6
5.	A Cloud bemutatása	7
5.1.	A Cloud alapvető jellemzői	8
5.2.	Szolgáltatási szintek - XaaS	9
5.3.	Telepítési szintek	11
5.4.	A Cloud terjedése	13
5.4.1.	Terjedésének okai	14
5.4.2.	Előnyök	15
5.4.3.	A technológia árnyoldala	15
5.5.	A világ jelenlegi állása	17
5.5.1.	Domino-elv	17
5.5.2.	A CIA háromszög	18
6.	Kockázatok	19
6.1.	Üzleti és jogi kockázatok	19
6.2.	Műszaki kockázatok	21
7.	A felhő szolgáltatás biztonsági kérdései a gyakorlatban	22
7.1.	Szállítói vállalatok és kínálat	22
7.1.1.	Google	22
7.1.2.	Amazon	23
7.1.3.	Microsoft Azure	25
7.2.	Vállalati interjúk	26
7.2.1.	A Deloitte CIO meglátásai	27
7.2.2.	S&T	32
7.2.3.	T-systems	36
8.	A kutatásom eredménye és összefoglalás	41
8.1.	Az interjúk összefoglalása	41
8.2.	Meglátásaim	42
9.	Zárszó	44
10.	Forrásjegyzék	45
11.	Ábrajegyzék	48
12.	Melléklet	49

1. Bevezetés és a téma jelentősége

2013 során rengeteget lehetett hallani a „Cloud” térnyeréséről és az ezzel kapcsolatos biztonsági kérdésekről az egyes szakmai fórumokon, újságokon, előadásokon és konferenciákon. Továbbá egyre több technikai eszköz rendelkezik internet kapcsolattal és ezzel párhuzamosan egyre kevesebb számítás történik helyben, az otthonainkban, irodáinkban.

Ennek eredményeként lassan már csak egy megjelenítő eszközre lesz szükségünk és a hagyományos értelemben vett IT infrastruktúra a felhasználók számára egy láthatatlan és érthetetlen mechanizmus lesz, mely a „Cloud” névre hallgat. Sokan nem tudják, hogy valójában mit jelent ez, mit takar a „kiteszem a felhőbe” kifejezés.

Azonban eltekintve a definíciós értelmezéstől, van ennek egy igen komoly vetülete. Mégpedig a biztonság.

Mi történik a felhőbe ki tett adatainkkal? Kik és hogyan kezelik ezeket? Mi történik a háttérben a felhasználók tudta nélkül? Miről nem tudunk? Milyen folyamatokat nem látunk?

2. Motiváció és a kérdésfelvetés

Engem személyesen mindig is a biztonság kérdése foglalkozott az élet számos területén. Legyen szó akár nyelvvizsga felkészítésről, érettségi előkészítőről, esettanulmány megoldásról, napi programok szervezéséről, én az indokoltnál mindig nagyobb hangsúlyt fektettem a pontosságra, megbízhatóságra, biztonságra. Ez utóbbit a lehetőségekhez mérten a legtöbb szempontból meg kívántam vizsgálni.

Amikor előző félévben először hallgattam „felhő” témáról szóló előadást, akkor azonnal a *bizalmasság*, *megbízhatóság*, *bizalom*, *kockázat*, *veszély*, *függőség* szavak jutottak eszembe, illetve az, hogy ez tulajdonképpen nem is olyan új dolog, csupán egy „hype”, egy divatos szó, mely alig különbözik az 1980-as években használt számítástechnikai módszertanoktól. Ezt követően kezdtem el vizsgálni!

Továbbá a Gartner 2013. október 31-ei cikkében felhívja a figyelmünket, hogy a vállalatok rengeteg pénzt fognak a felhő biztonsági részébe fektetni, és ez nem fog alább hagyni évek múltán sem, hiszen ha már okosotthonokról beszélünk, akkor ott elengedhetetlen a biztonság kérdése például.

Az egyes technológiai megoldások alapvetően megkönnyíthetik mindennapjainkat, de óvatosnak kell lennünk, hogy mit és hogyan teszünk.

A környezetemet vizsgálva, szaklapokat olvasva rájöttem, hogy a Clouddal kapcsolatban elég komoly ellenérzések vannak.

Ebben a dolgozatban azt kívánom megvizsgálni, hogy ezek az ellenérzések mennyire valósak és hogyan lehet ezeket kezelni. A kutatásomat mind elméleti mind gyakorlati szempontból kívánom kivitelezni!

3.A dolgozatom felépítése

A TDK dolgozatomat a következőképp építem fel:

Kezdetben egy szakirodalmi részben áttekintem, hogy a kedves olvasónak mit is érdemes tudnia a felhőről, milyen alapvető tulajdonságai vannak, milyen telepítési és szolgáltatásai szintekkel rendelkezik.

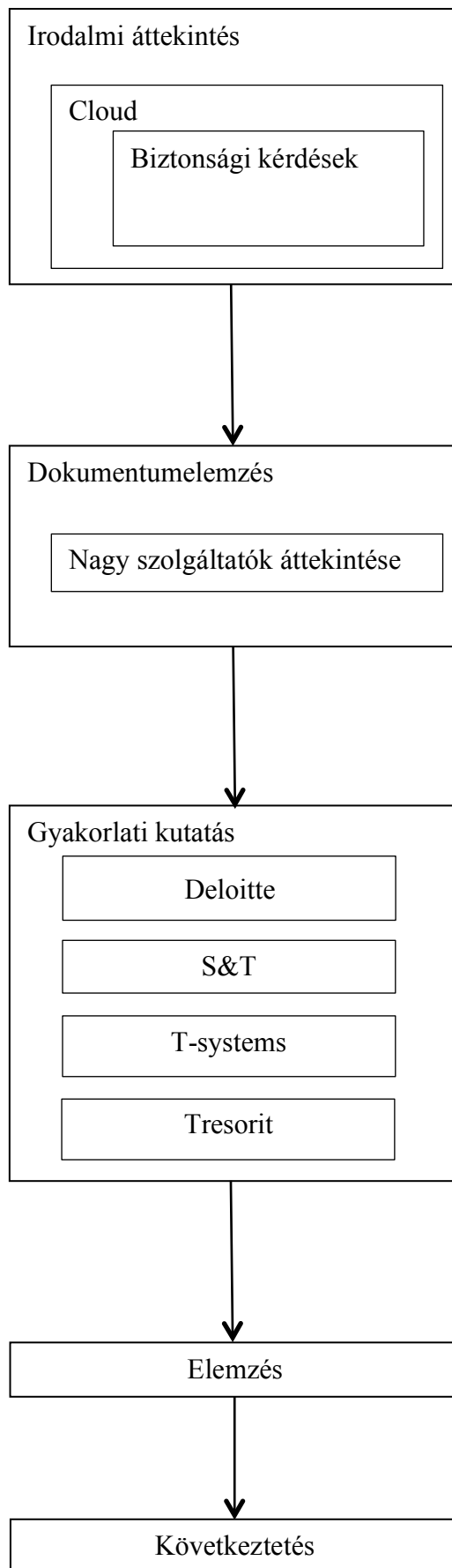
Ezt követően rátérek a dolgozat főbb kérdésére. Nevezetesen, hogy a felhőszolgáltatásnak milyen jogi, üzleti és műszaki kockázatai vannak. Az egésznek a fókuszában a szolgáltatói, szállítói vállalatok, megoldások állnak, melyeket az ügyfelek elvárásaival, hozzáállásával hasonlítok össze.

Mindamellet, hogy a vizsgálathoz jelenlegi felméréseket, kutatásokat használok fel, személyesen is megkérdezek vállalatvezetőket, akik napi szinten veszik igénybe és szolgáltatják is a felhőt, hogy nekik mi a meglátásuk, mit tapasztalnak biztonság terén.

Személyes interjút készítettem az S&T rendszerintegrátor cégcsoport szolgáltatásfejlesztési vezetőjével, továbbá a Deloitte közép-európai CIO-jával, valamint a T-systems cloud biztonságért felelős szakértőivel. Egytől egyig készségesen álltak rendelkezésemre, az elmúlt sok év tapasztalatát felhasználva fejtették ki véleményüket, meglátásaikat a Cloud biztonsága terén.

Ezúton is szeretnék köszönetet nyilvánítani konzulensemnek, Dr. Fehér Péternek, aki készségesen segített nekem a TDK-m megírása során!

A dolgozatom megírása során törekszem arra, hogy átfogó és mindenre kiterjedő részleteket közöljek, mely magát, a felhő szolgáltatást érinti az elemzésem kapcsán. Ezen megfontolásom miatt a munkám legelejétől a legvégéig a körülmények és a legmeghatározóbb tényezők figyelembe vételével szándékozom vizsgálgatni. Egységes és egész művet kívánok megalkotni.



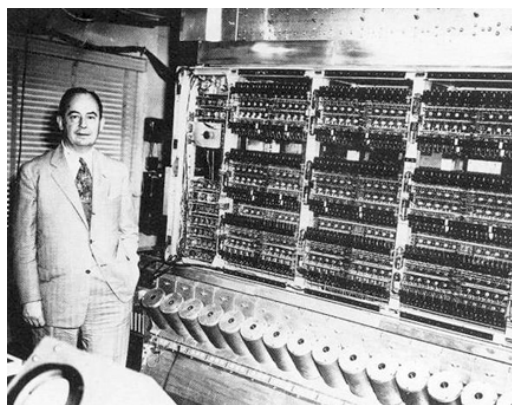
4. Történelmi felvezetés

Azért, hogy jobban megértsük ezt az új technológiai megoldást, vissza kell mennünk egészen a történelmi gyökerekig (mainframe, internet) és onnan nekifutni a felhő téma vizsgálatának. Ezáltal még teljesebb körben tudunk majd vizsgálni a későbbiekben!

A klasszikus, mai értelemben használt *számítógép* fogalma évszázadok alatt alakult ki, melyhez hozzájárultak olyan technikai fejlesztések, mint például: vákuumcső, tranzistor, nyomtatott áramkör, de röviden tekintsük át az erre vonatkozó történelmi részt:

Gondoljunk például a 0. generációs gépekre:

- Blaise Pascal – 1642 - mechanikus gépe
- Leibniz - 1700 - mechanikus gépe
- 1820-as évek - Charles Babbage differenciagépe
- 20. század - Konrad Zuse Z1 elnevezésű alkotása



1. ábra: Neumann János

Mindezek után pedig Neumann János lerakta az informatika alapjait, hiszen – többek között - a kettős számrendszer használata és az elektronikus működés alapján véve meghatározta az azóta eltelt időszakot. (Andrew S. Tanenbaum, 2006).

Az 1970-es években megjelentek a mainframe számítógépek, melyek fizikailag jóval nagyobbak voltak a jelenlegi gépeknél, és a háttérben hatalmas teljesítményükkel óriási mennyiségű adatok kezelésére és feldolgozására voltak képesek. Egy időben több ezer felhasználó igényeit is ki tudta szolgálni. Főleg nagyvállalatoknál, bankoknál, kormányzati szerveknél használták ezeket bérlet útján.

Később teljesítmény növelés céljából elkezdtek számítógépeket összekapcsolni, mely a Grid Computing megjelenését eredményezte. Az 1980-as évektől a magas integráltságnak (LSI) köszönhetően megjelentek a személyi számítógépek (PC), melyek mérete és számítási kapacitása egymással fordított arányban változtak. Ezt Moore 1965-ben már megjósolta.

A másik igen fontos összetevő az internet volt, melyet kezdetben katonai célokra használták fel, majd a lakosság számára is elérhetővé tették az 1990-es években.

Ezek jelentősége abban rejlik, hogy ezek a Cloud két igen fontos kulcs összetevője. Vizsgáljuk meg, hogy pontosan mi is ez!

5.A Cloud bemutatása

„...then computing may someday be organized as a public utility...” – mondta John McCarthy 1961-ben az MIT-n tartott előadásban, vagyis meglátása szerint egy nap a számítási kapacitást is közműként fogják árulni.

Most, több mint fél évszázaddal kijelentése után, igazolódni látszódik ez, de ahhoz, hogy ezt megértsük, vegyünk a következő analógiát: (Bögel, 2009).

Kezdetben az emberek kutakból merték a vizet, derítőt használtak csatornázáshoz, kandallóval melegítették otthonukat, de később megjelent a vízszolgáltatás, a csatornázás, a távhőszolgáltatás és a vezetékes gáz. Végül színre léptek az internetszolgáltatók (ISP). Azonban hogyan is illeszkedik ez a témámhoz?

Úgy, hogy az egyedi felhasználások után felmerült a tömeges fogyasztói igény – a fentebb említettekre -, az állam és a vállalatok rájöttek, hogy sokkal gazdaságosabban lehet ezeket működtetni, ha közműként nyújtják. Ebből következik, hogy maga a számítási kapacitás is ilyenné kezd válni, tehát indokolt lehet a közművesítése. Így megszületett a Cloud Computing fogalma.

Ezt magyarul felhőinformatikának fordítjuk. Lényegében ez egy kiszervezési fajta, mely – meglátásom szerint - nem egy új keletű találmány, hiszen a szakirodalom az „outsourcing” kifejezést már az 1990-es években is használta, amikor is a vállalatok költségmegtakarítás címszó alatt elkezdtek külső szolgáltatókkal végeztetni az egyes, nem a vállalati főtevékenységhez kapcsolódó feladatokat. Tehát dióhéjban: nem maga az adott vállalat, intézmény kezeli az például informatikai szolgáltatást, hanem másnak fizet ezért. (Chikán, 2008).

