

TDK dolgozat

Váradi József

Adatvédelem a számítási felhőben

Konzulens: Dr. Racskó Péter

Váradi József

Budapesti Corvinus Egyetem

Gazdálkodástudományi Kar

Alapképzés

Gazdaságinformatikus szak

II. évfolyam

2012. március 26.

REZÜMÉ

A cloud computing megjelenése, és elterjedése után napjainkban nagyon fontos kutatási kérdésként merül fel az adatvédelem a felhőben (privacy in cloud computing), hiszen ez az a tényező, ami a számítási felhő elterjedésének gátját képezi. Dolgozatomban bemutatom a felhő fogalmát, azt, hogy milyen típusai (szolgáltatásai), milyen telepítési modelljei léteznek, és mire is használják a felhőt. Majd IT biztonságtechnikai nézőpontból vizsgálom meg a témát, nevezetesen, egy elméleti alapként bemutatom az IT adatvédelmi elvárásait és ez alapján megnézem, hogy milyen fenyegetettségeket vet fel a cloud fogalma, ebből kifolyólag milyen biztonsági elvárások vannak vele szemben. A dolgozat végén az állami szabályozások, törvények különböző változatait mutatom be és elemzem. Végül, a kutatás és a dolgozat összegzéseként egy lehetséges irányt határozok meg a felhő fejlődésének.

ABSTRACT

After the emergence and spread of cloud computing, nowadays a very important research question is raised: the privacy in cloud computing. This is the factor which makes a barrier to the spread of the cloud. In my thesis I present the concept of cloud, what kind of services (types) it has, what kind of deployment models exist and what it is used for. Then I will investigate IT security perspective: first I present a theoretical basis for the privacy expectations of IT, then I will use it to take a look at what kind of threats the cloud concept raises and what are the defense requirements against these. At the end of my study I will present and analyze different state regulations, laws. Finally, at the summary of the research I will pose a possible direction in the cloud development.

TARTALOMJEGYZÉK

1	TÉMAFELVETÉS ÉS CÉLKITŰZÉS.....	1
2	BEVEZETÉS.....	1
3	MI A SZÁMÍTÁSI FELHŐ (CLOUD COMPUTING)?	2
3.1	Mit jelent maga a fogalom?	2
3.2	Milyen típusai vannak?	3
3.2.1	<i>Software as a Service (Szoftver, mint szolgáltatás)</i>	4
3.2.2	<i>Platform as a Service (Platform, mint szolgáltatás)</i>	4
3.2.3	<i>Infrastructure as a Service (Infrastruktúra, mint szolgáltatás)</i>	5
3.3	Milyen cloud telepítési modellek léteznek?	5
3.4	Mire használhatjuk a felhőt?	7
4	INFORMÁCIÓBIZTONSÁG A FELHŐBEN.....	7
4.1	A CIA elv	7
4.1.1	<i>Bizalmasság (Confidentiality)</i>	8
4.1.2	<i>Sértetlenség (Integrity)</i>	9
4.1.3	<i>Rendelkezésre állás (Availability)</i>	10
4.2	Felhő-specifikus kockázatok, sebezhetőségek.....	11
4.2.1	<i>Kockázat, sebezhetőség</i>	11
4.2.2	<i>A felhő kockázatai</i>	12
4.2.3	<i>A felhő sebezhetőségei</i>	13
5	ADATVÉDELEM A FELHŐBEN.....	16
5.1	Mi is az adatvédelem?	16
5.1.1	<i>Adatvédelmi elmélet</i>	16
5.2	Adatvédelmi kockázatok a felhőben	17
5.3	Adatvédelmi törvények, rendelkezések	18
5.3.1	<i>Helyzet az Amerikai Egyesült Államokban</i>	18
5.3.2	<i>Helyzet az Európai Unióban</i>	21
6	ÖSSZEFOGLALÁS.....	24

TÁBLÁZAT- ÉS ÁBRAJEGYZÉK

1. ábra – A számítási felhő típusai 1.	3
2. ábra – A számítási felhő alap típusai 2.	4
3. ábra – A CIA elv modellje	8
1. táblázat – A számítási felhő telepítési modelljeinek összehasonlítása	6

1 TÉMAFELVETÉS ÉS CÉLKITŰZÉS

A dolgozatom célja, hogy közelebbről megismertessem a számítási felhő fogalmát, szolgáltatási modelljeit, és felhasználását. Bemutatom a informatika biztonsági követeléseit, a felhő kockázatait. Megvizsgálom a manapság a felhővel szemben legtöbbet felvetett kérdést: az adatvédelem témáját. Elemzem a kapcsolódó törvényeket, szabályzatokat, az Amerikai Egyesült Államokban, és az Európai Unióban egyaránt. Végül megvizsgálom a lehetséges fejlődési irányokat, hogy hová tart a számítási felhő fejlődése.

2 BEVEZETÉS

A 21. században az emberek akár informatikához közeli területen dolgoznak akár nem, biztosan van valamennyi kapcsolatuk a számítástechnikával. Bármilyen szinten is, de a számítógépek mára életünk szerves részévé váltak. Számos esetben elengedhetetlen eszköz a munkánkhoz, más tekintetben megkönnyíti hétköznapijainkat (információszerzés, kommunikáció).

Nem volt ez mindig így. Korábban nagyon nehéz volt a gépek kezelése, használatuk, karbantartásuk drága volt, és csak korlátozott számban voltak elérhetőek. A technika terjedését, azonban nem lehet megakadályozni. A technológia fejlődésével, a gyártási költségek csökkenésével, és a széleskörű felhasználhatóság miatt minden családdhoz eljutott a PC. A személyi számítógépek elterjedése miatt kialakultak a számítógép hálózatok, és később ez hívta életre az Internetet.

Az Internet mára olyan nagy kiterjedésűvé vált, hogy az emberek már nem csak otthonukban, hanem munkahelyükön, könyvtárakban, buszokon, sőt az utcán is tudnak kapcsolódni rá. Ez a széleskörű elterjedés rengeteg új ötletet, lehetőséget hozott az informatika, azon belül is az Internet világában. Nagymértékben ezek alakították ki, formálták meg azt az irányt, amerre ma az informatika tart.

Bizonyára mindenki hallott már a számítási felhő, közzismertebb nevén cloud computing fogalmáról. Ez a fogalom teljesen megváltoztatta az informatika iparát. Talán nem vagyunk tisztában vele, de meglehet, hogy munkánk során, sőt akár otthon is nap, mint nap használjuk a felhő által biztosított lehetőségeket.

Vivek Kundra az Amerikai Egyesült Államok kormányának első informatikai igazgatóját idézve: „Egy időben, minden háztartásnak, városnak, farmnak vagy falunak megvolt a saját kútja. Ma közművek biztosítják számunkra a tiszta vizet, úgy, hogy csak simán megnyitjuk a csapot. Pontosan ugyanígy működik a számítási felhő is. Mint a víz a csap-

ból a konyhánkban, úgy a cloudszoolgáltatások is be- és kikapcsolhatók olyan gyorsan, és rugalmasan, ahogy szükséges. És úgy, mint a vízmű vállalatoknál, a cloud szolgáltatónál van egy csapat szakértő, mérnök, akik garantálják, hogy a szolgáltatás, amit nyújtanak, az biztos, biztonságos és elérhető a minden nap minden percében. Amikor a csap nincs nyitva, akkor nem csak vizet spórolunk meg, hanem nem is fizetünk azért az erőforrásért, amit éppen nem használunk” (Vivek Kundra: *Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud*, [2010])

3 MI A SZÁMÍTÁSI FELHŐ (CLOUD COMPUTING)?

Ebben a fejezetben definiálom a számítási felhő fogalmát. Mivel a fogalmat, magát nagyon nehéz konkrétan meghatározni – mert sokan inkább egy-egy termékhez, szolgáltatáshoz kötik – bemutatom az USA Nemzeti Szabványosítási és Technológiai Intézetének (NIST) a felhővel szemben támasztott legfőbb elvárásait. Meghatározom a cloud szolgáltatási modelljeit, melyekre példát is mutatok, továbbá a telepítési modelljeit. Végül egy szemléletes példát hozok a cloud felhasználására.

3.1 Mit jelent maga a fogalom?

A számítási felhő fogalma azt jelenti, hogy az informatika különböző adottságait (hardver, szoftver) fizikailag nem a saját számítógépünkön érzük el, hanem, mint egy szolgáltatást, vagy terméket megvásárolva valahol egy távoli informatikai erőforrásra például számítógépre, vagy szerverre kapcsolódva vesszük igénybe. A cloud computing esetében egy cloud szolgáltató úgy biztosít alkalmazásokat, tárhelyet, adatbázisokat a felhasználói számára, hogy azoknak nem kell tudniuk, hogy az adott számítási infrastruktúra hol helyezkedik el.

Az amerikai NIST definíciója szerint a cloud computingnek öt alapvető tulajdonsága van. A kéréseket önmagától kiszolgáló (on-demand self-service): a felhasználónak egyoldalú rendelkezése van a szolgáltatások felől – mint például a hálózati tárhely – amint szüksége van automatikusan, tehát nem igényel emberi beavatkozást a szolgáltatói oldalon.

Nagy kiterjedésű hálózati elérés (broad network access): a lehetőségek a teljes hálózaton elérhetők egyszerű mechanizmusokon keresztül, ami miatt különböző vékony és vastag klienseken (például mobiltelefonok, laptopok, táblagépek és munkaállomások) is használhatjuk azokat.

Közösen kezelt erőforrások (resource pooling): a számítási erőforrásokat együttesen kezeljük – összegyűjtjük őket egy úgynevezett medencébe (poolba) – ahonnan kioszthatjuk őket a felhasználók kérésének megfelelően.

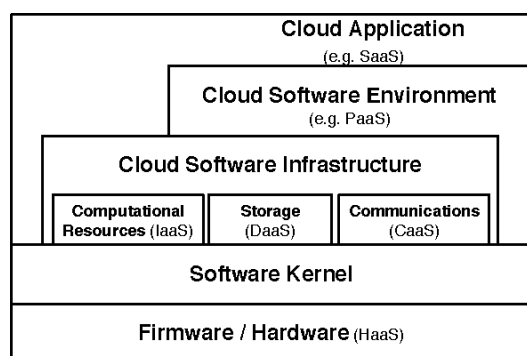
Gyors rugalmasság (rapid elasticity): a tárolási és számítási képességek gyorsan és rugalmasan rendelkezésünkre állnak; bizonyos esetben erőforrásigény szerint rögtön bővíthetjük, és amint az felszabadul, azonnal szűkíthetjük

Mérhető szolgáltatás (measured service): a cloud rendszerek a mérési képességüket felhasználva automatikusan szabályozzák, és optimalizálják az általuk biztosított erőforrások használatát (az igénybevett szolgáltatások típusának megfelelően) (*Peter Mell, Timothy Grance, [2011] 6. o.*)

3.2 Milyen típusai vannak?

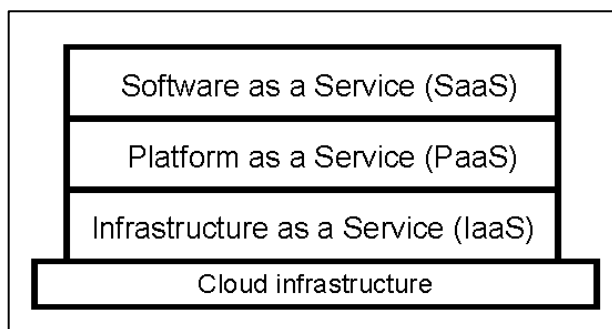
A mivel az informatika lehetőségeit nem mindenki ugyanarra a célra használja, ezért a többféle felhasználói igényre válaszul eltérő – úgynevezett – szolgáltatási modellek alakultak ki. Dr. Racskó Péter írásában egy általános betekintést ad a cloudszoolgáltatás és különböző modelljeinek kialakulásába: „A számítási felhőt, mint szolgáltatást néhány évvel ezelőtt, 2005-2007 között indították el azok a nagy multinacionális cégek, amelyek hatalmas számítástechnikai erőforrásokkal rendelkeztek saját rendszereik működtetéséhez, például az Amazon, a Microsoft, és a Google, és úgy gondolták, hogy ezeken az erőforrásokon másoknak is tudnak szolgáltatásokat nyújtani. Saját erőforrásaiknak, és üzleti érdekeiknek megfelelően más-más szolgáltatási modelleket dolgoztak ki. A szakirodalom ezeket XaaS (X as a service, ahol X sokféle jelentéssel bírhat) modelleknek nevezi.” (*Dr. Racskó Péter [2012] 5-6. o.*)

1. ábra – A számítási felhő típusai 1.



Forrás: L. Youseff, M. Butrico, D. Da Silva [2008] 4. o.

2. ábra – A számítási felhő alap típusai 2.



Forrás: J. T. Robles Hahn [2011] 28. o.

Egy 2008-as tanulmány nézőpontja szerint a cloudszoolgáltatásokat hatféle kategóriába sorolhatjuk. (1. ábra) Ez egy kicsit széttagoltabb értelmezése a már korábban említett Amerikai NIST által kidolgozott modellnek, ami szerint a cloudszoolgáltatások három halmazba sorolhatóak. (2. ábra) Ezeket a különböző hozzáférési igények mélységi tengelye mentén bontják fel. A következő részben az amerikai intézet tagolása szerint fogom bemutatni a felhő szolgáltatások modelljeit.

3.2.1 Software as a Service (Szoftver, mint szolgáltatás)

A legfelső réteg a *Software as a Service* (Szoftver, mint szolgáltatás), vagy más néven *SaaS*. A felhasználó itt, egy már teljesen kész (cloud) alkalmazást kap, amely a szolgáltató infrastruktúráján fut, ezeket többnyire internetes portálokon vagy vékony klienseken keresztül éri el. A fent említett tanulmány szerint erről a modelltől a közelmúltban bebizonyosodott, hogy sok felhasználó számára azért vonzó, mert enyhíti a felhasználókra nehezedő folyamatos működési és a karbantartási költségeket, továbbá a számítási munkát adatközpontokba exportálja, ahol a felhőalkalmazások is futnak. (L. Youseff, M. Butrico, D. Da Silva [2008] 3. o.) Erre egy elég elterjedt példa a Google által kínált levelezőrendszer a Gmail. Francisco Emanuel Liberal Rocha 2010-es diplomamunkájában nagyon jól meghúzza a határvonalat a SaaS és a többi szolgáltatási modell között: „Ebben az esetben a felhasználónak az az egyetlen érdeke van, hogy a legtöbbet hozza ki a cloud által biztosított alkalmazásból. Ezen a szinten a szolgáltató nem tekinti többé fejlesztőnek a felhasználót, számára egy egyszerű, felhasználóbarát megoldást kínál.” (Francisco Emanuel Liberal Rocha, [2010] 7. o.)

3.2.2 Platform as a Service (Platform, mint szolgáltatás)

Felülről lefelé haladva a sorban következő réteg a *Platform as a Service* (Platform, mint szolgáltatás), vagy más szóval *PaaS*. A réteg felhasználói már nem ugyanazok, az előbb

említett végfelhasználók. Itt cloud alkalmazásfejlesztők írják és telepítik a programjaikat. Platform as a Service-re egy jó példa a Windows Azure szolgáltatása. Kicsit közelebb kerülhetünk a rendszerükhöz, ha bemutatkozásukat elolvassuk a weboldalukon: A Windows Azure egy nyílt felhő platform, ami lehetővé teszi, hogy gyorsan létrehozzuk, telepítsük, és menedzseljük alkalmazásainkat a Microsoft által létrehozott adatközpontok globális hálóján. Az alkalmazásainkat ezen a felületen bármilyen nyelven, bármilyen keretrendszerben fejleszthetjük. (<http://www.windowsazure.com>) A fenti bemutatkozásból kiderül, hogy a fejlesztők teljes körűen adminisztrálhatják az alkalmazásaikat, és a hozzájuk kapcsolódó környezetet, de nem kell törődniük a mögöttes, mélyebb infrastruktúrával, melyet a szolgáltató – jelen esetben a Microsoft – biztosít számukra.

3.2.3 *Infrastructure as a Service (Infrastruktúra, mint szolgáltatás)*

A legalsó, legmélyebb réteg modellje az *Infrastructure as a Service* – magyarul Infrastruktúra, mint szolgáltatás. Az *IaaS* szintjén a szolgáltató egy virtuális számítógépet (Virtual Machine) biztosít a felhasználó részére. Itt a felhasználó maga rendelkezhet, a számára előre megszabott keretek között a nyers erőforrásokról, és csak a ténylegesen igénybe vett képességek után fizet a szolgáltatónak. Ilyen szolgáltatást biztosít az Amazon a felhasználóinak EC2 néven: az Amazon Elastic Compute Cloud (Amazon EC2) egy internetes szolgáltatás, amely a méretezhető számítási kapacitást nyújt a felhőben a fejlesztők számára. Racskó Péter összefoglalóját idézve az Amazon termékéről: „Virtuális számítógépes környezet, választható operációs rendszerrel, alkalmazásfejlesztő szoftve-ekkel, jogosultságkezelő rendszerrel, a programok futtatása tetszőleges számú virtuális rendszeren, a megrendelő által feltöltött futtatási környezetben. Létrehozhat egy virtuális gép saját alkalmazásokkal, könyvtárakkal, adatokkal, konfigurációval.” (Dr. Racskó Péter [2012] 6. o.) Visszacsatolva az első ábrán bemutatott modellhez, az alkotók bizonyos szempontok miatt külön vették az adattárolást és a kommunikációt, mint infrastrukturális lehetőségeket. Ezért szerepel az ábrájukon külön feliratként a DaaS (Data-Storage as a Service – Adattárolás, mint szolgáltatás) és a CaaS (Communication as a Service – Kommunikáció, mint szolgáltatás).

3.3 Milyen cloud telepítési modellek léteznek?

A Peter Mell és Timothy Grance által kidolgozott tanulmány egy másik csoportosítási rendszert is bemutat, ez pedig a cloud telepítési modelljeiről szól. Ez alapján, tulajdonosa-

ik szerint négy csoportba sorolhatjuk a különböző felhőket: nyilvános (public), saját (private), közösségi (community) és hibrid (hybrid).

Hogyan értelmezzük ezt a négy csoportot? Ha egy felhő nyilvános, akkor az a cloud alap-gondolata szerint, egy szolgáltató és több megrendelő kapcsolatáról szól. A szolgáltató biztosítja az igényelt cloud infrastruktúrát, a megrendelők pedig használják azt, bizonyos bérleti díjért. Ez természetesen bizonyos adatvédelmi kérdéseket is felvet a szolgáltatóval szemben, amik a dolgozat későbbi részében kerülnek majd bemutatásra.

A saját felhő ezzel ellentétben azt jelenti, hogy a tulajdonos, és a felhasználó ugyanaz az ember. Ennek persze mind előnyei, mind hátrányai is vannak. Francisco Emanuel Liberal Rocha írása alapján: Ez a megoldás költségesebb, mert a felhasználónak jelentős infrastruktúrális befektetésébe kerül, továbbá, a karbantartás és üzemeltetés díjait is ő fizeti. Persze az is igaz, hogy a nyilvános felhő előnyei, ebben a forgatókönyvben elvesztek. Elméletileg ez a modell sokkal biztonságosabb, mert nincs megosztva, és az egyetlen felhasználója, a tulajdonosa kontrolálja. *(Francisco Emanuel Liberal Rocha, [2010] 5. o.)*

A közösségi modell, nagyon hasonló a fenti sajátéhoz, csak itt a felhasználó egy közösség, tehát például egy cég, aki az üzemeltetést is saját kezében tartja. Végül pedig a hibrid cloud, ami az első két modell ötvözését foglalja magában, vagyis egy felhő, melynek bizonyos részei privát, más részei pedig nyilvános modell szerint működnek.

1. táblázat – A számítási felhő telepítési modelljeinek összehasonlítása

	ki menedzseli	infrastruktúra tulajdonosa	dedikált hardver
Nyilvános (public)	felhőszolgáltató	felhőszolgáltató	nem
Saját (private)	vállalaton belül	vállalaton belül	igen
Közösségi (community)	felhőszolgáltató	felhőszolgáltató	igen
Hibrid (hybrid)	vegyes	vegyes	a szolgáltatóval aláírt szerződéstől függ

Forrás: Joep Ruiter, Martijn Warnier [2011] 4. o.