Erre később még utalok a majd a Deloitte közép-európai CIO-jával készített interjúban! Elöljáróban annyit, hogy például az Infrastructure as a Service szinte alig különbözik attól, mint amikor mi a saját szervereinket kirakjuk egy külső gépterembe, de mégis Iaas-nak hívjuk és a „Cloud” jelzővel illetjük...

Definíció szerint a felhő a következő: „*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*” (NIST, 2011).

A lényege, hogy igényeinknek megfelelően kapunk hozzáférést olyan erőforrásokhoz, mint például tárhely, szerver, hálózat. Ezek távol vannak tőlünk – akár másik kontinensen is - és szinte automatikusan, a megrendelő és a megbízó között interakció nélkül zajlik le a „vásárlás” folyamata. 5 fontos jellemzője van, 3 szolgáltatási és 4 telepítési modellel rendelkezik.

Vizsgáljuk meg ezeket részletesebben is!

5.1. A Cloud alapvető jellemzői

A következőkben vizsgáljuk meg néhány alapvető tulajdonságát, melyek egyértelműen jellemzik ezt a szolgáltatás fajtát! (NIST, 2011).

A felhőinformatika egyik alapvető jellemzője a szélessávú hálózaton keresztüli hozzáférés, vagyis kizárólag internet segítségével lehet használni ezt a szolgáltatást. Ehhez kliens-szerver architektúra szükséges, mely szerepet a mai világban már egyre inkább a SmartPhone és a laptop tölti be. Láthatjuk, hogy ezek főleg azért fontosak, mert a mai világban a mobilitásra való igény egyre jobban terjed. Ez alatt azt értem: függetlenül attól, hogy hol vagyunk, mit akarunk intézni, már szinte bármi lehetséges. (Cisco, 2012).

A Cloud másik alapvető jellemzője az igény szerinti önkiszolgálás. Ennek lényege, hogy maga a fogyasztó dönt a számítási kapacitás igénybevételéről, a szolgáltatótól szinte teljesen függetlenül, automatikusan, interakció nélkül történik az igénylés, mely például lehet a hálózati tárolás vagy a szerver idő.

Ezek mellett tulajdonsága még az erőforrás felhalmozás. Tehát, hatalmas mennyiségű erőforrásokat gyűjtenek össze fizikailag és virtuálisan is, melyekkel ki tudnak szolgálni azonos időben rengeteg ügyféligényt. Ilyen felhalmozott erőforrás lehet például a memória, a sávszélesség vagy a tárhely.

Ez előbbi fogalomhoz tartozik az elaszticitás: ezen erőforrásoknak skálázhatónak, vagyis gyorsan bővíthetőnek és nagyon rugalmasnak kell lenniük, hiszen az aktuális fogyasztói igénybevételhez kell alkalmazkodni. A fogyasztók szinte bárhol, bármikor, bármennyit igényelhetnek ezekből. Számukra ez végtelennek tűnik a dinamikus működés miatt.

Maga a szolgáltatás mérhető. A rendszerek folyamatosan ellenőrzik és szabályozzák optimalizáció céljából a Cloud működését. Ehhez szükséges egy úgy nevezett absztrakciós szint, példának okáért ilyen a felhasználói fiókok aktív száma, melyekkel már lehet pontosan számolni és tervezni az erőforrásokkal. (Sipos, 2013).

Továbbá magától értetődő, hogy ez alapján véve egy távoli hozzáférés, hiszen nem helyben kapom a szolgáltatást, hanem interneten keresztül veszem igénybe, de ez - számunkra – felhasználóknak nem tűnik fel, sőt mi több, ugyanolyannak látjuk az egészet kívülről, nem tudhatjuk elsőre, hogy pontosan mi zajlik a „színfalak mögött”.

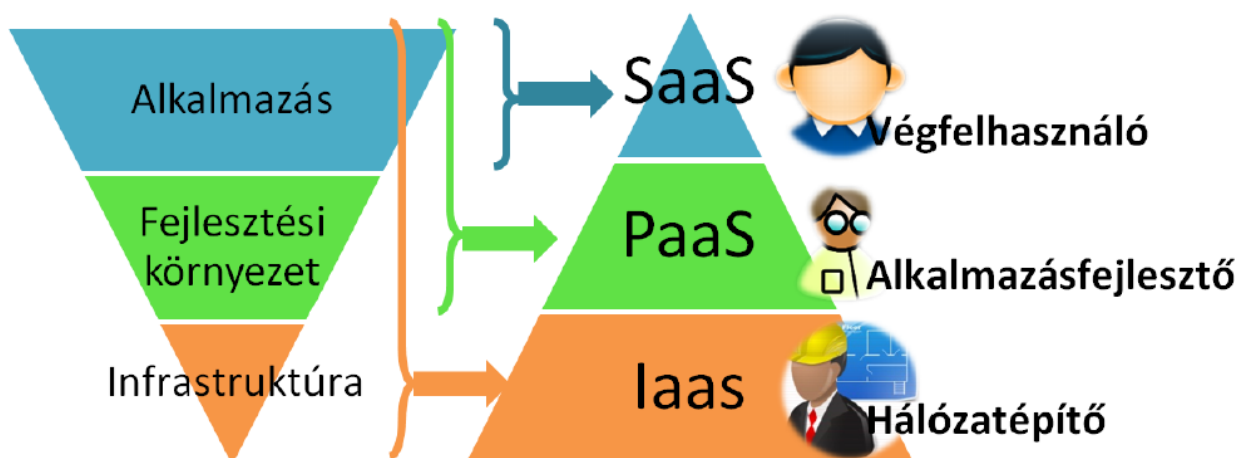
Ezek után nézzük meg, hogy a Cloud szolgáltatásnak milyen fajtái vannak!

5.2. Szolgáltatási szintek - XaaS

A felhő szolgáltatásnak számos fajtáját lehet megkülönböztetni az alapján, hogy mi maga a szolgáltatás tárgya, az alábbiakban néhány példa. Tetszőleges fogalmat lehet az „X” helyére tenni ezáltal (Racsó, 2012).

- Database as a Service
- Application as a Service
- Security as a Service
- Testing as a Service
- Information as a Service
- Integration as a Service
- Storage as a Service
- Process as a Service
- Management as a Service

A fentebb említettek közül három alapvető szolgáltatás részletesebben is kifejték. IaaS, PaaS, SaaS.



2. ábra: A szolgáltatási szintek hierarchiája

Kezdjük a legalsó szinttel!

Ez az Infrastructure as a Service (IaaS), vagyis magát az infrastruktúrát, a hardvert béreljük. Ekkor a bérelt virtuális számítógépünkön lehetőségünk nyílik szabadon választott alkalmazásokat és operációs rendszereket futtatni, melyhez a Cloud szolgáltató biztosítja magát a teljes hálózatot, a tárolást, a kiszolgálást és a virtualizációt is. Tehát nekünk csak használatarányosan kell fizetnünk az igénybevett erőforrásokért.

Példának okáért az Amazon által nyújtott Amazon Elastic Computing Cloud szolgáltatás keretein belül 2014.január 24-ei árazása szerint egy Windowsos virtuális gép 2 processzorral 7,5 GB memóriával, 32 GB SSD-vel óránként 0,225 dollárba kerül, ami nagyjából 50 Ft. Későbbiekben visszautalok még erre.

A következő szint ebben a „hierarchiában” a Platform as a Service (PaaS), amikor is maga a szolgáltató biztosítja a teljes mögöttes platformot, vagyis az operációs rendszert, a teljes hálózatot, a tárolást, a kiszolgálást és a virtualizációt is. Tehát nekünk elég csak az alkalmazást kifejleszteni és feltelepíteni a felhőbe. Ilyen bérelhető fejlesztési környezetet kínál a Microsoft Azure terméke, ahol például .NET nyelven megírt programokat lehet futtatni vagy éppen a versenytárs, a Google App Engine is hasonló szolgáltatást ajánl számunkra.

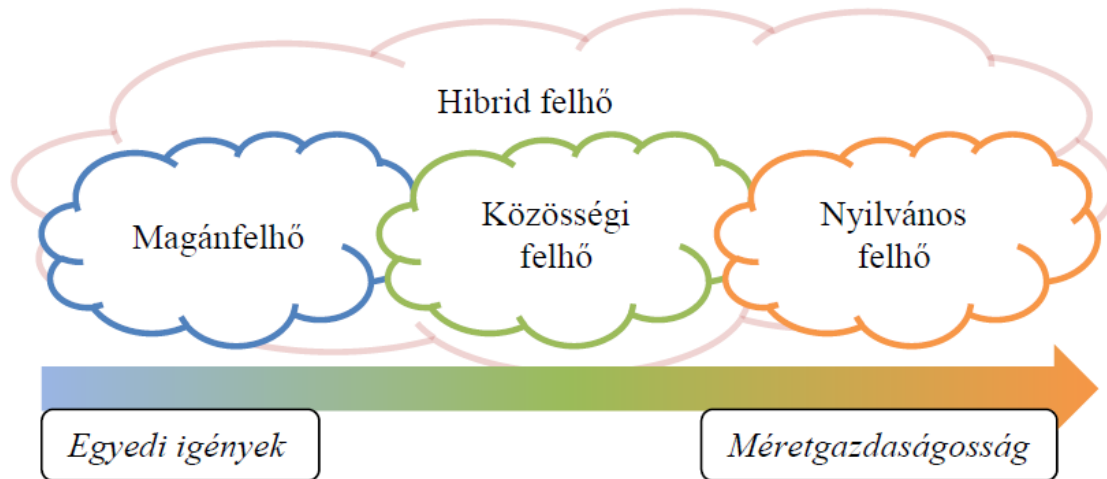
A piramis tetején a Software as a Service áll (SaaS), vagy más megközelítésben az Application Service Provider (ASP). Ekkor a szolgáltató kezel mindent: alkalmazást, adatokat, futtatókörnyezetet, köztes szoftvert, operációs rendszert, teljes hálózatot, a tárolást, a kiszolgálást és a virtualizációt. Nekünk, felhasználóknak csupán internetelérésre, böngészőre és egy alkalmas eszközre van szükségünk. Nem tudjuk befolyásolni a szoftver egyes funkcióit és nem érzékelünk semmit a platform vagy infrastruktúra jellemzőiből.

Gyakorlatilag ez egy vékonykliens architektúra, hiszen például az okostelefonunk szinte csak is kizárólag a grafikai megjelenítésért felel, minden mögöttes adatkezelés, számítás a szerver feladata. Annak ellenére, hogy sokan nap mint nap használjuk a Gmail-t, DropBoxot vagy éppen a Google Docs egyes funkcióit – meglátásom szerint – nem is nagyon vagyunk tisztában azzal, hogy ez éppen egy a felhőbe kihelyezett szoftver (SaaS).

Mindezek tudatában vizsgáljuk meg, hogy milyen elérhetőségeket biztosítanak a felhőbe kiszervezett egyes funkciók és szolgáltatások!

5.3. Telepítési szintek

A National Institute of Standards and Technology megkülönböztet privát, nyilvános, közösségi és hibrid felhőket. Egyesével bemutatom ezeket:



3. ábra: A telepítési szintek formái

A magánfelhő lényege, hogy ehhez csak is kizárólag egy vállalat férhet hozzá, senki más nem, éppen ellenkezőleg, ahogyan majd láthatjuk a nyilvános felhő esetében. Teljes mértékben a vállalat stratégiájához illeszthető, egyedileg konfigurálható. Ezt működtetheti az adott vállalat informatikai részlege, tehát belsős szakemberek, de lehetőség van külső, felhő szolgáltatónak kiszervezni ezt (Cisco, IBM, Dell, Microsoft, Amazon). Vállalatok körében jelenleg is vitatott ennek használta, hiszen biztonsági és bizalmatlansági kérdések merülnek fel ezzel kapcsolatban, melyre később ki is térek, és mélyebben is elemzek.

A közösségi felhőt több szervezet egymással megosztva használja, mert céljaik, a biztonsági követelmények vagy éppen a hatósági előírások ezt indokoltnak tartják. Működtetheti bármelyik belsős vállalat, de felhőszolgáltatónak is ki lehet szervezni ezt.

Az imént említettekkel ellentétben a nyilvános felhő bárki számára elérhető, a NIST definíciója szerint működtetheti a kormány valamely szerve, akadémiai szervezet vagy vállalat is, de ezek kombinációja is megjelenhet. Itt vegyük észre, ahogyan az ábra is mutatja, hogy a méretgazdaságossági kérdés előjön, hiszen tömeggyártáshoz hasonlóan a fajlagos költsége itt a legalacsonyabb.