3.4 Mire használhatjuk a felhőt?

Miután megismertük a fogalmat magát, talán világos lehet mire is használják magát a felhőt. Erre a kérdésre egy szemléletes példával válaszolnék Jonathan Strickland cikkéből: „Tegyük fel, hogy egy nagyvállalat vezetői vagyunk, és a speciális feladataink közé tartozik az, hogy minden alkalmazottunk számára biztosítsuk a megfelelő hardveres és szoftveres erőforrásokat, ami a munkájukhoz szükséges. Nem elég csak megvásárolni mindenki számára egy számítógépet, meg kell vinned a szoftvereket, illetve a szoftverek licenszét is, hogy az alkalmazottaknak meglegyenek a munkájukhoz szükséges eszközök. Amikor felveszel egy új embert, akkor újabb szoftvereket kell vinned, vagy meg kell bizonyosodnod, hogy a jelenlegi licensz elég még egy felhasználó számára.

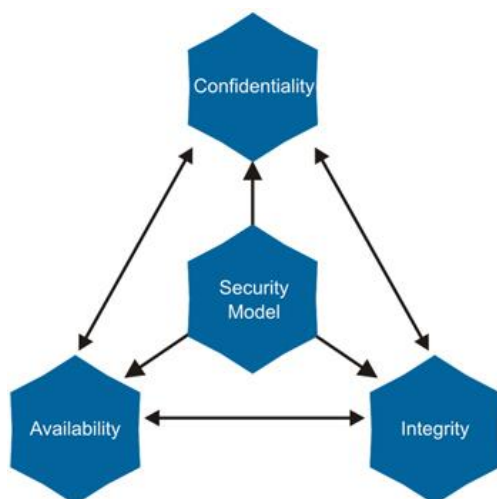
Mára van egy másik alternatíva az ilyen vezetőknek, mint amelynek helyébe képzeljük magunkat. Ahelyett, hogy egy sor szoftvert kellene installálni minden PC-re, csak be kell tölteni egy alkalmazást. Ez az alkalmazás lehetővé tenné a dolgozóknak, hogy bejelentkezzenek egy web-alapú szolgáltatásba, amely a munkájukhoz szükséges összes programot szolgáltatja. A távoli gépeken – amelyeket egy külsős cég biztosít a vállalatunknak – minden program elérhető, az e-mail klientsztól kezdve a szövegszerkesztőkön át az összetett adatfeldolgozó programokig. Ezt a szolgáltatást hívják cloud computingnak, és ez megváltoztatta a teljes informatikai piacot.” (*Jonathan Strickland, [2008]*). A példa nagyon jól alátámasztja a szolgáltatási modellek különválását. A felhasználókat egyértelműen kategorizálhatjuk munkakörük vagy pozíciójuk alapján, amiből következik az is, hogy mindenkiről tisztán megmondható, hogy milyen erőforrásokkal fog dolgozni.

4 INFORMÁCIÓBIZTONSÁG A FELHŐBEN

4.1 A CIA elv

A következő részben az információbiztonság legfőbb előírásáról, vagyis a CIA elvről írok. Ez a betűszó, az angol Confidentiality (Bizalmasság), Integrity (Sértetlenség) és Availability (Rendelkezésre állás) szavak kezdőbetűiből épül fel. Bemutatom azt a három faktort, ami egy információs rendszer általános biztonsági pillérének tekinthető. A témakörhöz kapcsolódó ábrák általában egy háromszög csúcsain ábrázolják a fogalmakat, ezzel is szemléltetve azt, amit az elv megfogalmaz: a biztonság ugyanolyan mértékben függ bármelyik tényezőtől, és bármelyik tényező hiánya egyformán sebezhetővé teszi a rendszert. Szót ejtek az elvhez szorosan kapcsolódó néhány más fogalomról, mint az hitelesítés (autentikáció), az engedélyezés (autorizáció) és az elszámoltathatóság.

3. ábra – A CIA elv modellje



Forrás: <http://www.irevna.com/compliance-and-infrastructure.html>

4.1.1 Bizalmasság (Confidentiality)

A bizalmasság kifejezés jelen esetben arra vonatkozik, hogy csak az arra felhatalmazott emberek és rendszerek férjenek hozzá a védett adatokhoz, a számunkra fontos információhoz. Különösen fontos ez a felhőben, ahol – mint ahogyan azt már az előző fejezetből megtudhattuk – a típustól, és telepítési modelltől függően nagyszámú felhasználó tevékenykedik egy szolgáltató infrastruktúráján. Azzal, hogy az adatainkat a felhőbe helyezzük, sokkal több mindenki számára lesznek elérhetőek. Többek között ez is hozzájárulhat az azok kompromittálódásához.

Az Addressing cloud computing security issues (A cloud computing biztonsági kérdéseinek kezelése) című dolgozatban az írók a felhő szempontjából a bizalmasságot két fő részre osztják, adatok bizalmasságára, és szoftver bizalmasságra. Az előbbi tulajdonképpen az elemekhez, mint például a memória, eszközök, szoftverek való hozzáférés ellenőrzésének a kérdését veti fel. Erre való az elektronikus azonosítása folyamata, ami létrehoz egy bizalmas csatornát a felhasználói egyedek és az információs rendszer között. (Dimitrios Zissis, Dimitrios Lekkas, [2010] 4. o)

A adatok bizalmassága a felhőben szorosan összefügg a felhasználói hitelesítéssel. A hitelesítés, vagy más szóval autentikáció szemléletesen egy kérdéssel jellemezhető: Honnan tudom, hogy az vagy, akinek mondd magad? Ezt a kérdést a mai elméletek szerint több módon is megválaszolhatjuk. A legelterjedtebb hitelesítési módszerek a valami, amit tudsz (jelszó), valami, amid van (kulcs, digitális tanúsítvány), valami, ami vagy (felhasználói azonosító, ujjlenyomat) és végül ahol vagy. Az erős hitelesítés hiánya a felhőkben

felhasználói fiókok jogosulatlan hozzáférésehez vezethet, ami egy rés az adatvédelem pajzsán.

A szoftver bizalmassága ugyanolyan fontos, mint a fentebb bemutatott adatbizalmasság. Ez a kifejezés arra a bizalomra vonatkozik, hogy az egyes alkalmazások, folyamatok, biztonságos módon kezelik és tartják karban a felhasználó személyes adatait. A felhőben a felhasználónak át kell ruháznia a „bizalmát” azokra az alkalmazásokra, amelyeket az infrastruktúrát szolgáltató szervezet üzemeltet. A szoftvereknek, melyek kapcsolatban állnak a felhasználó adataival feltétlenül tanúsítaniuk kell, hogy nem vetnek fel semmilyen további titoktartási és adatvédelmi kockázatokat. A felhőszolgáltató teljes mértékben felelős azért, hogy az általa nyújtott felhő olyan biztonságos legyen, hogy garantálja a felhasználók számára az adatvédelmet. (*Dimitrios Zissis, Dimitrios Lekkas, [2010] 4. o*)

4.1.2 Sértetlenség (Integrity)

Az információbiztonság következő fontos kérdése a sértetlenség, idegen szóval integritás. A sértetlenség szó a modellben az információk teljességének és pontosságának megőrzésére utal. Gyakorlatban azt jelenti, hogy a különböző elemeket (adat, szoftver, hardver) csak az arra jogosult személyek módosíthatják, illetve csak az engedélyezett módon módosíthatják. Az jogosultság kezelés, engedélyezés (autorizáció) kérdése a hitelesítésre építve azt mondja ki, hogy: Rendben, az vagy, akinek mondd magad, de mihez vannak jogaid? Az autorizáció az a mechanizmus, amely alapján egy rendszer meghatározza, milyen szintű hozzáférést adjon egy adott felhasználónak a bizalmas erőforrásokból.

Az előzőleg bemutatott tanulmány alapján (Addressing cloud computing security issues) elemzem az integritás kategóriáit. Az adatintegritás jelentése: megvédeni az adatokat a jogosulatlan törléstől, módosítástól, és létrehozástól. Ehhez szükséges a felhasználók hozzáféréseinek és jogainak szabályozása, ami garantálja azt, hogy az értékes adatokkal és szolgáltatásokkal nem élnek vissza, nem lopják el, és nem használják azokat jogellenesen. Mivel a felhőben a felhasználók és a rendszer elérési pontjainak száma nagy, ezért döntő fontosságú az, hogy csak a megfelelő jogokkal rendelkező egyedek kerülhessenek kapcsolatba az adatokkal. A szabályozások által jobb rálátást nyerünk arra is, hogy ki vagy mi változtatta meg a rendszer adatait. Ez az egyik potenciális tényezője a sértetlenségnek, az elszámoltathatóság. (*Dimitrios Zissis, Dimitrios Lekkas, [2010] 4. o*)

Az elszámoltathatóság alapja, hogy a felhasználók ugyanúgy felelősek tetteikért a rendszeren belül, mint a való életben. Az elv szerint biztosítani kell azt az ellenőrzési folyamatot, ami követi a felhasználó tevékenységeit a rendszerben. Miért tartják ezt az

autentkáció és autorizáció mellett a harmadik biztonsági szempontnak? Az elszámloltathatóság funkciója, hogy monitorozza, hogy a rendszerbe belépett entitás engedélyezett vagy nem engedélyezett tevékenységet folytatott e.

Dobromir Todorov könyvében található gondolata így hangzik: A felhasználók kaphatnak engedélyt, egy bizonyos erőforrás eléréséhez. Ha hozzáférnek ahhoz, akkor a rendszernek vagy az alkalmazásnak biztosítani kell egy ellenőrzési vonalat, amely szerint a felhasználó cselekedetei – mikor és hogyan használta az adatokat – teljes mértékben visszakövethetőek. Másrészről, ha egy felhasználó megpróbál hozzáférni olyan erőforráshoz, amelyhez nincs joga, szintén kell legyen egy ellenőrzési nyomvonal, amely alapján megállapítható a szándék miszerint a rendszer által rá kiosztott jogosultságokat és bizonyos esetekben a hitelesítési szabályokat megszegi. (*Dobromir Todorov, [2008] 8-9. o*)

A szoftver sértetlenség az alkalmazás védelmét biztosítja törlés, módosítás, lopás ellen. Fontos megjegyezni, hogy mind a törlés, mind a módosítás lehet szándékos vagy nem szándékos. Például egy elégedetlen munkavállaló valószínűleg szándékosan módosítana egy programot hogy, az leálljon, ha bizonyos feltételek teljesülésekor, vagy bizonyos idő elérése után. A felhőben a szoftver sértetlensége miatti felelősség a szoftver tulajdonosát vagy adminisztrátorát terheli. A hardver és hálózati sértetlenség olyan további kérdés, amellyel a felhőszolgáltatónak kell foglalkozni, úgy ahogy az is az ő felelősségét képi, hogy az általa használt hardvert megvédje a lopástól és módosítástól. (*Dimitrios Zissis, Dimitrios Lekkas, [2010] 4. o*)

4.1.3 Rendelkezésre állás (Availability)

Rendelkezésre állásnak nevezzük egy rendszernek azt a tulajdonságát, hogy a jogosult felhasználó kérésre az információ és a szolgáltatások bármikor elérhetőek, és használhatóak legyenek. Mint ahogyan az előző pilléreknél is, ennél a fogalomnál is elkülönítünk többféle rendelkezésre állást. A fogalom vonatkozhat adatra, alkalmazásra és még hardverre is.

Dimitrios Zissis és szerzőtársának tanulmánya szerint, a rendelkezésre állás fogalmához az is hozzátartozik, hogy a rendszer képes legyen műveletek elvégzésére, folytatására akkor is, ha a jogosultságkezelés nem megfelelő viselkedést mutat, vagy ha egy lehetséges biztonsági rés jelentkezik. Napjainkban a felhasználók teljesen mértékben bíznak a hardveres infrastruktúrában, ezzel még jobban erősítik kötődésüket a mindenütt jelen levő hálózathoz, és annak rendelkezésre állásához. A hálózati terhelés nagy részét általában az adatok feldolgozása és visszakeresése adja, ezért a cloud szolgáltatónak garantálnia kell

azt, hogy az információ és az információ feldolgozás bármikor elérhető legyen az ügyfelek számára. A cloudszoolgáltatások nagymértékben építenek az infrastruktúrára és a hálózatra, ezért is kiemelten fontos megérteni, majd tisztán dokumentálni a felhasználói (speciális) igényeket, mivel később erre alapszik majd a rendszer, és annak rendelkezésre állási feltételeit is ezekhez az igényekhez kell igazítani. (*Dimitrios Zissis, Dimitrios Lekkas, [2010] 4. o*)

4.2 Felhő-specifikus kockázatok, sebezhetőségek

Az előző részben egy általános képet kaphattunk az információbiztonság követelményeiről. De hogyan tudjuk ezeket az információkat levetíteni a dolgozat központi témájára a cloud computingra? Ebben a részben bemutatom a számítástechnikai felhő néhány kockázatát, és bizonyos sebezhetőségeit. Elsőként, nézzük át a kockázat, és a sebezhetőség definícióját.

4.2.1 Kockázat, sebezhetőség

Kockázat: „Egy esemény valószínűségének és következményének kombinációja.” (<http://www.idesol.hu/fogalomtar/informatika.html>) „A biztonság fogalma pozitív irányból közelíti meg az elérni kívánt állapotot (Mit szeretnék?), ezzel szemben a kockázat az ellenétes oldalról közelít (Minek a bekövetkezését szeretném megakadályozni? Mi ne történhessen meg?). A kockázat gyakorlatiasabb szemlélettel egy rendszert fenyegető veszélyeket veszi számba, és az általuk okozott károkat próbálja megbecsülni, összegezni. A kár értéke nagyon sok esetben nem könnyen meghatározható, pénzben nehezen számszerűsíthető, hiszen pl. egy információ elvesztésénél nemcsak az újbóli megszerzésének költsége merül fel, hanem áttételes károk is (illetéktelen kezekbe kerülése, ennek következtében a fogyasztók, felhasználók bizalom vesztese, ebből adódó presztízavesztések).” (*Berényi Melinda [2005] 10. o.*) „Az egyes fenyegető tényezők egymáshoz viszonyított kockázatbecslése azért az informatikai biztonság területén is jól kijelöli azon leggyengébb láncszemeket, ahol a védelmet célszerű erősíteni.” (<http://sdt.sulinet.hu>)

Sebezhetőség: A The Open Group nevű szervezet Risk Taxonomy című tanulmányában így definiálja a fogalmat: A sebezhetőség annak a valószínűsége, hogy az alany nem lesz képes ellenállni a fenyegetési tényezőnek. Sebezhetőség akkor alakulhat ki, amikor a fenyegetési tényező által alkalmazott hatóerő, és az alany védekezési képességének ereje eltérő nagyságúak. Ez alapján a két fő faktor, ami befolyásolja a sebezhetőséget a fenyegetettséggel szembeni ellenálló képesség és a szabályozási erő. (*The Open Group, [2009]*)

10. o.) „A rendszer biztonsági követelményeiben, tervezésében, implementációjában, vagy üzemeltetésében fellelhető olyan gyengeség, vagy hiba mely véletlenül kiváltható vagy szándékosan vissza lehet vele élni, és a rendszer biztonsági irányelvének megsértését vonja maga után.” (<http://www.idesol.hu/fogalomtar/informatika.html>)

4.2.2 A felhő kockázatai

Tekintsük át a cloud kockázatait. A felhőben a felmerülő kockázatok egyrésről a felhő jellemvonásaiból másrésről a szolgáltató hiányosságaiból erednek. A szolgáltatás felhő jellemvonásai alatt értem, az Internet, mint környezet kockázatait (kapcsolat kérdései) és emellett a böngészők, szerverek, kliensek kockázatait (titkosítás, terhelhetőség). A másik kategóriába a szolgáltató erőforrás gazdálkodási elvei, adatmenedzselési politikája és jogi szabályozottsága merül fel, mint kockázat.

Dr. Racskó Péter 2012-ben megjelent tanulmányában több példát hoz az említett kategóriákra, ezeket a fentebb már bemutatott szempontok szerint rendezem csoportokba. Elsőként nézzük a cloud jellemvonásaiból eredő kockázati tényezőket:

1. Adatok elfogása átvitelkor: „A számítási felhőben feldolgozott adatok mind az input, mind az output esetén többnyire a nyílt interneten közlekednek. Meg kell oldani az adatátvitel védelmét, ez csökkentheti a kockázatot.” (Dr. Racskó Péter [2012] 9. o.)
2. Adatszivárgás: „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 felhasználókhoz kerül.” (Dr. Racskó Péter [2012] 9. o.)
3. DDoS EDoS: „A számítási felhő webes szolgáltatás, ez pedig érzékeny az elosztott szolgáltatásmegtagadásos (Distributed Denial of Service), illetve a gazdasági szolgáltatásmegtagadásos (Economic Denial of Service) hackertámadásokra, azaz ha hackerek olyan tömegű szolgáltatást igényelnek a szervertől, amely azt jelentősen lelassítja, vagy a szolgáltatást meg is tagadhatja. Ennek gazdasági változata az, amikor a szolgáltatásmegtagadásos támadás célja az, hogy egy szereplőnek gazdasági kárt okozzon.” (Dr. Racskó Péter [2012] 9. o.)
4. Szkennelés: „A cloud-szolgáltatónak meg kell akadályoznia, hogy hackerek kitagadják rendszereinek támadhatósági pontjait.” (Dr. Racskó Péter [2012] 9. o.)

A jellemvonások elemzése után, térjünk át a szolgáltató hiányosságaiból, cselekedeteiből, működéséből kifolyó kockázatokra, vagyis a cloud egy következő érdekes kérdésére, a felhőszolgáltató vállára nehezedő felelősségekre.

1. Belső (alkalmazott általi) támadás: „Hogyan védi meg megrendelőit a cloud-szolgáltató a saját munkatársai részéről történő adatlopástól vagy adatmanipulációtól?” (Dr. Racskó Péter [2012] 8. o.)
2. Erőforráshiány: „A megrendelő abban a tudatban köt szerződést a cloud-szolgáltatóval, hogy bármilyen erőforrásigényt azonnal ki tud elégíteni. Bár az erőforrások hiánya nem túl valószínű, mert a jelenlegi cloudszolgáltatók erőforrásai igen jelentősek, ez a kockázat sem zárható ki.” (Dr. Racskó Péter [2012] 8. o.)
3. Hibás (hardver) szeparálás: „A különböző megrendelők által használt virtuális gépek többnyire ugyanazon a hardveren futnak. Mennyire lehet biztos egy megrendelő abban, hogy a „társbérlő” nem próbálja megszerezni az ő adatait? E tekintetben csak a cloud szolgáltató biztonsági eszközeiben bízhat, amelyekre semmilyen befolyása nincs.” (Dr. Racskó Péter [2012] 8. o.)
4. Nem biztonságos vagy nem hatékony az adatok megsemmisítése: „Ha az adatokat nem olyan technológiával törlik, hogy visszaállításuk lehetetlenné váljon, akkor a virtuális környezetben egy más felhasználó esetleg elolvashatja a nem jól törölt fájlokat.” (Dr. Racskó Péter [2012] 9. o.)
5. Jogi körülmények: „A számítási felhőt nem szabdalják fel az országhatárok. A szolgáltató gazdasági és biztonsági megfontolásokból sok országban helyezi el adatfeldolgozó központjait. A különböző országok jogrendje lényegesen eltér például az adatvédelemben. Egy EU-s országban érvényes adatvédelem lényegesen erősebb lehet, mint egy nem EU-s tagországban.” (Dr. Racskó Péter [2012] 9. o.)