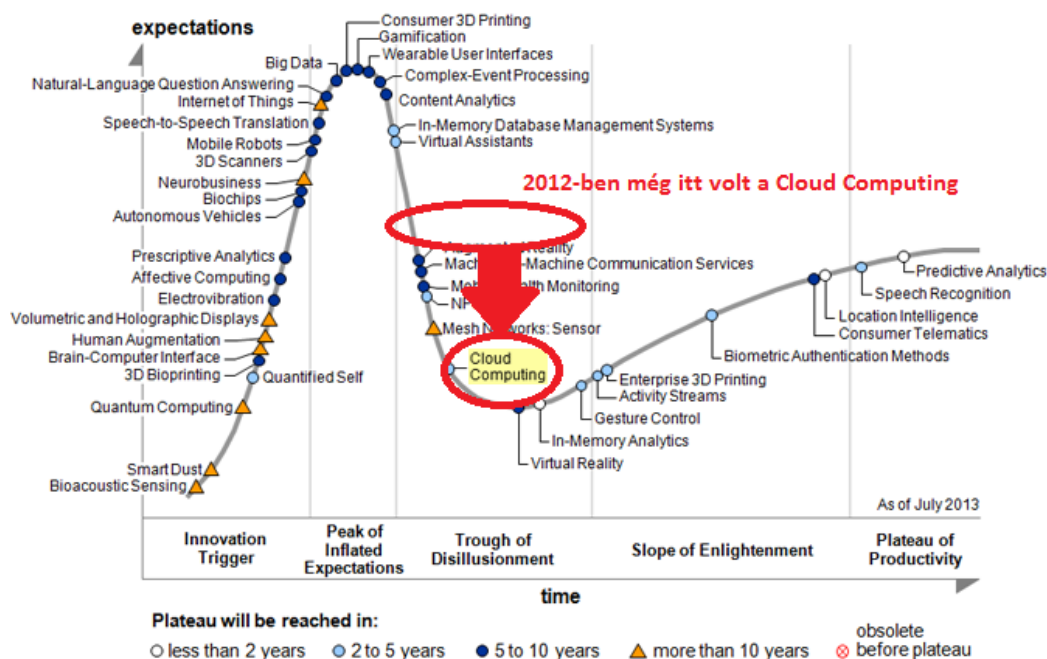
Végül pedig vizsgáljuk meg a hibrid felhő mibenlétét! Az előbb említett telepítési modellek közül bármely kettő ötvözéséből létrejöhet. Egy lehetséges megoldás, hogyha az adatokat például privátfelhőbe mentjük, hiszen így ezek viszonylag biztonságban vannak, míg

kevésbé fontos, nyilvánosságra hozható információk a nyilvános részben vannak. (Sípos, 2013).

Az eddigi elméleti és szakirodalmi éttekintő után nézzük meg, hogy miért is kezd egyre népszerűbbé válni a felhőinformatika!

5.4. A Cloud terjedése

A Gartner, mely egy 1979-ben alapított, connecticuti központú IT kutató és tanácsadó cég, évente elkészíti a Hype görbét, mely bemutatja, hogy az egyes technológiák milyen szakaszukban vannak (felfutó, kiábrándulás, érettség). Alább a 2013-as ábra látható.



4. ábra: A hype görbe

A fenti ábrán láthatjuk, hogy a Cloud megoldás a kezdeti fellángolás és kiábrándulás után szépen-lassan beáll egy állandó, stabil szintre és a termék az életciklus görbéjében pedig az érettség szakaszába lép majd.

2013.09.27-én a Gyulán tartott 51. Közgazdász Vándorgyűlésen részt vettem személyesen, ahol – többek között - Székely Zoltán tartott előadást a felhő témáról a KPMG 2012-es felmérése alapján, mely megállapítja a következőket:

Magáról a technológiáról nagyrészt az informatikai és műszaki igazgatók döntenek, akik szerint az e-mail mellett az értékesítés, a marketing, az irodai alkalmazások, ügyfélkezelés, valamint a HR is a felhőbe költözhethetne már most is, de 2 éven belül még ezen sorba be fog áll a tartalom menedzsment, üzleti intelligencia, a működés és a gyártás is.

A megkérdezettek 32%-a szerint a felhő megváltoztatja az üzleti modellüket és nagyobb átláthatóságot biztosít a menedzsment számára, 39%-uk szerint a vevőikkel és a szállítóikkal is megváltoztatja az interakciójukat, a válaszadók fele (!) számít jelentős költségcsökkentésre - a költségcsökkentő hatást szükséges minimumnak tekintik az IT

vezetők - és csupán 12%-uk vélte úgy, hogy nem lesz ennek jelentősebb hatása. Tehát, ha mást nem is, de a költségek csökkentését alapvető, kötelező hozadéknak tekinti.

Vizsgáljuk meg, hogy miért is volt ez eddig ennyire felkapott és milyen előnyökkel kecsegtetett a felhő! A következő részben nagyban támaszkodom a *Cisco Global Cloud Index: Forecast and Methodology, 2012–2017* nevű felmérésre.

5.4.1. Terjedésének okai

5.4.1.1. A környezet

Ahhoz, hogy ezt megértsük, előbb meg kell értenünk azt a környezetet, amiben a felhő iránti igény létrejött és azóta is működik. Először az internethez való kapcsolatát, aztán pedig az előnyöket vizsgálva véleményezem a technológia terjedését!

Ahogy a történelmi felvezetőben is utaltam már rá, az internet térhódítása óriási mértékben hozzájárult ezen technológia fejlődéséhez, hiszen jelenleg a 21. században a világ 40%-a használja az internetet, hazánkban ez a szám több mint 70%. (Google, 2014). A Cisco felmérésében 30-80% közötti növekedést vár 2017-ig a mobilinternet felhasználások terén. E mellé párosul, hogy a sávszélesség dinamikusan nő. Hazánkban 10-20 megabites internete bárkinek lehet, Londonban már 1,4 terrabit (!) sebességet értek el szakemberek (Computerworld, 2014).

Ez főleg a mobil eszközök, mint vékonykliens architektúra terjedésében segít, hiszen a vezeték nélküli hálózatok lefedettsége és minősége is javul. Az International Telecommunication Union 2013-as felmérése szerint a világban 100 emberenként 46-nak volt mobilinternet előfizetése, míg 2012-ben csak 36-nak. (Cisco, 2012) Ráadásul a jelenlegi 3G, HSDPA technológiák mellett a LTE térnyerését is szorgalmazza 2015-től az EU. (Paul Rasmussen, 2012). Továbbá roham léptékben csökkennek az adattárolási költségek és egyre inkább mobilabbak vagyunk, földrajzi helytől függetlenül már szinte bármit el kívánunk intézni. (Cisco, 2012).

Azonban a Cloud milyen előnyöket rejt magában egy ilyen dinamikusan változó környezetben?

5.4.2. Előnyök

A továbbiakban felsorolom a felhő néhány előnyét, melyek nagyban hozzájárulnak az üzleti sikerességéhez és felhasználásához. (Balogh, 2013):

- Kisebb helyi IT szakember csapat kell a vállalathoz
- Költséghatékonyabb működés a kapacitás optimalizálása miatt, hiszen csak azért fizetek, amit használok
- Igény szerinti kapacitást kell csak kifizetni
- Gyorsabb és egyszerűbb kiépítés, mint a „hagyományos rendszereknél”
- Nincs hardware üzemeltetési költség (humán, hardware, infrastruktúra)
- Egyszeri, nagy összegű beruházás helyett folyamatos költség
- Az alkalmazások bárholnan elérhetőek
- Azonnali verzióterítés
- Az alkalmazások terjesztésének költsége elhanyagolható
- Végtelennek tűnő kapacitás a fogyasztó számára
- Szabványos rendszercsatolók használata, mely egyfajta átjárhatóságot biztosít

Ilyen környezetben, ilyen előnyök járultak hozzá – többek között – a Cloud terjedéséhez, de ami igazán fontos, melyek miatt is foglalkozom a témával, és ami a TDK dolgozatom főbb tárgya, az a hátránya, pontosabban a biztonsági kérdések. A következőkben rátérek ezen legfőbb kérdés vizsgálatára.

5.4.3. A technológia árnyoldala

A tanulmányom eddigi részében általánosan áttekintettem a felhő szakirodalmi hátterét és előnyeit is, de valójában mi ennek a technológiának az igazi árnyoldala?

Személyesen én sokszor tapasztaltam magamon, ha például megszakad az internetkapcsolatom a szolgáltató hibájából, akkor olyan érzésem támad, mintha teljesen elváltak volna a külvilágtól. Ilyen esetben televízió és telefon sincs nálunk. Tudjuk, hogy ma már e-mail cím nélkül létezni teljességgel lehetetlen. Vetítsük ki ezt egy vállalatra... Igen, döbbenetes, leállhat a működés, bevételkiesés, pánik, információhiány...

A másik, ami a legfontosabb az a biztonsági kérdések. Nem tudjuk pontosan, hogy a személyes adataink hol vannak, kinél vannak, ki mit csinál ezekkel, ki mit lát, ki hogyan fog ezzel visszaélni és még számos ilyen kérdés merül fel bennünk.

Egy 2012-es KPMG felmérés szerint a következő kihívásokkal kell majd szembenézni a vállalatoknak az elkövetkezendő években, ha a felhőt kívánják használni:

- makrogazdasági szinten:
 - az egyes országokban eltérőek az adatvédelmi előírások
 - egyelőre hiányoznak alapvető szabályozások és módszertanok – meglátásom szerint ez annak tudható be, hogy a felhő a termékélet ciklus görbéjén még csak halad az érettségi szakasza felé, ennek következtében nem létezik még kiforrott megoldás és megfelelő szakértelem erre a technológiára
- általános kihívások:
 - biztonság, adatvédelem
 - erős függőség a Cloud szolgáltatótól (!)
 - megbízhatóság, rendelkezésre állás
 - implementációs és változáskezelési kérdések
 - testreszabhatóság csak mérsékelten
 - kulturális ellenállás
 - szabályozói környezet és változásai
 - adózási kérdések
 - „lock-in” - exit - kilépési feltételek, avagy hogyan lehetne egy Cloud szolgáltatót ott hagyni, hogy az adatainkkal ne éljenek vissza?!
 - erősebb IT költség-menedzsment

A megkérdezettek 33%-a szerint túl magasak az integrációs és implementációs költségek, valamint - leszámítva a költségeket - 31%-uk úgy véli, hogy problémás lenne a bevezetés folyamata.

A fentebb említett korlátok gátló és késleltető tényezőként mutatkoznak meg egyelőre – később interjúk keretében utánajárok, hogy vállalatvezetők 2014 tavaszán, hogyan vélekednek erről a kérdésekről!

5.5. A világ jelenlegi állása

5.5.1. Domino-elv

Az elmúlt időben történt sorozatos adatbiztonsági botrányok bizonyára mindnyájunkat megráztak. Mi is történt?

Edward Snowden, amerikai születésű informatikus, IT szakember. Egészen 2013 nyaráig az amerikai Központi Hírszerző Ügynökségnek (CIA) és a Nemzetbiztonsági Ügynökségnek (NSA) dolgozott. A világ – kivétel nélkül – össze



5. ábra: Edward Snowden

sajtóorgánuma azóta foglalkozik ügyével, mely az egész világot megbotránkoztatta. jelenleg Oroszországban bujkál. Nyilvánosságra hozott olyan szigorúan titkosított dokumentumokat, melyek bizonyítják, hogy Amerika az alapvető emberi jogokat sérti azzal, hogy figyeli és elemzi a világ állampolgárainak internetes tevékenységét, mobiltelefon aktivitásokat. Érintett között van a Facebook, Yahoo, Gmail, akik kérésre bárkinek kiadták személyes levelezéseit, adatait az amerikai hatóságoknak. Nemrégiben derült ki, hogy még az EU egyes intézményi üléseit is lehallgatták, és ez még csak a jéghegy csúcs... Snowden egy láncreakciót indított be, ki tudja mi lesz ennek a vége? (New York Times, The Guardian, The Washington post, Der Spiegel, CNN, 2013-2014).

A kedves olvasóval csak ezen rövid, időszerű példával szerettem volna érzékelteni az adatbiztonság jelentőségét, és hogy én miért foglalkozom ezzel a témával.

Ilyen körülmények között a vállalatok vezetői és magánszemélyek hogyan is mernék külső szolgáltatóknak adni kezelésre legféltebb adatait?

5.5.2. A CIA háromszög

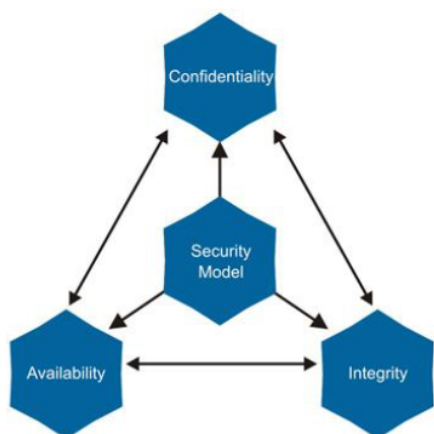
A Genfben található nemzetközi szabványokért felelős ISO szervezet, ISO/IEC 27000:2009 kiadásában határozzák meg az IT biztonság axiómáit, melyek a következők:

Confidentiality (Bizalmasság): Csak is kizárólag azon rendszerek és személyek férjenek hozzá adatainkhoz, akik megfelelő felhatalmazással rendelkeznek. Meglátásom szerint, felhő használata esetén ez a feltétel sérülhet, hiszen gondoljunk bele, hogy egy tárhelyre feltöltött fájl sokkal több ember számára válik elérhetővé, mely veszélyforrás lehet! Amíg a saját

számítógépünkön vagy pendrive-on van az adott fájl egy példányban, addig nem akkora kockázat.