4.2.3 A felhő sebezhetőségei

Több – a témában kutató – ember feltette már előttem a kérdést, hogy mitől mondhatunk valamilyen sebezhetőséget felhő specifikusnak? Erre a kérdésre B. Grobauer, T. Walloschek és E. Stöcker próbálta megfogalmazni a választ – a szerzők tanulmányukban részletesen kifejtik a kategóriákat, példákat is mutatnak rájuk; a könnyebb megértés érdekében én is bemutatok röviden a csoportokat. Egy sebezhetőséget cloud specifikusnak mondunk, ha legalább az egyik igaz rá az alábbi mutatók közül:

1. lényeges vagy elterjedt a számítási felhő alapvető technológiájában

A számítási felhő alapvető technológiáinak – webes alkalmazások, virtualizáció, kriptográfia – vannak olyan sebezhetőségei, melyek lényegesen technológia szempontból, vagy elterjedtek a technológia korszerű kivitelezésében. Például: virtuális gépből (környezetből) kiszökés lehetősége, munkamenet eltérítés, bizonytalan/elavult titkosítás.

2. az oka a NIST által megfogalmazott alapvető felhőjellemzők között található

A dolgozat elején már bemutatattam a NIST által felsorolt, alapvető felhőtulajdonságokat, de ismétlésként tekintsük át ezeket még egyszer: a kéréseket önmagától kiszolgáló, nagy kiterjedésű hálózati elérés, közösen kezelt erőforrások, gyors rugalmasság, mérhető szolgáltatás. Vannak sebezhetőségek, melyek oka egy vagy több tulajdonságban rejlik, néhány esetet például véve: jogosulatlan hozzáférés a menedzsment felülethez, internet protokoll sebezhetőségek, adat visszanyerés sebezhetősége, mérés számlázás kijátszása.

3. a felhő innovációban kipróbált és tesztelt védelmi szabályozás nehéz vagy lehetetlen végrehajtása okozza

Az alapvető biztonsági ellenőrzésekkel kapcsolatos sebezhetőségeket felhő specifikusnak kell tekinteni akkor, ha a cloud innovációk közvetlen nehézségeket okoznak az ellenőrzések végrehajtásában. Példának okáért: nem elég hálózat-alapú ellenőrzés a virtualizált hálózatokon, gyenge kulcskezelési eljárások, a biztonsági mutatók nincsenek a felhő erőforrásaihoz igazítva.

4. elterjedt a létesített korszerű felhő ajánlatokban

Ha a biztonsági rés elterjedt a legkorszerűbb felhő kínálatokban, akkor azt felhő-specifikusnak kell tekinteni. Legelterjedtebb példák ma a „befecskendezés” sebezhetőség (SQL befecskendezés, parancs befecskendezés, cross-site scripting) és a gyenge hitelesítési rendszerek.

(B. Grobauer, T. Walloschek, E. Stöcker [2010] 5. o.)

Az elméleti bemutatás után nézzünk meg néhány valós esetet, példát napjainkból. Jose Tomas Robles Hahn, Biztonság, adatvédelem és Cloud computing (Security, Privacy and Cloud Computing) című munkájában találhatunk néhány példát biztonsági résekre a felhőben, a következő részben, én is ezeket az általa bemutatott példákat fogom részletesen bemutatni.

A cloud szolgáltatók nem biztosítanak titkosítást a felhasználóknak. Az imént bemutatott tanulmány két olyan mindennapi problémát mutat be, amit szemfülesebb felhasználók az internetet böngészve már talán észrevettek. A webmail szolgáltatók, mint a Yahoo! Mail

titkosítják a bejelentkezési oldalukat, majd visszatérnek sima HTTP-re. Habár ez által a jelszavaink védve maradnak, az e-mail tranzakcióink már titkosítatlan formátumban kerülnek továbbításra. (*Jose Tomas Robles Hahn [2011] 29. o.*) Egy másik példa a Facebook nevű közösségi portálhoz kapcsolódik, ahol a felhasználónak nem automatikusan kínálja fel az oldal a HTTPs protokoll használatát, hanem azt önmagának kell beállítani, tehát ha a felhasználó nem figyelmes, vagy nem ért annyira az informatikához az adatai egyszerűen, támadók által olvasható formában kerülnek továbbításra.

De nézzük meg tömören mi is a különbség a HTTP és a HTTPS szabványok között. Míg a HTTP a teljes forgalmat titkosítatlan formában (egyszerű szövegként) küldi tovább az internet csatornáin keresztül, addig a HTTPS mögött az az ötlet áll, hogy egy biztonságos csatornát létesítsenek a nem biztonságos hálózatban; ezt úgy valósítják meg, hogy egy titkosítási és egy hitelesítési réteget (ahol a szerver tanúsítványát ellenőrizhetjük) iktatnak be a kommunikációba.

Mindenkiben felmerül a kérdés, hogy miért nem biztosítja a szolgáltató a titkosítást? Ennek több oka van. Elsőként a magasabb működési költségek: a titkosított hozzáférés több processzoridőt vesz igénybe kliensenként (felhasználónként). Tehát ahhoz, hogy ugyanannyi titkosított kapcsolatot tartsunk fent, mint titkosítatlant több hardverre van szükségünk, hogy a szolgáltatás minőségét állandó szinten tarthassuk. Ha mindemellett a szolgáltatás is ingyenes, akkor ez a tény még kevésbé ösztönzi a szolgáltatókat, hogy biztosítsák a titkosítást. Végül, de nem utolsó sorban a kereslet is egy kérdés. Amíg a felhasználók nem követelik meg a titkosítást, addig az nem is lesz nekik felajánlva. Ennek a helyzetnek az okozója az információhiány, hiszen a cloud szolgáltatók nem teszik nyíltan közzé azokat a kockázatokat, melyek alá a felhasználói adatok esnek. (*Jose Tomas Robles Hahn [2011] 29. o.*)

Adattitkosítási fenntartások. Mielőtt alkalmaznánk bármilyen adattitkosítási technológiát néhány fontos kérdést meg kell fontolnunk. A válaszok ezekre a kérdésekre majd kirajzolják az adattitkosítás határait. Első kérdés, hogy hol lesz majd tárolva a titkosító kulcs? Ha a felhőszolgáltatónál, akkor a megrendelő megfelelő bizalommal kell legyen felé, hogy nem fogja jogosulatlan célokra használni, továbbá biztonságosan fogja azt tárolni, úgy hogy ne férhessenek hozzá a hackerek. Továbbá fontos tudni, hogy a cloud szolgáltatót a törvény kényszerítheti, hogy adja ki a titkos kulcsot számára, bizonyos esetekben úgy, hogy megtiltják a megrendelő tájékoztatását erről. (*Jose Tomas Robles Hahn [2011] 30. o.*)

Második lényeges kérdés az, hogy hol lesz végrehajtva a kódolás és dekódolás folyamata? Ha a felhőszolgáltató tárolja a kulcsot, akkor a kódolás-dekódolást is ő fogja elvégezni. További kifejtést igényel az az eset, mikor az ügyfél kizárólagos birtokában van a kulcsnak. Egyrészt, ha a titkosítási és visszafejtési eljárások kizárólag az ügyfél telephelyein történnek, akkor a cloud szolgáltató biztosan nem fér hozzá a kulcshoz. Másrészt, ha a megrendelő minden egyes alkalommal, amikor adatot akar titkosítani illetve visszafejteni, átadja a kulcsot a szolgáltatónak – majd mikor az végzett a folyamattal akkor törli a kulcsot a memóriából – akkor a kulcs veszélyeztetett helyzetben van. (*Jose Tomas Robles Hahn [2011] 30. o.*)

Függetlenül attól, hogy mely választásokat hozzuk a fenti két kérdésben egy dolgot minden esetben fontos kikötnünk: A titkosítás nem egy varázsszer; a titkosított adatot korlátlanul lehet tárolni addig, amíg nem lesz elég számítási erőforrás a visszafejtéshez. És amit ma lehetetlennek gondolunk az lehetséges lesz öt-tíz éven belül. (*Jose Tomas Robles Hahn [2011] 30. o.*)

5 ADATVÉDELEM A FELHŐBEN

Miután képet kaptunk a szállítási felhő fogalmáról, az információbiztonság előírásairól és végigvettük a cloud specifikus kockázatokat, felelősségeket – ezekkel együtt azt is, hogy milyen felelősségek nehezednek a szolgáltatóra, és milyen döntéseket kell meghozzon az ügyfél, most rátérek az adatvédelem kérdésére. A dolgozat záró részében bemutatom az adatvédelem fogalmát a felhő szempontjából, az adatvédelem főbb kérdéseit, legvégül pedig különböző adatvédelmi törvények, rendelkezések előírásait.

5.1 Mi is az adatvédelem?

Az adatvédelem egyszerre egyénileg és társadalmilag hasznos. Mint egyénnek, az adatvédelem autonómiát biztosít: lehetőséget, hogy félelem és leplezés nélkül tegyük fel érzékeny kérdéseinket; képességet, hogy felfedezzük a személyiségünk és egyéniségünk különböző oldalait; hatalmat, hogy szoros kötődést alakítsunk valakivel, másokat kizárva. Az adatvédelem biztosítja a társadalom számára az egyensúlyt az egyéni szabadságjogok, és a kormány hatásköre között. Ezek alapján kijelenthetjük azt, hogy a magánélet az erős demokrácia alapvető építőeleme. (*Nicole A. Ozer, Chris Conley [2010] 3. o.*)

5.1.1 Adatvédelmi elmélet

Adatvédelmi elmélet azt mondja ki, hogy az egyének követelése határozza meg azt, hogy mikor, hogyan, és milyen mértékben legyenek (lehetnek) közölhetőek a róluk szóló

információk. Több irodalom foglalkozik az egyedüllét fizikai állapotával. Négy állapotot különítenek el: a magányt, az intimitást, az anonimitást, és az óvatosságot. A magány jelentése a fizikai elválasztás a csoporttól. Az intimitás, részvétel egy kis egységben, amely megvalósítja a csoportos („vállalati”) magányt. A névtelenség a szabadság az azonosítás és felügyelet alól – lehet információs vagy fizikai. Az óvatosság feltételezi egy pszichológiai gát létrehozását, amely megvédi az egyént a nem kívánt behatolástól. (Harry Katzan, Jr. [2010] 8. o.)

5.2 Adatvédelmi kockázatok a felhőben

A cloudszoftverek tárolhatják a fogyasztó naplóit, üzleti feljegyzéseit, fényképeit, naptárait, címjegyzégeit, orvosi leleteit, és sok más érzékeny dokumentumot is – amelyeket a fogyasztók sajátjának tekintenek. Az információk, melyet ezek a dokumentumok tartalmaznak, körülölelik a felhasználó életének minden részét – a családot és barátokat, a politikát és a vallást, érdeklődéseit és tevékenységeit – éppen ezért magas szintű biztosítást igényelnek, hogy megvédjék magánéletét és cselekvési szabadságát. (Nicole A. Ozer, Chris Conley [2010] 3. o.)

Mindemellett, a tevékenységünk a számítási felhőben – úgy, mint bármely más internetes tevékenységünk – további információkat generál, mint például, hogy melyik vásárló mikor jelentkezett be az üzletbe és honnan tette ezt, amiket a szolgáltató szintén gyűjthet rólunk. Egy konkrét eset, amikor a felhasználó bejelentkezik a Google Docs-ba a Google adatokat rögzít, a tevékenységéről (például: tárhely használat, bejelentkezések száma), a megjelenített adatokról illetve kattintásokról (például: felhasználói felület elemei, linkek), és más naplózható tényekről (például: böngésző típusa, IP-cím, dátum és idő, a cookie-azonosító). Ezen információk összegyűjtése adatvédelmi kérdéseket vet fel, akkor is, ha önálló tevékenységként történik, és akkor is, ha más cloud tevékenységgel együtt végzik. Elsőként azt a fenyegetést hordozza magában, hogy sokkal több információt fed fel a szolgáltató a fogyasztóról, mint amire gondolnánk. Az IP címekből például kideríthető az, hogy mikor és hol volt a felhasználó a belépéskor – és ki használta még ugyanazt a számítógépet – abban az esetben, ha nem otthonról jelentkezik be. (Nicole A. Ozer, Chris Conley [2010] 3. o.)

Továbbá, néhány felhőszolgáltató mellékszerződésként eladja a szolgáltatás bizonyos részeit további harmadik feleknek, akik bizonyos fokú hozzáférést kapnak személyes adatok. Egyes vállalatok, mint az Amazon, hosting szolgáltatásokat nyújtanak, vagyis lehetővé teszik más vállalatok számára, hogy használják a szervereiket webes alkalmazások

futtatásához, és tárolják rajta az adataikat; de emellett kérik azt a jogot, hogy az adatokat bizonyos körülmények között felfedhessék. (Nicole A. Ozer, Chris Conley [2010] 3. o.)

5.3 Adatvédelmi törvények, rendelkezések

A törvényben már régen felismerték a magánélet fontosságát egyrészt úgy, mint a személyes autonómia légtérét másrészt, pedig mint egy szükséges korlátot a kormány hatalmának hatókörére. A legtöbb adatvédelmi törvényt azonban évtizedekkel ezelőtt írták az Internet és a többi kommunikációs technológia eljövedele előtt. Az elavult törvények, és a gyorsan fejlődő technológia kombinációja napjainkban ellentmondásos és bizonytalan adatvédelemhez vezet. A világos és naprakész törvények, szabályozások hiánya minden érintettet károsít: a fogyasztókat, a vállalkozásokat, és a kormányt. (Nicole A. Ozer, Chris Conley [2010] 4. o.)

Azt, hogy az amerikai és az európai adatvédelmi normák eltérőek, a kormányok eltérő szerepe gazdaságban és a kereskedelmi szektor különbözősége indokolja. Az európai vállalatirányítási megközelítés a nyilvános feladatok elérése céljából megköveteli a szoros részvételt az üzlet és a kormányzat között. A kormányt aktív partnernek tekintik a nagyobb ipari résztvevők mellett, amellyel megtárgyalják a megvalósítani kívánt célokat és stratégiákat. Sőt, mi több európai döntéshozók hajlamosak arra, hogy egy szélesebb körű szerepet tulajdonítsanak az államnak, például a szociális problémák kezelésében. Ezzel szemben az amerikai döntéshozók jellemzően az úgynevezett „laissez-faire” megközelítésnek kedveztek a vállalatirányítás szempontjából; emellett kihangsúlyozták az egyéni szereplők és a piaci erők szerepét a társadalmi kihívások enyhítésében. (Lauren B. Movius, Nathalie Krup [2009] 171. o.)

A következő részben bemutatom az Amerikai Egyesült Államok, és az Európai Unió legfontosabb adatvédelmi törvényeit, szabályozásait a számítási felhőre vonatkozóan.

5.3.1 Helyzet az Amerikai Egyesült Államokban

Az Egyesült Államokban a kormány folyamatosan bővíti a felhő felügyeletét. Az amerikai kormány egyik legfontosabb jogi eszköze, amivel a felhőszolgáltatókat kényszerítheti, hogy adja át neki a felhasználók saját adatait az a harmadik fél doktrína. Egyéb vonatkozó törvények közé tartozik a Wiretap Act, az All Writs Act és a Foreign Intelligence Surveillance Act. (Jose Tomas Robles Hahn [2011] 33. o.)

Az adatvédelem alapvető polgári szabadságjog, ami mind az Egyesült Államok Alkotmánya mind pedig az egyes államok alkotmánya által védve van. A saját adatok védelme –

amely megtiltja az indokolatlan kutatást és lefoglalást, a szövetségi alkotmány negyedik módosításában található. A Legfelsőbb Bíróság döntések hosszú sorozata után kiterjesztette ezt a védelmet az otthonon túl minden olyan helyre, ahol az egyén indokoltan elvárhatja a magánszféra meglétét. (Nicole A. Ozer, Chris Conley [2010] 5. o.)

Az alkotmány negyedik módosítása a tárolók különböző formáit védi, többek között a személyes tárolókat (pénztárca), a fizikai tárolókat (széf, bérelt tároló szekrény), a személyi számítógépeket és hálózati számítógépek fájljait. Mondhatjuk, hogy a számítási felhő valójában egy modern változata egy tároló szekrénynek vagy a számítógép merevlemezének, ezért a számítási felhőfogyasztók elvárják, hogy a negyedik módosítás értelmében adataik a felhőben teljes védelmet kapjanak, és kizárják azokat indokolatlan keresések alól. (Nicole A. Ozer, Chris Conley [2010] 5. o.)

Az előző rész után nyilvánvalóan sok mindenkiben felvetődik a kérdés az online adatvédelemmel kapcsolatban, mely magába foglalja a számítási felhő adatainak védelmét is. Ezzel a kérdéssel a jogtudományban úgynevezett business record doctrine (üzleti adat doktrína) vagy, más néven third party doctrine (harmadik fél doktrína) foglalkozik. Az üzleti rekord elmélet, amely még egy pár pre-Internet korszakban (az internet elterjedése előtt) felmerült legfelsőbb bírósági ügy idején alakult, úgy tartja, hogy nincs ésszerű magyarázat az adatvédelemre abban az esetben, mikor egy egyén információt ad egy üzleti harmadik fél számára. A személy így lemond kizárólagos ellenőrzési jogáról az információ felett, és vállalja a kockázatot, hogy a harmadik fél ezt az információt önként továbbadhatja, és így már ésszerűen nem tekintik az információt privátnak. Ez alapján, az elmélet alapján a törvény végrehajtók azt állították, hogy az online tevékenységek adatait nem védi a negyedik módosítás. (Nicole A. Ozer, Chris Conley [2010] 6. o.)

A kérdés mindmáig nem egyhangúan tisztázott jogi körökben. A alkotmány ellenére jogászok, bíróságok továbbra is megosztott véleményen vannak. Tovább bonyolítja a helyzetet az, hogy az állami alkotmányos védelem is alkalmazandó, ha a szövetségi alkotmányos védelem nem. Ebből kifolyólag a kaliforniai Legfelsőbb Bíróság kifejezetten elutasította a harmadik fél doktrína korlátozásait a magánélethez való joggal szemben. Így az adatvédelem a cloud computing felhasználó számára eltérhet attól függően, hogy hol lakik illetve, hogy hol tárolódnak az adatai. (Nicole A. Ozer, Chris Conley [2010] 6. o.)

Habár jogi tájon zavarosnak tűnhet a kérdés, a felhasználói elvárások az alkotmányos adatvédelemmel kapcsolatban teljesen egyhangúak. Mint azt már fentebb is említettem ők a csomagmegőrző, széf, iratszekrény, merevlemez, és számítógépek modern megfelelőjének gondolják a cloudot, és elvárják, hogy az ott tárolt dokumentumok sajátok maradjak

nak, és teljes védelmet kapjanak az alkotmány negyedik módosítása, és az állami alkotmányos rendelkezések szerint. (Nicole A. Ozer, Chris Conley [2010] 6. o.)

Az alkotmányon túl szövetségi és állami törvények, jogszabályok további forrásait biztosítják az adatvédelemnek. Az ilyen törvények különösen fontosak lehetnek olyan esetekben, mint a számítási felhő, ahol a technológia folyamatosan fejlődik és az alkotmányos védelmet még nem vizsgálták gyakorlatban. Sajnos – ahogy a jelenlegi rész bevezetésében is írtam – azok közül a törvények közül, melyeknek hatása lehetne a cloudszolgáltatásokra, sokat több tíz éve írtak, még mielőtt az Internet kifejlődött volna. Ezért az általuk megfogalmazott védelem a cloud computing felhasználók számára is kérdéses. (Nicole A. Ozer, Chris Conley [2010] 6. o.)

Főleg az elektronikus távközlési adatvédelmi törvénynek (ECPA) kellene egyértelműen meghatározni – de nem teszi – a törvényes alkalmazandó védelmet a számítási felhő szolgáltatásaival kapcsolatban. Az ECPA egy szövetségi törvény, amely konkrét védelmet biztosít az elektronikus kommunikációban (az átvitel vagy tárolás területén), hogy kiegészítése a védelmet, melyet az alkotmány negyedik módosítása tartalmaz. Az ECPA nem tisztázza egyértelműen, hogy a dokumentumok, melyeket a számítási felhő szolgáltatásai által tárolunk, védettek-e egyáltalán. Az ECPA a jelenlegi verziója szerint, védelmet nyújt akkor, ha a tartalom tárolása olyan szolgáltatás segítségével történt, mely: "kizárólagos célja, tárolási vagy számítógépes feldolgozási szolgáltatások nyújtása az előfizetőknek vagy ügyfeleknek, és a szolgáltatónak nincs jogosultsága hozzáférni a tartalomhoz bármilyen szolgáltatástól (tárolási vagy számítógépes feldolgozás) eltérő kommunikáció céljából." (Nicole A. Ozer, Chris Conley [2010] 7. o.)