Integrity (Sértetlenség): A szóban forgó modell ezen feltétele biztosítana minket, – elvileg - hogy az adataink pontosságát és teljességét megőrzi.

Availability (Rendelkezésre állás): A rendelkezésre állás azt jelenti, hogy a szolgáltatás és a kért információ a megfelelő jogosultság birtokában bármikor elérhető, valamint használható.



6. ábra: Az információ bizalmasság alapja, a CIA háromszög

6. Kockázatok

Ebben a részben megvizsgálom, hogy a felhőszolgáltatásnak milyen üzleti, jogi és műszaki kockázati merülhetnek fel működés közben, melyeket később összehasonlítok a vállalati SLA-kal és személyesen is véleményeztettem Cloud felhasználókkal.

Először is mi, felhasználók - később esetleg szolgáltatók – emberek vagyunk, néha elfáradunk, érzelmeink vannak, figyelmetlenek vagyunk, hibázunk... Miért is fontos ez? Azért, mert az emberi tényezővel mindig számolnunk kell, hiszen végső soron sok minden nálunk dől el!

A Social Engineering meglepte aggodalomra ad okot, hiszen – gondoljuk csak végig – sok alkalmazottnak, vezetőnek van hozzáférése üzleti információkat tartalmazó adatokhoz. A mai világban rengeteg megvesztegetésről, csalásról, árulásról hallhatunk, mely minket is elérhet, ha nem vagyunk elég körültekintőek! Ezen emberektől ellophatják, elveszítjük a belépési kódokat, megtudhatják – akár zsarolás útján is – a vállalatunk legféltettebb titkait stb...

Szerintem a felhasználói tudatosságot és az emberek hozzáállást proaktívan kell kezelni. Minden fronton meg kell előzni a problémát!

6.1. Üzleti és jogi kockázatok

Számomra a legkétségesebb tényező az a „lock-in” nevezetű jelenség, vagyis, amikor egyszerűen a szolgáltatótól függünk, és nem igazán tudunk elszakadni tőle veszteség nélkül. Ha például más Cloud szolgáltatóhoz szeretnék átmenni, akkor hogyan tudom csak úgy otthagyni a korábbi? Nála van rengeteg értékes adatom. Hogyan bizonyosodom meg, hogy valóban „büntetlenül” elenged? Erre a kérdésre még nincs pontos szabályzás, de a későbbiekben kutatásom során megkérdezem az érintett személyeket, hogyan vélekednek erről és ezt ők hogyan tudnák kivitelezni.

Egyébként a Cloud szolgáltató piac éretlensége miatt nem is igazán tudunk annyira más megoldásra áttérni. (Racsó, 2012)

Továbbá én, mint vállalatvezető és egyben megbízó is úgy érezném, hogy részben elveszítem az irányítást, hiszen a szolgáltatóra bízom adataimat. Ekkor nyújthat segítséget nekünk a Service Level Agreement – Szolgáltatási szint szerződés (SLA) eszköze, melyben pontosan meghatározzuk a kapott szolgáltatás egyes paraméterei vonatkozó elvárásainkat.

Ezek mellett a feladatokat, folyamatokat és a felelősséget is kikötjük (IBM, 2004). Továbbá azt is ki kell kötnünk az egyes kéréseink, problémáinkra milyen gyorsan és milyen minőségben reagálnak, valamint ha ez még sem történik meg, akkor mi lesz ennek a következménye!

Mindezek mellett a rossz szomszédság is veszélyforrás lehet, mely megítélésem szerint részben műszaki kockázat is egyben – erre utalok a következő részben. Szerintem ez magától értetődő, hiszen gondoljunk bele, egy ilyen virtualizált környezetben előfordulhat, hogy a mi legféltebb üzleti adataink ugyanazon a tárhelyen vannak, mint vállalatunk versenytársaié. Továbbá mi történik akkor, ha ezen a „közös” helyen a szomszédunk illegális tartalmakat tárol? Jön a rendőrség és lefoglalja a tárhelyet, ekkor mi a teendő? Mi lesz az adataimmal...?

Végezetül, mi történik akkor, ha éppen ezt a Cloud szolgáltatót vásárolja fel éppen a mi versenytársunk? Elmondhatatlanul nagy veszteség érheti cégünket ez esetben. (Balogh, 2013).

Befejezésül pedig röviden tekintsük át, hogy a Felhőnek kimondottan milyen jogi vetülete van.

Kezdjük egy kiindulóponttal: A 95/46/EC Európai Unió irányelv a személyazonosságunkkal kapcsolatos adatokról rendelkezik. E szerint minden olyan információ személyes adatnak minősül, mely egyértelműen azonosítani képes az érintett személyt. (Dr. Tátrai, 2013).

A 2012-ben elfogadott új törvény még határozottabban fellép személyes adataink védelme érdekében, de ennek csak az elkövetkezendő években lesz gyakorlati megjelenése, főleg a 2014-es EU-s választások közeledtével. (Rogers, 2013).

Cloud esetén figyelmesnek kell lenni, hiszen az egyes országok, régiók eltérően rendelkeznek adatvédelem kapcsán. Emiatt tanácsolom mindenkinek, hogy olyan szolgáltatóval szerződjön, akinek az adatközpontja az EU határain belül van, mert így - véleményem szerint - nagyobb biztonságban lehetnek adataink az európai, kicsit szigorúbb szabályozása miatt. (Patrick Van Eecke, 2014).

Összességében elmondhatom, hogy a felhő „éretlenségéből” kifolyólag rengeteg a kérdés, de proaktívan, alapos tervezéssel és rengeteg utánajárással sok bonyodalomtól kímélhetjük meg vállalatunkat és magunkat is! Néhány példával szemléltettem, hogy mi lehet kritikus, de mindenkinek a saját helyzetét megítélve kell a legjobb döntést hozni!

6.2. Műszaki kockázatok

Hogyan biztosítom azt, hogy egy adott üzleti információkat tartalmazó dokumentum egészen a létrejöttétől kezdve az interneten keresztüli feltöltésen át egészen a Cloud tárhelyig biztonságban legyen? Amerikai filmekben sokat lehetett látni, hogy pont ilyenkor az átvitelkor kapják el a kritikus adatokat (Balogh, 2013).

Megjelenhet még az adatszivárgás is: *„Ez a jelenség az adatok fel- és letöltésénél léphet fel, ha az autentikációs, autorizációs és ellenőrzési rendszerek nem megfelelőek, vagy a cloudon belül nem elég erős a védelem, esetleg hibás az alkalmazás vagy a menedzsment. Az adatszivárgás során a megrendelő adatainak egy része illetéktelen felhasználókhöz kerül.”* (Racsó, 2012).

Mi, egyetemisták gyakran találkozhatunk tárgyfelvételkor és vizsgajelentkezéskor a NEPTUN rendszerben a DDOS (Distributed Denial of Service) esettel. Tudniillik, hogy mindenféle rosszindulat nélkül, akaratlanul „támadást indítunk” a szerverek ellen, hiszen egy időben rengeteg utasítást adunk, melyet a BCE szerverei nem igazán tudnak jelenleg feldolgozni. Ez magyarul – persze erős sarkítással – hackertámadás! (Varga, 2013).

Szinte biztos védelmet jelent, ha a felhőbe feltöltött adatainkat titkosítjuk, de ha a különböző kulcsokat elveszítjük, akkor viszont ez olyan, mintha a szóban forgó adataink megsemmisültek volna. (Racsó, 2012).



7. ábra: A felhő kockázatai

Egyébként előfordulhat az is, hogy a szolgáltató elszámolja magát és egyszerűen nem rendelkezik a szükséges erőforrásokkal – bár szerintem a 21. században, ahol 6 nanos processzorokat gyártanak (Computerworld, 2013) és vércukormérő kontaktlencsét terveznek (The Guardian, 2014) ott elvileg nem kéne ilyennek előfordulnia. (Racsó, 2012).

Zárva a sort a virtualizációért felelős program is meghibásodhat és akkor az egész Cloud összeomolhat. (Racsó, 2012).

Ezek után először a három nagy szolgáltató ÁSZF pontjait elemzem, utána pedig - ahogyan a dolgozatom elején írtam - elkezdem személyes interjúk keretein belül megvizsgálni a fentebb tárgyalt pontokat: megkérdezem az S&T rendszerintegrátor cégcsoport szolgáltatásfejlesztési vezetőjét, továbbá a Deloitte közép-európai CIO-jának, valamint a T-systems cloud biztonságért felelős szakértőinek véleményét.

7.A felhő szolgáltatás biztonsági kérdései a gyakorlatban

7.1. Szállítói vállalások és kínálat

Ebben a részben olyan kérdésekre keresem a választ, mint például:

- Milyen biztonsági intézkedéseket tesznek adataink védelmének érdekében?
- Mit tudni az adatközpontokról?
- Mi történik, ha elvesztik adataimat?
- Hogyan titkosítják adataimat?

Továbbá azt is kutatom, hogy a nagyobb szolgáltatók a *privacy policy* és *terms and conditions* dokumentumaikban mit vállalnak az adott szolgáltatással kapcsolatban. Mekkora a minőségi és mennyiségi különbség és egyezés van ezek között?

7.1.1. Google

Kutatásom során, sajnálatos módon arra a következtetésre jutottam, hogy a keresőóriás általános szerződési feltételei alapján elég nagy alá-fölérendeltségi viszony alakul ki közte és ügyfele között! Bővebben erről a mellékletben.

Nagy kutatómunka eredményként megállapítom: Egyáltalán nem derül ki a hivatalos honlapjáról, hogy az iskoláknak, kormányzati szervezeteknek és vállalatoknak kínált csomagjaiban az adatainkról pontosan milyen ÁSZF alapján rendelkeznek! Pont azon adatokat hiányoznak, melyek a legjobban érdekelnének minket, mint leendő ügyfelüket!

Azonban nézzük meg, hogy mit is kínál számunkra:

A Google üzleti felhasználásra a következő szolgáltatásokat biztosítja: felhőalapú fájlmegosztás, csoportmunka elősegítése: közös naptárral, dokumentumokkal, táblázatokkal, prezentációkkal, Hangouts, különböző házirendet tartalmazó Chrome, hirdetések és még több mint egy tucat szolgáltatást ajánl. Azonban biztonsági kérdések tekintetében mi a helyzet?

2014. január 30-án a Google SLA pontjai között következő biztonsági elemeket kínálja vállalatoknak:

A vállalattal megosztott adataink a mi tulajdonunkat képezik ezek után is, folyamatos biztonsági mentés készül a háttérben, adatközpontjaik 99,9%-os rendelkezésre állást biztosítanak, mely azt jelenti, hogy 1 hónap alatt összesen 16 perc a megengedett kiesési idő, alkalmanként 1 perc maximumban. (Csala, 2013).

SSL protokollal titkosítják a munkafolyamatunkat, és megkapták az Ernst & Young vállalattól az ISO 27001 tanúsítványát, mely kiterjed a biztonsági előírásoktól kezdve egészen a munkaerő felvételen és elbocsátáson át egészen a rendszerek fizikai védelméig. (ISO, 2013)

Ezen felül, bármilyen internet kapcsolattal rendelkező böngészőről dolgozhatunk a vállalati projekteken egyedül és csoportosan is, vagyis nagyban támogatja a mobilitást, mely korunk egyik legnagyobb igénye, hogy földrajzilag függetlenül, bárhol, bármikor, bármit elvégezhessünk. Támogatja mind az Android, iPhone és mint a Windows Phone készülékek közötti munkát.

Személyre szabott e-mail címet ajánl, éjjel-nappal elérhető ügyfélszolgálatot és folyamatos szoftverfrissítést, az árazási struktúrája is elfogadható, hiszen felhasználónként éves szinten 10-12 ezer forintból biztosított a szolgáltatás.

Főleg az USA-ban és Észak-Európában: Írországból, Belgium és Finnországból vannak az adatközpontok. Az itt tárolt adatok főleg emberi mulasztás miatt veszhetnek el, például véletlen törlés, felülírás miatt. (Computerworld, Anonymus, 2013)

7.1.2. Amazon



A Seattle-ben székelő amerikai cég az internetes kereskedelem mellett a felhőszolgáltatások terén is megjelent ajánlataival 2006-ban mind az USA-ban, mind Európában: S3 (Simple Storage Service) és EC2 (Elastic Compute Cloud). Míg az első felhő alapú tárhelyet biztosít, addig másikkal – mint korábban már említettem – infrastruktúrát tudunk bérelni.

Ebben a részben az Amazon hivatalos, jelenleg hatályos adatvédelmi irányelveit elemzem:

Hasonlóan az előbbi céghez itt is nehézkes volt előkeríteni valami hasznos dokumentumot a weboldalukról, melyből megtudhatnánk, hogy adatbiztonság terén mi a helyzet. Az Amazon web services rész - mely alatt a felhőt kell, hogy értsük most, - adatvédelmi irányelvei – mint nehezen kiderült - megegyeznek a hagyományos Amazonasokkal, vagyis:

Amennyiben vállalatunk bármilyen adatot a szolgáltató birtokába juttat, akkor mi teljes körű engedélyt adunk nekik bármire az adott fájlal kapcsolatban.

SLA-k tekintetében hasonlót ajánlanak, mint a Google, vagyis 99,95%-os rendelkezésre állást, de – „nagy meglepődésemre” ez tájékoztat minket túl sok mindenről.

Technikailag a következőket biztosít: HTTPS-en keresztüli hozzáférést – adatszivárgás ellen véd minket, beépített tűzfalat, különböző hozzáférési szinteket lehet kiadni az alkalmazottaknak, éjjel-nappal lehet őket hívni segítségért, VPN-es hozzáférés, az adatokat titkosítva tárolják AES 256-os szabványt felhasználva – melyet a Tresorit is alkalmaz (erre később kitérek).

Bármikor felmondhatják a szolgáltatást és nem is mindig tájékoztatnak minket, ha valami megváltozik a szerződésben!

Adatainkat Dublinban, Londonban, Frankfurtban elhelyezkedő adatközpontjaikban tárolják. (Rich, 2008). A Business Insider beszámol egy 2011-es hatalmas adatvesztésről: ekkor kiderült, hogy nem is igazán volt megfelelő biztonsági másolat és a 99,9%-os rendelkezésre állást sem tudták biztosítani. Rengeteg ügyfél adata elveszett örökre....

Összességében elmondható a fenti két vállalatról, hogy technikailag, műszakilag fejlett technológiákat és módszertanokat alkalmaznak adataink biztonsága érdekében. Azonban, ami ennél is lényegesebb, hogy a működése elvük, szellemiségük és hozzáállásuk kételyeket ébresztenek bennünk, hiszen – szemmel látható - nem rendezik megnyugtatóan az adatvédelem kérdését! Mint láthattunk, még ha állítanak is valamit, nem biztos, hogy az úgy lesz, és mivel elég nagyok, így sok mindent megtehetnek büntetlenül.

Egy 2013-as Symantec felmérés szerint a 3200 megkérdezett vállalat 43%-ának veszett már el valamilyen adata felhőszolgáltatásból és az adatbiztonság kérdése még kritikus is marad egy ideig!

Érdemi információt pedig nem találni a „lock-in” nevezetű jelenségről!

Hiába nagy a szolgáltató, 2012 Karácsonyán egy teljes napra leállt a felhőszolgáltatása, mely emberek és dollárok millióit is érintett. (Reuters, 2012)

7.1.3. Microsoft Azure

Amikor például a Bing internetes weboldalon keresünk, akkor utasításokat adunk a háttérben megbújó hatalmas infrastruktúrának (felhő), mely a másodperc tört része alatt eredményt szolgáltat. Hasznos és kényelmes, de biztonság tekintetében mit kínál a Microsoft?



A szoftveróriás felhő platformjának biztonsági kérdéseit – a fentiekhez hasonlóan – elemzem ebben a részben. Az Azure szolgáltatásra

is egy általános adatvédelmi leírás tartozik: Vállalként a következőkről kell tudnunk:

Adatainkat megoszthatják leányvállalataikkal, vállalati összeolvasás és eladás esetén, beszállítóknak, ügynököknek, törvényi kötelezettségből kifolyólag. Tehát – hasonlóan – az eddigi tapasztalatokhoz személyes adataink itt is nyilvánosságra kerülhetnek.

USA-ban és Európán belül Írországban, Hollandiában vannak fizikai központok. A Service Level Agreement-ben mindenre 99% fölötti megbízhatóságot garantálnak például: helyreállítás, adatok tárolása, SQL adatbázis.

Éjjel-nappal hívhatjuk őket segítségért, rendelkeznek az *ISO/IEC 27001:2005* és a *SAS 70 Type I and II* szabvánnyal, melyeket elolvasva komoly technikai felkészültséget feltételezhetünk és állításuk szerint könnyen konfigurálható a szolgáltatás.

Arra kérdésre, hogy adatvesztést hogyan lehetne elkerülni, azt tanácsolják, hogy használjunk másodlagos adatközpontokat, de hogy hol, kiért stb... nem írják le a honlapjukon. Azonban egy régióban nem csak egy adatközpont van, így adataink másolatát könnyen helyre lehet állítani probléma esetén.

A NIST titkosítási specifikációját (AES)-t használják adataink titkosítására.

Az eddigi három példa nagyjából ugyanazt ajánlja a felhő terén, mint kutatásom során kiderült a *privacy policy* és *terms and conditions* nem adnak elegendő támpontot, hogy ügyfélként hozzájuk forduljunk!

7.2. Vállalati interjúk

A következőkben rátérek a gyakorlati kutatásom főbb pontjaira. Rendre a Deloitte, a S&T és a T-systems vállalatoknál készített interjúkat közlöm alább. A strukturáltabb áttekintés és megértés érdekében itt felsorolom, hogy milyen pontokat fogok érinteni:

- Biztonságtechnológia
- Üzemeltetésbiztonság (BCP, DRP)
- Kockázatkezelés
- Szállítómenedzsment (Trust)
- Szerződés, jogi kérdések
- CIA – Bizalmasság, Sértetlenség, Rendelkezésre állás
- Emberi tényezők
- „lock-in” jelenség
- SLA
- „rossz szomszédság”

7.2.1. A Deloitte CIO meglátásai

7.2.1.1. Bevezetés

A vállalati kutatás első interjút Kerékfy Pállal készítettem el, aki a Deloitte Central Europe IT vezetője. Ebben a részben bemutatom, hogy a CIO az elmúlt másfél évtizedes tapasztalata alapján hogyan látja a Cloud szolgáltatást érintő biztonsági kérdéseit.



Szerinte Edward Snowden leleplezése nem mutatott be forradalmian új körülményeket, hiszen ezt már régóta tudhattuk. Tehát a vállalatok stratégiájukat nem befolyásolja akkora mértékben, inkább csak jobban átgondolják, hogy mit raknak ki a felhőbe. Azonban egy Deloitte-hoz hasonló méretű vállalatnak vigyázni kell olyan szempontból, hogy ha például az e-maileket ki szeretnék tenni felhőbe, akkor az emberekben felmerülhetnek aggályok, hiszen a sajtó rengeteget foglalkozott a témával. Még ha nincs is valós veszély, az ügyfelek kételkedni kezhetnek, és ennek eredménye akár hosszú időre is rányomhatja a bélyegét a vállalat jövőjére. Olyan intézményeknél, mint bankoknál, egészségügyi intézményeknél, ahol szigorúbb szabályozások vannak, még körültekintőbben kell eljárni, például tavaly szeptemberben az EuroCloud hazai konferenciáján jelentették be, hogy az MKB belső levelezését kiszervezték külső felhőbe a PSZÁF – most már MNB – előírásait betartva. (Laikus ügyfélként, aki csupán a *felhő* szót és a lehallgatási botrányt ismerem, elkezdenének aggályaim lenni a bankom megbízhatóságát illetően.)

7.2.1.2. Biztonságtechnológia

Az interjúalany szerint mindenekelőtt viszonyítási alapként tisztázni kell, hogy mi az a biztonság, mit tekintünk annak, mihez viszonyítunk.

Tapasztalata szerint a biztonság akadályozza a használatot. A nulla biztonság kényelmes használatot tesz lehetővé, a maximális biztonság pedig már szinte akadályoz minket, és pont az az előny és kényelem veszik el, amit a felhő adhat nekünk. Például a

felhőben működő e-mail, mely elég kényelmes, hiszen bárhol, bármikor használható: táblagépről, telefonról, számítógépről, internet kávézóból.

Azonban, ha ezt elkezdem védelemmel körülvenni, akkor elkezd bonyolulttá válni ennek a kezelése. Lehet end-to-end titkosítást használni Outlook esetén és úgy dönteni, hogy vannak - akár - nyilvánosságra is hozható e-mailek és kritikus információkat tartalmazó levelek. Ezeket titkosítjuk, de akkor böngészőből nem lehet használni, csak a megfelelő kliens szoftverrel érhetem el leveleimet, mely telefonon és táblagépen nem működik, internetkávézóban meg esetleg USB-ről futtatható programmal lehet használni... Elég kényelmetlenné válik így a használat és a felhő elveszíti pont az egyszerűségét és kényelmességét, amit alapjában szolgál.

7.2.1.3. Bizalmassági kérdések

Az elmúlt több mint másfél évtized tapasztalata azt mutatja, hogy a házon belül tartott adatokkal vagy éppen a vállalati szoftverekkel kapcsolatos információbizalmasság egyáltalán nem magasabb a kis- és középvállalatoknál, de még a nagyvállalatoknál sem, mint ha kiszerveznék egy megfelelő vállalatnak. Tehát nem csak az új technológiai megoldás rossz oldalát kell nézni, hanem meg kell vizsgálnunk, hogy az eddigiekhez képest milyen szintű változást hozhat.

A CIO meglátása szerint nagyon sok olyan eset van a felhőt leszámítva, amikor egy cég szállítója hozzáférhet a vállalat adataihoz!

Az interjúalanyom példákkal támasztotta alá a fenti állítást: Az irodában keletkezett papírokat megsemmisítetik egy külső vállalkozóval, mert nem olyan egyszerű azt szakszerűen elvégezni, vagy amikor vállalati adathordozókat, HDD-ket semmisíttetnek meg külső vállalkozóval, valamint amikor saját cégünk nyomtatóit javítja egy másik fél, melyek jelenleg „kész számítógépek” és a korábban kinyomtatott dokumentumokat is ki lehet még nyerni ezekről. Továbbá, ha garanciális javítást végez valaki egy szerveren, laptopon.

A vállalatok lépten-nyomon lehetővé teszik azt, hogy külső szállítók hozzáférjenek akár a vállalat legféltebb adataihoz, és pontosan ilyen maga a felhő is. Ez ellen megfelelő szerződéssel és reputációval rendelkező külső cég alkalmazásával lehet védekezni

7.2.1.4. Szállítómenedzsment és jogi kérdések

Kerékfy Pál szerint a cégeknek meg kell találniuk az egyensúlyt a megfelelő mértékű biztonság és a használat kényelmessége terén. Például mikro- és kisvállalatoknak egyszerűen nem éri meg saját e-mail szervert fenntartani, mert az ezzel járó hardverek, szoftverek, szakértelem, üzembiztonság és még sok más rengeteg pénzbe kerül, ha meg külső szolgáltatótól veszi igénybe, akkor biztonság terén megint előjönnek a kérdések.

SLA-k tekintetében eddigi tapasztalata szerint nem azt kell figyelni, amit vállalnak pl. 99,99%-os rendelkezésre állás, hanem amit valójában teljesíteni tudnak. A jó kérdés elmondása szerint - melyet szem előtt kéne mindnyájunknak tartani -, hogy mennyire gyakoriak a hibák és ezeket mennyi idő alatt tudják elhárítani?

A CIO szerint az egyes országok eltérő adatvédelmi előírásai erős függőségben állnak azzal, hogy az adott országban hogyan értelmezik a törvényt az egyes esetekben. illetve milyen jogi szankciók vannak, hiszen ha például 3000 dollár a büntetés, de a vállalatunk nyer ezen 250.000 dollárt, akkor megéri, de ha a vállalat vezetőit börtönbüntetés fenyegeti, akkor már más a helyzet. Ha mi innen Amerikába helyeznénk ki adatainkat egy felhőszolgáltatóhoz, akkor probléma lehet, hogy hiába fordítjuk le a szabályokat magyarra, biztosan nem értenénk ezeket megfelelő szinten, mert ugyanis ezeket a helyi jog alkalmazása szerint kell érteni, vagyis meg kell értenünk egy másik ország jogrendszerét, amit mi innen, ilyen távolról elég nehezen tudnánk kivitelezni.

Továbbá mindent le lehet szabályozni és jogi szankciót bevezetni például, ha az adataimat elviszi a rendőrség egy adatközpontból, mert a szomszéd éppen illegális filmeket tartott ott. Ehhez semmi közöm, de még is én szenvedek kárt. Kiköthetem a szerződésben, hogy ilyen esetben \$1.000.000 kártérítést kapjak, de akkor a vállalatnak ezt a pénzt előre be kell gyűjtenie arra az esetre, ha ez előfordulna. Ez viszont beleépülhet az árakba, vagyis, akkor meg megint nem lesz költséghatékony, mert ugyebár jóval magasabb áron vehetem igénybe a szolgáltatást.

7.2.1.5. Üzemeltetésbiztonság és a „Lock-in” jelenség

Eddigi meglátásai szerint két egymástól független felhőszolgáltatót kell használni párhuzamosan.

Az elmúlt időszakban jelentek meg a kimondottan disaster recovery eset megelőzésére használatos szolgáltatások. Ezeknek a lényege, hogy csak tárolásra küldjük adatainkat a tárhely szolgáltatónak és nem akarjuk vissza olvasni. Ez számunkra alacsonyabb költséget jelent, valószínűleg ez a szolgáltatónak technikailag kevesebb erőforrásköltséggel jár pl. nem pörgő winchesteren tartja az adatokat. Másik előnye, hogy még akkor is, ha földrajzilag két független helyen van az adatközpont, akkor is előfordulhat a szoftveres probléma, így megszakad a virtualizáció folyamata, vagyis egyik helyről sem érhetjük el adatainkat.