ECPA-on túl, léteznek konkrét adatvédelmi törvények és rendeletek, melyeknél felmerül a kérdés, hogy vajon teljes körű védelmet biztosítanak-e a számítási felhőt egyes szolgáltatásait használó fogyasztók számára. Például, a Health Insurance Portability and Accountability Act (HIPAA) célja az egészségügyi dokumentumok adatvédelme. A HIPAA azonban csak az egészségügyi szolgáltatókra, az egészségügyi elszámolási helyekre és az egészségügyi biztosítókra vonatkozik. Vonatkozik-e a HIPAA védelme a számítási felhő szolgáltatásaira, ahol a fogyasztók egészségügyi adataikat tárolják? Hasonlóképpen a Video Privacy Protection Act (VPPA) – amely a kölcsönzött video anyagok törvényi védelmét biztosítja – biztosítja-e az audiovizuális anyagok megosztásának vagy letöltésének védelmét a cloud computing szolgáltatásain keresztül? (Nicole A. Ozer, Chris Conley [2010] 7. o.)

Láthatjuk, hogy egységes adatvédelmi törvény nélkül Amerikában a fogyasztóknak maximum ágazat specifikus adatvédelmi törvények egyvelege áll rendelkezésre, hogy megvédjék jogaikat. Tekintettel a már amúgy is gyenge, és most egyre bizonytalanabb védelemre, amit az ECPA és egyéb adatvédelmi törvények nyújtanak, itt az idő most, hogy egy alapos pillantást vessenek a törvényeikre és újraírják az adatvédelmi törvény(ek)e)t, hogy lépést tartsanak a modern on-line világgal. (Nicole A. Ozer, Chris Conley [2010] 7. o.)

5.3.2 Helyzet az Európai Unióban

„Az Európai Unió az 1995-ös Adatvédelmi Irányelv megjelenése óta vezető szerepet játszik az adatvédelem területén. Ezt a vezető szerepet a cloud computing elterjedésével is szeretné megőrizni. Az EU tagországaiban a személyes adatokat az Unió Adatvédelmi irányelve (Adatvédelmi irányelv, 1995) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló irányelvek alapján kell megvédeni. Nyilvánvalóan az irányelvet kell alkalmazni a cloudszoolgáltatás igénybevétele esetén is.” (Dr. Racskó Péter [2012] 13. o.)

Az EU adatvédelmi irányelv (1995), amely 1998-ban lépett hatályba, jelenleg a leginkább átfogó és leginkább sikeres nemzetközi eszköz az adatvédelmi törvények között. (Swire & Litan [199]; Bennett & Raab [2006] idézi: Michael D. Birnhack [2008] 8. o.). Ma ez az irányelv a legnagyobb húzóerő a globalizálódó adatvédelemben. A hatálya az Európai Unió 27 tagállamára és az Európai Gazdasági Térség három tagjára (Izland, Lichtenstein, Norvégia) terjed ki. Az irányelv fő célja az volt, hogy összehangolja az adatvédelmi törvényeket, melyek az Európai Unió különböző tagállamaiban léteztek, továbbá, hogy egy egységes szabványt hozzon létre az adatvédelemre az unión belül. A tények azt mutatják, hogy egyre nagyobb hatása van; például a benne megfogalmazott EU területén kívüli mechanizmusok sikeresek, míg ezzel ellentétben más ilyen kezdeményezések elbuktak. (Michael D. Birnhack [2008] 8. o.)

A 95/46/EC irányelv a személyes adatokkal, vagy személyazonosításra alkalmas adatokkal foglalkozik. Személyes adatnak tekinthető a meghatározás szerint minden olyan információ, amely egy azonosított vagy azonosítható természetes személyhez (érintetthez) kapcsolódik. Az azonosítható személy lehet közvetlenül vagy közvetve azonosított, például egy azonosító szám illetve egy vagy több egyedi tényező – jellemzően: a személy fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális identitása – alapján. Az irányelv egyrészt az Európai Unió lakosainak adatvédelme érdekében jött létre, más-

résről, pedig hogy integrálják az uniós tagországok különböző adatvédelmi jogszabályait. Számos módja van az elv alkalmazásának, azonban az EU-s szervezetek mindenképp meg kell felelniük az alapelveknek. (Joep Ruiter, Martijn Warnier [2011] 5-6. o.)

„Az irányelv kimondja, hogy az adatvédelmet mindig az adatkezelő székhelyén érvényes törvényeknek megfelelően kell alkalmazni, akkor is, ha a feldolgozás más helyszínen történik, vagy az adatok alanyai más országban laknak. Az Adatvédelmi irányelvet kell alkalmazni, ha az adatkezelő az EU-ban székel, vagy az adatfeldolgozó eszközök az EU területén vannak, kivéve, ha az eszközök csak adatátvitelre szolgálnak.” (Dr. Racskó Péter [2012] 13. o.)

Adatkezelő: „az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.” (Dr. Racskó Péter [2012] 13. o.)

Adatfeldolgozó: „az a természetes vagy jogi személy, igazgatási vagy egyéb szervezet, amely az adatkezelő megbízásából személyes adatot dolgoz fel.” (Dr. Racskó Péter [2012] 13. o.)

Az Európai Unió törvényeinek, szabályzatainak szempontjából, az Egyesült Államok nem biztosít megfelelő védelmet az EU-s állampolgárok adatainak. Ez felveti azt a problémát, hogy az adatátvitel Európa és az Egyesült Államok között – adatvédelmi okokból – ellehetetlenül. Ennek a megoldására készült el az Európai Bizottság és az Egyesült Államok Kereskedelmi Minisztériuma által hosszan tárgyalt megegyezés: a Safe Harbor Agreement. A Safe Harbor megállapodás csak az Egyesült Államok és az Európai Unió közötti adatátvitelt részletezi, ezért kizárólag arra érvényes. Az Egyesült Államokon kívüli szervezeteknek, akik üzleti tevékenységet akarnak folytatni az EU-n belül, különböző mechanizmusokra kell támaszkodniuk, hogy megvalósítsák a Transborder Transfer principle-t (határon átnyúló (adat)átviteli elv), melyet az 1995-ös Adatvédelmi Irányelv részletez. Ez az elv megköveteli azt, hogy a személyes azonosításra alkalmas adatokat csak olyan országokba mozgathassák, amelyeket megfelelően biztonságosnak ítélnék az EU irányelve alapján. Egy amerikai székhelyű szervezetet a Safe Harbor megállapodás kötelez, ami helyettesíti a megfelelő védelmet, abban és csak abban az esetben, ha a vállalat követi a Safe Harbor Agreement-ben foglalt alapokat, és azokat közzéteszi az adatvédelmi politikájában. (Joep Ruiter, Martijn Warnier [2011] 6. o.)

„A cloud-szolgáltatás igénybevételénél az érintett ország adatvédelmi előírásainak betartásáért kizárólag a cloud-megrendelő felel. A törvények be nem tartása az adatkezelő számára szankciókkal, esetenként büntügyi szankciókkal járhat. A cloud megrendelőjének saját felelősségét a cloudszolgáltatóval kötött szerződésben célszerű részletezni, és ahol ez lehetséges, a szolgáltatótól garanciákat kérni arra, hogy az előírásoknak megfelel. Ehhez természetesen szankciókat kell társítani.” (Dr. Racskó Péter [2012] 14. o.)

Az Európai Hálózat-és Információbiztonsági Ügynökség (ENISA) 2009 végén közzétette egy cloud computingről szóló tanulmány eredményeit. Írásában kifejtette, hogy a számítási felhő egy kétélű kard jellemzőit hordozza magában biztonság tekintetében: a méretgazdaságosság és a rugalmasság a felhő alapú védelemben lehetővé teszi a szilárd, skálázható és költséghatékony biztonsági megközelítést; de a hatalmas erőforrások koncentrációja és a felhőben levő adatok viszont vonzó célpontot jelentenek a támadók számára.

A jelentés tíz-tíz biztonsági előnyt és hátrányt azonosított a számítási felhő három különböző általános használati esetére hivatkozva. A biztonsági előnyök közé sorolták az alábbiakat: méret (olcsóbb a biztonsági intézkedéseket nagyobb méreteken végrehajtani); a biztonság megjelenése, a keresleti preferenciák között; szabványosított interfészek használata a kezelt biztonsági szolgáltatások között; a felhőszolgáltató képessége, hogy gyorsan és okosan felossza az erőforrásokat; jobb lehetőségek auditokra és bizonyítékgyűjtésre; a frissítések, és az előtelepítések fejlettebb kezelhetősége; az erőforrás koncentrációval kapcsolatos biztonsági előnyök. A biztonsági kockázatok a következőket tartalmazzák: az uralom elvesztése; adat, alkalmazás és szolgáltatás rögzítettség (lock-in); elkülönítési hiba; megfelelési kockázatok (felhő szolgáltatás igénybevétele költséges tanúsításokat hoz felszínre, sőt kizárja a részvétel bizonyos piacokon). További kockázatot jelentenek: veszélyeztetett kezelőfelület (súlyosabb, ha távoli hozzáféréssel és a böngészők biztonsági részeivel kombinálják); adatok védelme; bizonytalan vagy hiányos adattörlés (nem igazi az adatok törlése); valamint a rosszakaró bennfentesek kockázata. (ENISA (2009a) idézi: N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese, P. Hopkins [2011] 26. o.)

„Az Enisa-jelentés is felhívja arra a figyelmet, hogy a számítási felhő alkalmazása szükségessé teszi az irányelvek pontosítását annak érdekében, hogy az egyértelmű szabályozás elősegítse az alkalmazást.” (Dr. Racskó Péter [2012] 15. o.)