A biztonságot tekintve az IT vezető szerint itt is a korábbi megoldás párhuzamos, két szolgáltatós modell a megoldás. Azonban mielőtt megkötnénk a szerződést tisztázzuk, hogyan kaphatjuk vissza adatainkat. Tapasztalatból tudjuk, hogy ez nem olyan egyszerű!

Erre egy jó példa a mai bankrendszer, hiszen a pénzünket ingyen betehetjük a bankszámlánkra, de a kivételért már egy halom pénzt számolnak fel nekünk. Itt is hasonló a helyzet, mint a nagy felhőt kínáló vállalatoknál – mint korábban már bemutattam – könnyedén, egyszerűen feltöltöm adataimat, de utána nincs visszaút, ott marad szinte örökre a nyoma, teljes mértékben nem tudjuk eltüntetni a „nyomokat”.

7.2.1.6. Emberi tényezők és a változáskezelés

Szerződéskötés során vizsgálendő a következő: a szerződés lehetővé teszi-e, hogy néhány HDD-vel odamenjünk és ott helyben az adatközpontnál letöltsük ezekre adatainkat.

A papír mindent elbír, mindent le lehet szabályozni, be lehet állítani, de az emberi tényezővel mindig számolni kell! Ő ugyanis az adatokat kiviheti a cégből, elhagyhatja a belépési kódokat, a vállalati e-maileket Gmail-ben is olvashatja és kijátszhatja a biztonsági intézkedéseinket. Pontosan emiatt ésszerű lehet a belső vállalati biztonsági szint okozta kényelmetlenségeket csökkenteni - látszólag – a biztonság rovására, de gyakorlatilag ilyenkor a biztonságot növeljük, mert az alkalmazottaink nem azon fognak gondolkodni, hogyan játsszák ki a belső szabályozást. Alapos tervezéssel meg kell vizsgálni, hogy az egyes biztonsági intézkedések mit váltanak ki az emberekből!

A szakember szerint nincs nagy befolyásunk, hogy melyik funkció, gomb és egyéb összetevők hogyan változnak, hova kerülnek át a programban. Tőlünk függetlenül történik ezen ügyekben a döntéshozatal, hiszen a felhő méretgazdaságossági okok miatt tudja azt a bizonyos szolgáltatást olyan minőségben nyújtani. Ha pedig mindenkinek külön rendszert szolgáltatnánk, akkor már egyáltalán nem érné meg neki.

7.2.1.7. Összefoglalás

Összefoglalva az interjú tanulságait, számomra a következő következtetések voltak jelentősek: Ahogyan az élet minden területén itt is rendkívül fontos, hogy az *Aurea mediocritast*, vagyis, hogy az arany középutat megtaláljuk! Vállalattól és helyzettől függően mérlegelni kell, hogy mi az a biztonsági szint, ami már véd, de még nem akadályoz minket a mindennapi hatékony működésben.

A Cloud szolgáltatás minőségét meghatározza maga az ár is. („*Olcsó húsnak híg a leve!*”) Nem minden esetben éri meg költséghatékonyságra hivatkozni döntéshozatal során, mert lehet, hogy nem véletlen olcsóbb az a szolgáltatás.

7.2.2. S&T

7.2.2.1. Bevezetés

A felhő biztonsági kérdéseinek vizsgálatát az S&T cégnél készítettem. Kresz Balázst kérdeztem meg, hogy ő hogyan vélekedik a felhő biztonsági kérdéseiről. Ő korábban folyamatmenedzsmenttel foglalkozó tanácsadóként dolgozott, jelenleg a 19 országot lefedő S&T rendszerintegrátor cégcsoportnál szolgáltatásfejlesztési vezetői pozícióban van.

Mivel a cég Microsoft Azure szolgáltatást ad tovább ügyfeleinek megnövelt értékkel, így erről fog bővebben beszámolni az elmúlt időszak tapasztalatát felhasználva, melyet főleg nagyvállalati szempontból látott.

Úgy látja, hogy az elmúlt időszakot érintő adatbiztonsági botrányok nem befolyásolták nagymértékben az emberek hozzáállását, magatartását és gondolkodásmódját, hiszen ez nem volt meglepő. Eddig is lehetett tudni, hogy az NSA és egyéb kormánysszervek kényük-kedvük szerint megtudhatnak Rólunk, a vállalatokról bármit, főleg, hogy 2001 szeptembere után a terrorizmus elleni védekezésben szinte bármilyen eszköz megengedett. A helyes kérdés sokkal inkább: „Ki gondolta, hogy ez nem így van?!”

Edward Snowden és a történetek szerinte egy indok, illetve egy kifogás lett, amelyet felhasználva a vállalatok vezetői el tudják halasztani időlegesen a felhőt alkalmazását – annak ellenére, hogy mennyi előnye és kényelmessége is van.

Kresz Balázs úgy véli, hogy az emberek félnek – főleg- vállalati felhasználásban, mert egy esetleges rossz döntés, mely a cég hírnevét érinti, akár az állásába is kerülhet a felelős döntéshozónak. Magánemberként másfajta és más mértékű a felelősség és a kár, mint vezetőként egy vállalatnál. „*A változás az kockázatos.*” Ebben az esetben felhő irányába elmozdulni az kockázatos!

7.2.2.2. Biztonságtechnológia

Kiemelte, hogy egy kulcs elem van itt, mely a felhőt érinti. Ez pedig nem más, mint a „*hangulatok és érzések*”, melyek az emberekben keletkeznek és pszichológiailag

magyarázhatóak. Csak azért, mert nem hazánkban van, és én nem tudunk odamenni fizikailag a szerverekhez, nem szabad téves feltételezéssel élni. Ha nekünk jól definiált és előre megtervezett biztonsági igényeink vannak a szolgáltatás kapcsán, akkor ezeket a Top-down elv mentén el tudjuk érni.

Ezt úgy kell érteni, hogy ha eljutunk szakmailag arra a szintre, hogy nekünk pontos definiált, műszaki igényeink vannak például azzal kapcsolatban, hogy a titkosításnak mi legyen a mértéke, az adatátviteli csatorna mennyire legyen megbízható, akkor látni fogjuk, hogy a nagyobb felhőszolgáltatók alapvetően már ezen követelményeknek megfelelnek vagy mi tehetünk azért, hogy ez így legyen.

Úgy véli, ha biztonságról beszélünk, akkor fizikai és logikai szempontokat kell figyelembe venni. Személyes tapasztalata, hogy a Microsoft adatközpontjában nagyon szigorú előírásokat kell betartani.

A logikai biztonság terén felhívta a figyelmemet a Microsoft egy óriási előrelépésére a biztonság terén. Néhány héttel korábban, januárban a Microsoft megkapta a PCIDSS megfelelésséget, melynek megléte minden olyan cégnek kötelező, amelyik kártyaadatokat kíván kezelni. Ez rendkívül fontos, mert így elérhetővé vált a szoftveróriás számára, hogy olyan rendszereket építsen ki, melyek bankkártya adatokat is képesek megbízhatóan kezelni a felhőben!

Eddigi meglátásai szerint a céget felkereső leendő ügyfelek főleg két nagyobb, aggályosnak nevezhető tényező iránt érdeklődnek kimondottan. Egyrészt a kommunikációs csatorna és annak titkosítása, másrészt az adataik titkossága és hozzáférhetősége.

Az elsőre megfelelő megoldás az, ha a felhő – jelen esetben az Azure – és a vállalat saját hálózata között egy VPN csatornát alakítunk ki, mely önmagában is már titkosított.

A másik felvetésre pedig az a gyakorlati tapasztalat, hogy a vállalatok azokat az adataikat teszik ki egyelőre a felhőbe, melyek egy esetleges nyilvánosságra kerülés esetén sem okoznának nagyobb problémát a vállalatnál, mely a hibrid felhő modelljét követi.

Felhívta a figyelmemet, hogy az egyes adatközpontokban magasabb hőmérsékletet hagynak az utóbbi időben.

Ennek az oka, hogy így gazdaságilag sokkal jobban megéri, ha kevésbé hűtik ezeket a termeket, mert olcsóbb megsemmisíteni és újat venni az adattárolókból, mint állandóan fenntartani azt az alacsony hőmérsékletet, mely biztosítaná a tárolók hosszabb élettartamát.

A Microsoft Azure használata során, amikor tárhelyet akarunk például bérelni, akkor egy management felületen keresztül be lehet állítani, hogy a duplikációt hogyan kívánjuk

igénybe venni, vagyis például, hogy földrajzilag hol legyenek ezek Európán belül (Amszterdam, Dublin), egy helyen, több helyen.

7.2.2.2. Bizalmassági kérdések

CIA modellt illetően elmondta, hogy jelenleg a kétfaktoros autentikáció jellemző Azure alatt, mely „C” előtagot érinti. Ez azt jelenti, hogy a klasszikus felhasználónév és jelszó pároson kívül megjelenik még egy lépcső, melyet így ír le: „*something that you are*”, „*something that you know*”, „*something that you got*”

Az első rész utal arra, hogy mi kik is vagyunk valójában, mi a nevünk, a második rész gondoskodik arról, hogy mi az, amit csak mi tudunk, vagyis mi őrizzük ennek a titkát és végül pedig a harmadik összetevő, ami csak is kizárólag nekünk van például a mobiltoken, mely eléggé elterjedt a mai világban. Mobiltoken alatt azt értjük, hogy miután beírtuk helyesen a felhasználónevünket és jelszavunkat, kapunk sms-ben egy belépési kódot, amit kér a rendszer ráadásként.

A CIA modell „A” összetevőjét elemezve elmondta, mint érdekesség, hogy ezt a 99% fölötti rendelkezésre nem a műszaki és technológiai háttér a lényeges, hanem sokkal inkább a kialakított logika, amely mentén ez működik!

7.2.2.3. Szerződéses és jogi kérdések

Kikértem Balázs véleményét azzal kapcsolatban, hogy mit gondol arról, mint kihívásról, hogy makrogazdasági szinten eltérőek az adatvédelmi irányelvek:

Szocsiban most zajlik a téli olimpia – Az oroszoknak meglehetősen tetszik a felhő „intézményesítése”, hiszen Oroszországban másfajta az állam hatalmi felfogása, ami a felhő esetében hatalmas előny. Nem lehet fizikailag „csak úgy” elvenni valakitől valamilyen informatikai berendezést, hiszen „nem tudni hol van”. Ennek ott kimondottan örülnek ott a helybéliek.

Sajnos semmilyen lehetőségünk sincs módosítani, személyre szabni a Microsoft nyújtotta szerződést, ÁSZF egyes részeit. Elfogadjuk vagy nem! Ez a két lehetőségünk van.

A korábban tárgyalt „rossz szomszédság” esetéről elmondta, hogy a Microsoft nem adja ki fizikailag senkinek sem az adattárolókat. Bűncselekmény gyanúja esetén kiszolgálja az egyes országok kormányzszerveit, de nem kell attól tartanunk, hogy a felhőben tárolt adataink

elvesznek, mert a virtualizáció következtében éppen egy illegális fájlmegosztó lett a szomszédunk a felhőben!

A „lock-in” jelenségtől igenis van félni valónk, hiszen, ha egy kódot megírunk és az futtatható a Microsoft platformján, akkor az egyáltalán nem biztos, hogy kompatibilis más szolgáltató Paas szolgáltatásával.

SLA-k tekintetében elmondta, hogy 100%-ban semmit sem garantál a cég, mert mindig vannak külső, véletlentényezők, melyek nem lehet előre látni. Ez esetben mi nekünk be kell bizonyítanunk, hogy a szolgáltatás kiesése kárt okozott, és jogosan követelhetjük a bíróságon a cég biztosításából a minket illető részt.

7.2.2.4. Befejezés

Zárszóként Balázs a kockázattal arányos védelmet ajánlotta és a bizalom kérdését vetette fel. Egy kollégája Gyenes István gondolatát ismertette, hogy mi is az a felhőszolgáltatás valójában, melyben senki sem kételkedik egyáltalán, senki sem fél, még gyermekek életét is érinti, de senki sem teszi fel a kérdést nap mint nap, hogy biztonságos-e?

Ez pedig a csapvíz. Megisszuk, gyermeke fürdenek ebben, megisszák. Mégsem vonjuk kérdőre a Fővárosi Vízműveket folyamatosan, hogy megbízható-e a szolgáltatás, tiszta-e a víz, hanem megbízunk és hiszünk nekik, tudván, ők a szakemberek, ez a szakmájuk, ezt tanulták. Emiatt lehet, hogy jobban értenek ehhez, mint mi!

7.2.3. T-systems

7.2.3.1. Bevezetés

A T-systems vállalatnál Gélák Róbertet és Németh Mihályt kérdeztem arról, hogy ők a vállalatnál mit tapasztaltak a TDK témám illetően. Róbert a cég Cloud biztonsági részével foglalkozott, míg Mihály a Cloud menedzsmenttel és annak eszköz támogatásával. A T-systems a Microsoft Azure termékét veszi igénybe.

Mindketten ijesztőnek vélik, hogy tapasztalatik szerint nem befolyásolta az emberek és főleg a vállalatok magatartását semmilyen irányban sem Edward Snowden, a WikiLeaks és egyéb adatbiztonsági botrányok. Az emberek még csak össze sem kötik a kettőt egymással! Mondván, hogy Amerika messze van és minket úgy sem ér el annyira, valamint inkább bulvár hírként kezelik, mely magyarázza ennek a jelentőségvesztését.

7.2.3.2. Biztonságtechnológia

Vannak olyan speciális iparágak, mint egy pénzügyi szolgáltató, ahol a – korábbi PSZÁF – MNB igen komoly külső előírásainak kell megfelelni. Például, bankkártyás tranzakciók lebonyolításához PCIDSS megfelelésséggel kell rendelkezni – mint azt korábban már én is említettem. Azonban ezeknek a feltételeknek a jelenleg hatályos jogszabályi környezetben egy ilyen felhő szolgáltató nem tud megfelelni, emiatt bankok nem is szerveznek ki felhőbe semmit.

A kis cégeket nem is foglalkozik azzal, hogy a szolgáltató hogyan éri el a vállalt 99,5%-os rendelkezésre állást. Különböző ISO szabványokkal kell rendelkezni, melyeknek a megléte kötelező, ezek szerint működni elvárható, de a legtöbb esetben nem is kell bemutatni, bizonyítani ezek meglétét.

Interjúalanyaim meglátása szerint ezek hangzatos szavak, de nem hangsúlyosak. Egyszerűen ránéznek az ISO papírra, örülnek, de ha más 20 százalékkal olcsóbb, akkor azt választják az ügyfelek a magyar piacon.

Alapvető kérdés, melyet nekünk kell eldöntenünk, mikor felhőt veszünk igénybe, hogy mennyire értékes az adott adat, folyamat.

A klasszikus háromszögben a Saas, a jéghegy csúcsa. Például, ha egy MS exchange szolgáltatást veszünk igénybe a vállalati levelezés működtetéséhez, kezeléséhez. Ebben az esetben az ügyfelek csak is kizárólag a legfelső, logikai szintet látják és nincsenek tisztában azzal és nem is láthatják, hogy mi történik egy szinttel lejjebb a levelek tárolása, kezelése tekintetében.

A Saas alatt fut egy operációsrendszer. A mailboxok pedig valamilyen fájlokban ott vannak, de ezt az operációs rendszert valakinek üzemeltetnie is kell, vagyis hozzáférése van a fájljainkhoz. Klasszikusan ilyen a Gmail példája. A leveleink átmennek SPAM szűrőkhöz, melyek folyamatosan olvassák ezeket. Nem tudhatjuk pontosan, hogy mi történik törlés esetén és honnan tudom, hogy az valóban törlődik-e.

A szakértők úgy vélik, hogy törlés esetén csupán a mi megjelenítési rétegünkben törlődik az adott levél, vagyis a mi szempontunkból.

A mentést, tárolást illetően felhívták a figyelmemet, hogy a szolgáltatók, hogy garantálják a leveleim folyamatos rendelkezésre állását és teljességét.

Ez nagy valószínűséggel azzal jár, hogy a mi mailboxainkat folyamatosan mentik a háttérben, hogy ha a technológiában valamilyen probléma adódik, akkor az számunkra teljesen láthatatlan módon „megoldódik” a háttérben.

A Paas kockázatait tekintve szerintük a legnagyobb kockázat a kompatibilitásban rejlik, és a frissítések kezelésén múlik. Amennyiben a platform standard módon módosításra kerül, amit szolgáltatásként nyújtanak, azon már bizonyos programok nem tudnak futni. Ha az ügyfél használ egy elavult szoftvert, de nem akarja upgradelni a programot, de az alatta lévő rendszert java 1.6-ról 1.7-re akarják cserélni, akkor nagy lehet a baj. A szóban forgó alkalmazás szoftverszinten képes előbbin futni, de a frissebb változaton már nem. Másik példa, ha Internet Explorer 6-ban meg tudunk valamit jeleníteni, de 9-ben már nem.

Úgy vélik, a „legalsó”, IaaS szinten arra kell figyelni, hogy egy olyan szolgáltatót vegyünk igénybe, aminek olyan széles a portfóliója és olyan platform választása szükséges, mely bármelyik infrastruktúrán futtatható! Ezt a felhasználási feltételekben le kell mindenféleképpen szabályozni.

7.2.3.3. Üzemeltetésbiztonság

A BCP, DRP „páros” vizsgálható, hogy fizikai eszközök, szabályozások, logikai, hálózati elhatárolások szintjén ez hogyan valósul meg. Felhívták a figyelmet, hogy – eddigi tapasztalataik szerint - az ügyfelek igen alacsony százalék tér ki arra a szerződésben, hogy az adatok hány százaléka veszhet el, mert abból indulnak ki, hogy nulla. Nagyobb tenderek estében kikötik, hogy a back-upokból való visszaállítás hány százalékanak kell sikeresnek lennie és sikertelen esetben milyen büntetési tétel várható, melyet százalékban, különböző szorzókkal, SLA pontbeli sérülések számával határoznak meg. Ez nem standard, hanem egyéni megegyezés kérdése.

Tapasztalatuk szerint jellemző, hogy a legtöbben egyedi, személyre szabott szolgáltatást szeretnének igénybe venni üzemeltetéssel. Ez utóbbi azt jelenti, hogy például vásárol 40 processzor magot, 100 gigabájt memóriát és 8 terabájt tárhelyet, melyeken windows szervert fog üzemeltetni, de kéri továbbá szolgáltatótól, hogy ők üzemeltessék. Így a patchelést, szerverek mentését, monitoringát és a karbantartás is teljes mértékben a T-systems végzi.

7.2.3.4. Szállítómenedzsment

A vizsgálatokhoz elengedhetetlen – szerintük -, hogy a vállalat jól körülhatárolható ügyfélköröket hozzon létre és ez alapján vizsgáljuk meg a biztonságtechnológiai, üzemeltetésbiztonsági, szerződéses kapcsolatot. Ilyen lehet például a külső szabályozói szempontból nem speciális közép- és nagyvállalatok, hiszen ők inkább érzékenyek és nem annyira biztonságcentrikusak. Meglátásuk szerint ezen kategóriába tartozó vállalatok nagy hangsúlyt fektet a megfelelő rendelkezésre állásra és kevesebbet a bizalmasságra.

Eddigi tapasztalataik szerint hazánkban a cégek félnek az SLA fogalmától, gyakran megijednek a „csupán” 99,5%-os rendelkezésre állástól, nem értik továbbá a havi és az éves rendelkezésre állás fogalmát, hiszen az adott időszakon belül várható adott kiesési idő teljesen más lehet.

A legtöbben elvárják, hogy egyéni ügyfélként kezeljék őket, testreszabott megoldásokat igénybe véve, de a szakértelem és a megoldások éretlenségéből kifolyólag könnyen el is lehet hitetni az ügyféllel, hogy őt egyénként kezelik. Elég, ha az ügyfél azt gondolja, hogy ez speciális, a háttérben meg minden standardizált. Azonban ez már csak „sales” kérdése, nem technológiai kérdés. Egyébként elvétele, néhol vannak igen hozzáértő

emberek, akik eléggé bele tudnak mászni, hogy technikailag minden úgy történjen, ahogyan kell.

Az ügyfelek sok mindenbe szeretnének belelátni, de az onnantól fogva már nem Cloud. Egyébként ez megoldható, de ekkor már a vállalat más szolgáltatását kínálja fel. A felhő igazi jelentését nem értik, csak a divatos szót és a költségcsökkentő tényezőt látják ebben. Ami miatt pont olcsóbb lenne, azt ráadásként rápakoltatnák. Tehát egy erős fogalmi zavar is jelen van az emberi tényezőket illetően.

Úgy vélik, hogy szolgáltatói oldalról problémás lehet, hogy az ügyfél nem látja, ez valójában mekkora beruházás a másik oldalon, hiszen a költséget itt tulajdonképpen havi részletekben, hosszú távon kell „visszaszednie”. Mint korábban írtam, a méretgazdaságosság itt az egyik kulcstényező, mellyel fenn lehet tartani hosszú távon a felhő informatikát – lásd korábban a Google és Amazon példáját. Különböző kötbérezéssel kell a szolgáltatónak bebiztosítani magát olyan esetekre, hogy az óriási beruházás után az ügyfél ne hagyja ott három hónap után.

Tehát, ha a szolgáltató nem bízik, és nem él a méretgazdaságossággal, tehát nem vállalja a kockázatot, akkor drága lesz a szolgáltatás. Ha hűségidőt kötünk ki, akkor pont a Cloud egyik alapfelvetését sértjük, mi szerint igény szerint vehetem igénybe a szolgáltatást.

7.2.3.5. Jogi kérdések és a CIA

Hangsúlyozták, hogy megdöbbentő a magyar adatvédelmi szabályozás erről rendelkező, jelenleg hatályos törvény, mely nem megfelelő. Például egy biztosító vállalat, mely adatkezelési tevékenységet folytat más számára, igénybe vehet adatfeldolgozót. Azonban azt már nem engedi meg, hogy ez az adatfeldolgozó más adatfeldolgozót vegyen igénybe. Ez azt jelenti, hogy ha a biztosító az IT például üzemeltetését ki szeretné szervezni, akkor ez a cég – a törvény szerint – már nem vehet igénybe még egy céget a munka elvégzéséhez.

Az elmúlt évek tapasztalata azt mutatja, hogy a büntetési tételeknek nincs elég visszatartó erejük! Sokkal többet nyernek azon a vállalatok, ha nem tartják be az adatvédelmi előírásokat, hiszen a büntetés összegét kiegyenlíti az ilyen módon elért nyereség, mely a kisebb kiadásból fakad. *(Azonban ez is túlmutat a kutatási területemen, hiszen itt a lobbizás és a politikai kérdések merülnek fel.)*

Makrogazdasági szinten eltérőek az adatvédelmi előírások. Külön kell kezelni az Eu-n belüli és az azon kívülre irányuló szolgáltatásokat. Az USA-ben létezik egy Safe Harbour nevű megállapodás, melynek lényege, hogy az ehhez kapcsolódó cégek betartják az Eu-s irányelveket. Így némi bizonyosságra szert tehetünk amerikai vállalat esetén, de még mindig kérdéses, hogy itthon ezt elfogadják-e.

A CIA háromszög egyes elemeit illetően elmondták, azt kell figyelembe venni, hogy az ügyfelek mit szeretnének elérni, mely főleg iparágfüggő. Ha mi például egy standard gyártósort vezérelünk, akkor nyilvánvalóan a rendelkezésre állás, az Availability a legfontosabb, hiszen az a legfájóbb, ha megáll a gyártás, míg bank esetében a Confidentiality kiemelkedően fontos szerepet játszik. Bankok legfeljebb belső felhőt alkalmaznának, de jelenleg a költségcsökkentő hatás miatt nem fognak kitenni semmit a felhőbe.

7.2.3.6. Zárszó

Zárásképpen a jövőt illetően megjegyezték, hogy 3 éven belül nagyobb változás a vállalati szektorban nem történhet, míg a hétköznapi ember a kényelmesség és egyszerűség miatt még jobban elkezd majd használni. Hozzá tették, hogy a vállalatoknál – sajnos – sokszor nem a leghozzáértőbb személy hozza a döntést az informatikai beruházás, így a Cloud kapcsán is, emiatt maga a technológia felhasználásából eredő hatékonyság nem fog megjelenni a mindennapi működésben.

8.A kutatásom eredménye és összefoglalás

8.1. Az interjúk összefoglalása

	Deloitte	S&T	T-systems
Biztonságtechnológia	Érték arányos védelem, mely nem akadályozza a használatot. Titkosítások használata	Jól definiált műszaki elvárások. Megfelelő logikai tervezés.	Iparágfüggő, alapos mérlegelés szükséges a különböző szintek igénybevételéhez
Bizalmassági kérdések	A vállalat legféltebb információihoz sok külső beszállító cég hozzáfér!	Elengedhetetlen a megfelelően kialakított logika, mely mentén működik a szolgáltatás.	Iparáganként eltérő, hogy melyikre fektetnek nagyobb hangsúlyt
Szállítómenedzsment	Hibák gyakorisága és elhárításuk időtartama	Ügyfelek aggályainak kezelése	Vállalatmérettől függ
Jogi kérdések	Betartatni a szerződésben foglaltakat.	Alaposan kidolgozott és betartható SLA, jogi szabályozást kell kialakítani	A hazai törvényi szabályozás nem megfelelő, éretlenség
Üzemeltetésbiztonság	Tanácsos Disaster Recovery használata felhőben.	A duplikációk miatt ma már nem igazán kelthet aggályokat.	Ügyfelek alacsony tájékozottsága.
„lock-in” jelenség	Párhuzamosan két vagy több szolgáltató igénybevétele.	Fenn áll a veszély!	Fenntartásokkal kell kezelni.
emberi tényezők	Ha nagy a szigor, az alkalmazottak kizárhatják a rendszert, mely óriási veszélyt jelenthet!	Pszichológiai és magatartástudománnyal kapcsolatos kérdések.	Információhiány, tájékoztatatlanság, egyéni és testreszabott szolgáltatások

8.2. Meglátásaim

Ebben a részben röviden felhívom a kedves olvasó figyelmét, hogy mire is kéne figyelnie, ha felhőbe szeretné vinni a saját adatait, vállalatát.