6 ÖSSZEFOGLALÁS

A dolgozatomban bemutattam napjaink egyik legérdekesebb technológiájának a cloud computingnak a működését. Áttekintettem az informatikai adatvédelem elvárásait, ezzel együtt a számítási felhő kockázatait, sebezhetőségeit. Legvégül pedig megnéztem a cloud szolgáltatók és az kormányok felé leggyakrabban feltett kérdést, konkrétan azt, hogy milyen törvények, szabályozások védik a felhasználók adatait a felhőben.

Zárásként levonom kutatásom következtetéseit arra a kérdésre vonatkozólag, hogy hová tart a számítási felhő, mi lehet, lesz a szolgáltatásnak a jövője? Véleményem szerint a cloud szolgáltatásai a legtöbb felhasználó életét megkönnyítenék, vagy legalábbis bizonyos tekintetben leegyszerűsítenék, azonban bizonyos okokból kifolyólag mégse használja mindenki. Mik is ezek az okok? Ha az okokat csoportokba kategorizálnám, akkor ez első a törvényi szabályozások csoportja lenne, melyben az adatvédelmi törvények és a felelősség merülnének fel. Másodikként a biztonsági kérdések, ami az adatok szállítását a és a fent már leírt valamennyi felhő-specifikus kockázatot foglalná magába, és végül az üzleti okokat amelyik csoport az adatok elkülönítésére, végleges törlésére, esetleg elvesztésére utal. (*World Economic Forum [2011] 2. o.*)

Az esetek többségében ezek az okok merülnek fel a felhasználók, cégek által. Hogyan lehet megoldani a fenti kérdéseket? – merül fel mindenkiben a kérdés. A megoldás nem feltétlenül egyszerű, viszont e nélkül nem moccan előre a sem felhő előfizetőinek száma, sem a népszerűségi görbéje. Elsőként nagyon fontos az ENISA által is említett törvényi szabályozások megvizsgálása mind állami, mind szolgáltatói oldalról. Ha az állam az adatvédelmet megfelelő törvényekkel szabályozza, akkor ez által a számítási felhő a felhasználók számára biztonságos szolgáltatások halmazát fogja jelenteni, és könnyebben „adják oda” az adataikat külsős cégeknek. Ez persze nem ilyen egyszerű, ugyanis a szolgáltató(k)nak is le kell tenniük valamit az asztalra, mégpedig a megfelelőséget a törvényeknek, a megbízható, biztonságos adatközpontokat. Az adatközpontok telepítése fontos tényezőként merül fel egy szolgáltató stratégiájában. Láthattuk, hogy az eltérő szabályozások milyen mértékben korlátozzák az adatok mozgását, és a milyen szigorú feltételeket szabnak a más országokban (EU-n kívül) telepített adatközpontokkal szemben. Valószínűleg, hogy ha a nagy szolgáltatók – akik amúgy túlnyomó részt amerikai tulajdonban vannak – nem nyitnak Európai adatközpontokat, akkor nehéz lesz az ott jegyzett cégeket – akiket az Európai Jog szabályoz – a felhőbe csábítani.

Másodszor a biztonsági kérdések csoportja került fel a listára, amire talán a legnehezebb megoldást találni, hiszen a technika fejlődésével folyamatosan újabb és újabb kockázatok, sebezhetőségek jelennek meg. Ez persze nem jelenti azt, hogy a második bekezdésben részletezett egyik sebezhetőségre sincs megoldás. Ahogy említettem a titkosított (HTTPS) hozzáférés biztosításának csak anyagi vonzatai vannak.

Végül, de nem utolsó sorban az üzleti kockázatokról írok. Az üzleti kockázatok kategóriájának megoldása egyértelműen a szolgáltató felelőssége. A szolgáltatót terhelik azok a biztonsági fejlesztések, melyek lehetővé teszik azt, hogy a felhasználók, megrendelők ne léphessenek ki a virtuális környezetükből, hogy hozzáférjenek más adataikhoz, és hogy a törölt adatok visszaállíthatatlanul, tényleges törlésre kerüljenek.

A fenti szempontok teljesülése esetén van létjogosultsága a nyilvános számítási felhőnek, mint technológiának. Persze a megvalósítás nem megy egyik napról a másikra, úgyhogy az idő sem elhanyagolható szereplője a folyamatnak. Van azonban egy csak részben eltérő technológia, ami szintén jelen van, mint versenytárs. Ez pedig a saját számítási felhő. Ha a cégeknek szükségük van a felhő technológiájára, és a szolgáltatók, kormányok idővel nem tesznek azért, hogy a biztonságos cloud computing elterjedhessen, akkor a vállalatok létrehozzák majd a saját felhőjüket, ami természetesen csak bizonyos részben egyszerűsíti le a dolgozatban felvetett kérdéseket.

Merre tart a számítási felhő? Összegzésképpen úgy gondolom, a kérdésre a válasz az, hogy a számítási felhő olyan fontos technikai újítást hordoz magában, hogy mindenképp meg fog maradni a jövőben, a kérdés inkább az, hogy ki és mit fog lépni. Nevezetesen: a szolgáltatók és az államok megfogadják-e a kutatások, tanulmányok javaslatai illetve a vállalatok milyen körülmények mellett lesznek hajlandóak a felhőbe mozgatni az adataikat?

FELHASZNÁLT IRODALOM:

Ann Cavoukian: Privacy in the clouds, 2008,

<http://www.cloudhosting.co.uk/files/Privacy%20in%20the%20Clouds.pdf>

letöltve: 2012.03.24.

Berényi Melinda: Informatikai biztonsági mintaszabályzatok, 2005,

<http://www.kiszombor.hu/images/nyomtatvanyok/berenyi.pdf> letöltve: 2012.03.15.

Bernd Grobauer, Tobias Walloschek, Elmar Stöcker: Understanding Cloud-computing vulnerabilities, 2011, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5487489

letöltve: 2012.03.15.

Christopher Soghoian: Caught in the cloud: Privacy, Encryption, and Government back doors in the web 2.0 era, 2009,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553 letöltve: 2012.03.07.

Dimitrios Zissis, Dimitrios Lekkas: Addressing cloud computing security issues, 2010,

<http://www.sciencedirect.com/science/article/pii/S0167739X10002554>

letöltve: 2012.03.15.

Dobromir Todorov: Mechanics of User Identification and Authentication: Fundamentals of Identity Management, 2008

Dr. Racskó Péter: A számítási felhő az Európai Unió egén, 2012, Vezetéstudomány 1, 2-16.

Daniele Catteddu and Giles Hogben: Enisa Report: Cloud Computing – Benefits, Risks and Recommendations for Information Security, 2009,

<http://www.enisa.europa.eu/act/rm/files/deliverables/> letöltve: 2012.03.24

Francisco Emanuel Liberal Rocha: Privacy in Cloud Computing, 2010,

<http://docs.di.fc.ul.pt/jspui/handle/10455/6702> letöltve: 2012.03.04.

Harry Katzan, Jr.: On The Privacy Of Cloud Computing, 2010,

<http://journals.cluteonline.com/index.php/IJMIS/article/view/824> letöltve: 2012.03.22.

Jared Strauss, Kenneth S. Rogerson: Policies for online privacy in the United States and the European Union, 2002,

<http://www.egov.ufsc.br/portal/sites/default/files/anexos/29673-29689-1-PB.pdf>

letöltve: 2012.03.24.

Joep Ruiter, Martijn Warnier: Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice. Computers, 2011,
<http://homepage.tudelft.nl/68x7e/Papers/spcc10.pdf> letöltve: 2012.03.24.

Jonathan Strickland: How Cloud Computing Works, 2008,
<http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm> letöltve: 2012.03.04.

Jose Tomas Robles Hahn: Security, Privacy and Cloud Computing, 2011,
http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2011-05-2/NET-2011-05-2_05.pdf
letöltve: 2012.03.05.

Lamia Youseff, Maria Butrico, Dilma Da Silva: Toward a Unified Ontology of Cloud Computing, 2008, <http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf>
letöltve: 2012.03.04.

Lauren B. Movius, Nathalie Krup: U.S. and EU Privacy Policy: Comparison of Regulatory Approaches, 2009, <http://ijoc.org/ojs/index.php/ijoc/article/download/405/305>
letöltve: 2012.03.24.

Mark D. Ryan Cloud Computing Privacy Concerns on Our Doorstep, 2011,
<http://cacm.acm.org/magazines/2011/1/103200-cloud-computing-privacy-concerns-on-our-doorstep/fulltext> letöltve: 2012.03.07.

Michael D. Birnhack: The EU Data Protection Directive: An Engine of a Global Regime, 2008, http://works.bepress.com/michael_birnhack/14/ letöltve: 2012.03.24.

Miranda Mowbra: The Fog over the Grimpen Mire: Cloud Computing and the Law, 2009, www.hpl.hp.com/techreports/2009/HPL-2009-99.pdf letöltve: 2012.03.25.

Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese, Paul Hopkins: The Cloud: Understanding the Security, Privacy and Trust Challenges, 2011,
http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR933.pdf
letöltve: 2012.03.24.

Nicole A. Ozer, Chris Conley: Cloud Computing: Storm Warning for Privacy? 2010,
<http://www.dotrights.org/cloud-computing-storm-warning-privacy-issue-paper>letöltve: 2012.03.22.

Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing, 2011,
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> letöltve: 2012.03.04.

Robert Gellman: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, 2009,
http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf
letöltve: 2012.03.15

The Open Group: Risk Taxonomy, 2009,
<http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf> letöltve 2012.03.15.

Vivek Kundra: Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud, 2010, <http://www.cio.gov/pages.cfm/page/Vivek-Kundra-Testimony-on-Cloud-Computing> letöltve: 2012.03.04.

World Economic Forum: Advancing Cloud Computing: What to Do Now? Priorities for Industry and Governments, 2011, <http://www.weforum.org/reports/advancing-cloud-computing-what-do-now> letöltve: 2012.03.25.

<http://www.idesol.hu/fogalomtar/informatika.html> letöltve: 2012.03.15

<http://www.irevna.com/compliance-and-infrastructure.html> letöltve: 2012.03.15

<http://sdt.sulinet.hu> letöltve: 2012.03.15

<http://www.windowsazure.com> letöltve: 2012.03.15