Arra a következtetésre jutottam, hogy a bizalmi kérdésekből vezethető le szinte minden. Meglátásom szerint ha magánemberként vesszük igénybe a nagyobb felhő szolgáltatók kínálatait, akkor kiszolgáltatott helyzetbe és függőségi viszonyba kerülünk. A Google, Amazon, Windows ÁSZF pontjai egyszerűen felháborítóak. Szó szerint leírják – ahogyan a mellékletekben is olvasható –, hogy szinte bármit megtehetnek adatainkkal és mi ez ellen nem is tehetünk semmit, vagyis igen, hogy ha nem vesszük igénybe a szolgáltatást.



8. ábra: Ígéretesnek tűnő, magyar tárhely szolgáltató

Kutatásom során interjút készítettem Szilágyi Györggyel, aki a Tresorit COO-ja. A magyar fiatalok 2009-ben indították el vállalkozásukat. Ők a fenti nagy szolgáltatókhoz képest hasonló biztonsági szinttel, de a *zero knowledge* eszközével élnek. A számítógépre letöltött kliens szoftver már alaptól titkosítja fájljainkat, emiatt nem is kell egyáltalán megbízni a szállítóban, hiszen – elmondásuk alapján ez egy end-to-end titkosítás fajta – ők semmit nem tudnak fájljainkról, még ha akarnának, akkor sem tudhatnának meg semmit. A titkosítás erősségét jól jelzi, hogy míg 2013 tavaszán 10.000 dollárt ajánlottak fel a világ hackerjeinek, hogy törjék fel őket, addig 2013 őszén már 25.000 dollárra nőtt a tét és még senki sem tudta feltörni őket.

Mivel a „régik nagyokhoz” képest kicsinek számítanak, nem igazán merik használni az emberek. Én személyesen, amint elolvastam a Google ÁSZF-jét, egyből letöröltem minden adatot a Drive-ból és elkezdtem a Tresoritot használni a bizalmassági kérdések kapcsán. Jól működik, megbízható, a mobil változata is rendkívül jól kezelhető. Mindenkinek ajánlom!

Vállalatoknak javaslom, hogy jogi szempontból alaposan gondolják át, hogy a szerződésekben, SLA-ban ki, mit vállal, milyen gyakoriak lehetnek a hibák és ezeket mennyi időn belül javítják ki. E mellé szükséges, hogy jól képzett, megfelelő gondolkodásmódú munkaerőt vegyünk fel, mert – mint bizonyítottam – mindig lesz olyan, aki valamilyen szinten hozzáfér bizalmas információkhoz, ezt nem lehet kiküszöbölni, csak a kockázatot lehet csökkenteni a megfelelő emberi erőforrással és a bizalom beépítésével a szervezeti kultúrába.

Mindezek mellett, konkrét technikai, műszaki igényeket kell megfogalmazni mindenféle biztonsági szinten, hogy mi mit szeretnénk kapni a pénzünkért cserébe. Ehhez tapasztalt clouddal foglalkozó szakember segítségét kell kérni, ahogyan én is tettem munkám során.

Úgy gondolom, hogy olyan nézőpontokat, véleményeket közvetítek ezen tapasztalt szakértőktől, melyeken egyértelműen megéri elgondolkodni. Amivel kezdtem a dolgozatomat, most azzal is zárom:

A Gartner szerint növekvő népszerűségnek örvend a biztonsági kérdések vizsgálata a felhőn belül és ez az évek során sem fog alábbhagyni. Én ehhez kívántam hozzátenni egy kis darabot a világ számára.

9. Zárszó

Kutatásom alapja a Cloud biztonsági kérdései voltak. Először megvizsgáltam, hogy a szakirodalomban mit lehet erről olvasni, a nagyobb cégek például a Gartner, Cisco, KPMG mit tartanak aggályosnak.

Azonban ezt nem találtam elegendőnek, szerettem volna, ha személyesen is hallom ezzel foglalkozó emberektől, hogy ők mit gondolnak a jogi, üzleti és műszaki kockázatok terén.

Az egyetemi vizsgaidőszakban TDK-t írni meglehetősen megterhelő dolog, főleg, ha az ember számára az 5.0 a cél. Azonban kutatásom egy percét sem bántam meg, mert olyan tapasztalatokhoz jutottam, melyeket majd fel fogok használni későbbi vállalkozóként és azon leszek, hogy a lehető legbiztonságosabban tudjam majd kezelni ügyfeleim adatait.

Remélem, hogy a kedves olvasónak is hasonló véleménye van, volt és lesz is a TDK-m kapcsán!

10. Forrásjegyzék

- Amazon (2008) Adatközpontok:
<http://www.datacenterknowledge.com/archives/2008/11/18/where-amazons-data-centers-are-located/>
- Amazon (2014) ÁSZF:
http://www.amazon.com/gp/help/customer/display.html/ref=hp_rel_topic?ie=UTF8&nodeId=200557360
- Amazon (2014):
<http://www.amazon.com/gp/help/customer/display.html?nodeId=468496>
- Andrew S. Tanenbaum – Számítógép-architektúrák (2006)
- Balogh Zoltán (2013) – BCE előadás
- Bögel György (2009) http://epa.oszk.hu/00000/00017/00161/pdf/5_bogel.pdf
- Business Insider (2011) Amazon lost data: <http://www.businessinsider.com/amazon-lost-data-2011-4>
- Business Insider (2013) A hero or traitor poll:
<http://www.businessinsider.com/edward-snowden-a-hero-or-traitor-poll-2013-6>
- Chikán (2008) Vállalatgazdaságtan 400. oldal
- Cisco (2012) :
http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/CLOUD_Index_White_Paper.pdf
- CNN (2013) Edward Snowden: <http://edition.cnn.com/2013/06/10/politics/edward-snowden-profile/>
- Computerworld (2013) Szomorú trend , növekvő adatszivárgás és károk:
<http://computerworld.hu/cio/szomoru-trend-novekvo-adatszivargas-es-karok.html>
- Computerworld (2014) Sávészélesség-rekord született:
<http://computerworld.hu/computerworld/savszelesseg-rekord-szuletett.html>
- Der Spiegel (2014) Edward Snowden:
http://www.spiegel.de/international/topic/edward_snowden/
- Dr. Csala Péter (2013) BCE előadás
- Dr. Tátrai Tünde (2013) Személyes adatok védelme: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:HU:PDF>
- Gartner (2013) <http://www.gartner.com/newsroom/id/2616115>
- Gartner (2013) <http://www.gartner.com/technology/research/cloud-computing/report/>

- Google (2014) :
https://www.google.hu/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:HUN&dl=hu&hl=hu&q=internet%20felhaszn%C3%A1l%C3%B3k#!ctype=l&strail=false&bcs=d&nselm=h&met_y=it_net_user_p2&scale_y=lin&ind_y=false&rdim=region&idim=country:HUN&ifdim=region&tdim=true&hl=hu&dl=hu&ind=false
- Google (2014) Google tests smart contact lens diabetics:
<http://www.theguardian.com/technology/2014/jan/17/google-tests-smart-contact-lens-diabetics>
- IBM (2004) SLA: <http://www.redbooks.ibm.com/redbooks/pdfs/sg246464.pdf>
- InformationWeek (2013) Microsoft's Azure Cloud Move: What It Means:
<http://www.informationweek.com/cloud/infrastructure-as-a-service/microsofts-azure-cloud-move-what-it-means/d/d-id/1111872?>
- ISO (2005) szabvány leírás: http://www.iso.org/iso/catalogue_detail?csnumber=42103
- ISO (2013) Licence Agreement for standards: <http://standards.iso.org/ittf/licence.html>
- Kathryn Rogers (2014) EU Data Protection Reform – Are we nearly there yet?:
<http://lawinthecloud.com/>
- New York Times (2014) [Edward Snowdenm Whistle-Blower:](http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html)
<http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html>
- NIST Cloud Computing definíció <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Patrick Van Eecke (2014)
http://www.nytimes.com/2014/02/19/business/international/eu-leaders-seek-way-to-protect-individuals-data.html?_r=0
- Portdolio(2014)
http://www.portfolio.hu/vallalatok/it/igy_allunk_a_regioban_az_informatika_teruleten.2.196865.html
- Racskó Péter (2012) - http://unipub.lib.uni-corvinus.hu/500/1/vt_201201p2.pdf
- Sipos Cintia (2013) BCE szakdolgozat
- Symantec (2013) Cloud Computing users losing data
<http://finance.yahoo.com/news/cloud-computing-users-losing-data-205500612.html>
- The Guardian (2014) Edward Snowden: <http://www.theguardian.com/world/edward-snowden>

- The Washington Post (2013) Edward Snowden, after months of NSA revelations, says his mission's accomplished: http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html
- Varga Krisztián (2013) IT Biztonság előadás Dr. Fehér Péter előadásán

11. Ábrajegyzék

1. ábra: Neumann János, forrása: www.iskola.nejanet.hu , hozzáférés 2014. január	6
2. ábra: A szolgáltatási szintek hierarchiája, forrása: Balogh Zoltán előadása	9
3. ábra: A telepítési szintek formái, forrása: Balogh Zoltán előadása.....	11
4. ábra: A hype görbe, forrása: Balogh Zoltán előadása	13
5. ábra: Edward Snowden, forrása: http://www.businessinsider.com/edward-snowden-a-hero-or-traitor-poll-2013-6 , hozzáférés ideje: 2014. február.....	17
6. ábra: Az információ bizalmasság alapja, a CIA háromszög, Balogh Zoltán előadása.....	18
7. ábra: A felhő kockázatai, forrása: http://www.altirnao.com/solutions/protect-your-files/ , hozzáférés ideje: 2014. február	
8. ábra: Családi képből óriás plakát, forrása: http://www.nbcnews.com/id/31214408/#.UufDTLSCvIV , hozzáférés ideje: 2014 március...	21

12. Melléklet

A keresőóriás 2014. január 28-án hatályos adatvédelmi irányelvei között a következő néhány sor olvasható, olvassuk el figyelmesen, főleg a kiemelt szavakra hívnám fel a kedves olvasó figyelmét!

*„Amikor feltölt vagy valamilyen más módon elküld tartalmakat a Szolgáltatásainkba, világszerte érvényes engedélyt ad a Google-nak (és a Google-lal együttműködőknek) az ilyen **tartalmak felhasználására, hosztolására, tárolására, reprodukálására, módosítására, származékos művek létrehozására** (így olyan művekre, amelyek fordítás, adaptálás vagy más módon történő módosítás eredményeképpen jöttek létre annak érdekében, hogy az Ön tartalma jobban megfeleljen a Szolgáltatásainkkal történő használatnak), **megosztására, közzétételére, nyilvános előadására, nyilvános megjelenítésére és terjesztésére.**”*

Én sem akartam elhinni, de ezek szerint bármit is elhelyezünk a Google szerverin, azzal Ők bármikor, bármit csinálhatnak, még reklám gyanánt is felhasználhatják legféltettebb családi titkainkat, mely valóban



9. ábra: Családi képből óriás plakát

megtörtént már! Engem személyesen ledöbbsentett az ügy!

Egy Saint Louis-i család Karácsonykor megosztotta Gmail segítségével saját képét barátokkal, ismerősökkel, melynek az lett az eredménye, hogy Csehországban egy óriás plakáton jelentek meg. Azonban miért is történhetett ez meg? (NBC, 2009)

Mindezek mellett az ÁSZF felhatalmazza a Google-t, hogy adatokat gyűjtsön a következőkről: hardvereink, operációs rendszerünk, mobilhálózati információink, telefonszámok: mikor, kit, mennyi időre, milyen minőségben hívtunk; SMS üzenetek útválasztási információi, IP-cím, rendszertevékenységek, hardverbeállítások, cookie-k, mobileszközök GPS-jelei, valamint készüléken tárolt személyes adatok (!).

Tehát majdnem, hogy minden adatot tárolnak rólunk, nem beszélve arról, hogy az iPhone 5S már ujjlenyomat olvasóval is rendelkezik, és innentől kezdve rengeteg aggály merülhet fel bennünk... (HVG, 2013)

Továbbá bármilyen külső fél számára is átadhatják adatainkat feldolgozás céljából – titoktartási és biztonsági intézkedések mellett-, akiket ők „megbízható üzleti vállalkozásoknak” ítélnék meg!

Végezetül, ha mindez nem lenne elég, akkor a szolgáltatásunkat bármelyik pillanatban felfüggesztheti vagy korlátozhatja. Tehát, adataink ott ragadhatnak a Google szerverein, még törölni sem tudjuk ezeket ilyen esetben!

Összességében, a Google ÁSZF fentebb idézett része lehetőséget ad saját magának, hogy szinte bármilyen célra felhasználja feltöltött adatainkat. Nos, akkor vállalatok esetében miért is mernénk ilyet használni?

Alább közlöm az Amazon feltételeit eredeti nyelven, az érdekesség és megbotrántoztatás kedvéért:

*„3.3 **Our Use of Your Files to Provide the Service.** We may use, access, and retain Your Files in order to provide the Service to you and enforce the terms of the Agreement, and you give us all permissions we need to do so. These permissions include, for example, the rights to copy Your Files for backup purposes, modify Your Files to enable access in different formats, and access Your Files to provide technical support. Amazon respects your privacy and Your Files are subject to the [Amazon.com Privacy Notice](#).”*