RACSKÓ Péter

A SZÁMÍTÁSI FELHŐ AZ EURÓPAI UNIÓ EGÉN

Napjaink informatikai világának talán legkeresettebb hívó szava a cloud computing, vagy magyar fordításban, a számítási felhő. A fordítás forrása az EU-s (Digitális Menetrend magyar változata, 2010) A számítási felhő üzleti modelljének részletes leírását adja (Bőgel, 2009). Bőgel György ismerteti az új, közműszerű informatikai szolgáltatás kialakulását és gazdasági előnyeit, nagy jövőt jósolva a számítási felhőnek az üzleti modellek versenyében. A szerző – a számítási felhő üzleti előnyei mellett – nagyobb hangsúlyt fektet dolgozatában a gyors elterjedést gátló tényezőkre, és arra, hogy mit jelentenek az előnyök és a hátrányok egy üzleti, informatikai vagy megfelelőségi vezető számára. Nem csökkentve a cloud modell gazdasági jelentőségét, fontosnak tartja, hogy a problémákról és a kockázatokról is szóljon. Kiemeli, hogy a kockázatokban – különösen a biztonsági és adatvédelmi kockázatokban – lényeges különbségek vannak az Európai Gazdasági Térség és a világ többi része, pl. az Amerikai Egyesült Államok között. A cikkben rámutat ezekre a különbségekre, és az olvasó magyarázatot kap arra is, hogy miért várható a számítási felhő lassabb terjedése Európában, mint a világ más részein. Bemutatja az EU erőfeszítéseit is a számítási felhő európai terjedésének elősegítésére, tekintettel a modell versenyképességet növelő hatására.*

Kulcsszavak: **számítási felhő, cloud computing, informatikai közmű, kockázatmenedzsment**

Minden kisebb és nagyobb vállalkozás üzleti és különösen informatikai vezetőjében felmerül a kérdés, hogy van-e teendője a számítástechnikai felhővel kapcsolatban. Az alábbiakban erre a kérdésre keressük a választ, megpróbáljuk kiemelni a számítási felhőt a körülötte kialakult, bizonyos esetekben szándékosan kialakított „ködből". Feltárjuk valós előnyeit és az ugyanolyan súlyú, szintén valós, ellene szóló érveket. A feltett kérdésre nem tudunk egyértelmű igennel vagy nemmel válaszolni, a bemutatott érvrendszerből minden döntéshozó összeállíthatja a saját üzleti szektorának és stratégiai céljainak, tevékenységének, kockázatviselő képességének és üzleti felfogásának megfelelő részhalmazt, ami segíthet a számítási felhő alkalmazásával kapcsolatos döntésben. Mielőtt azonban elkezdenénk az elemzést, pozicionáljuk a számítási felhő modellt a világ informatikai piacán.

A globális informatikai piac volumenének becslésekor a piackutató cégek is komoly kihívásokkal küzdenek, ugyanis nehéz meghúzni a „tiszta" informatikai eszközök, a beágyazott eszközök, valamint a telekommunikáció közötti határokat. Mi sem próbálkozunk ezzel, ehelyett a nagyságrendeket érzékeltetjük. Az OECD-statisztika (OECD Key ICT Indicators, 2010) szerint a harminc legnagyobb IT-vállalat egyéves árbevétele meghaladja az ezermilliárd USD-t. Az IDC számításifelhő-kutatásai (IDC on cloud computing, 2009) szerint a nyilvános felhőből származó 2009-es bevétel a világon elérte a 16 Mrd USD-t, és 2014-ben megközelíti az 55,5 Mrd USD-t, ami éves szinten 27,4%-os növekedést jelent. A fenti adatok természetesen csak a nagyságrendek érzékeltetésére alkalmasak, de azt kimondhatjuk, hogy a számítási felhő még néhány év múlva is egy lehetséges döntési alternatíva lesz, és nem kötelező üzleti modell.

A számítási felhő régi probléma, ugyanakkor az informatika közművesítésének újabb, igen perspektivikus fejezete. Az informatika mint közmű fogalmát John McCarthy, a Princeton Egyetem tanára vezette be 1961-ben, amikor az időosztásos számítógépekről az MIT-n tartott beszédében megjósolta, hogy az informatika egyszer ugyanolyan szolgáltatás lesz, mint bármely más közmű, a víz- vagy a villanyszolgáltatás (Greenberger, 1962). Az 1960-as évek elején a számítástechnikában bevezetett időosztás tette ugyanis lehetővé, hogy egy gép egyszerre több programot is kiszolgáljon, és ez a technikai vívmány egyúttal azt is jelentette, hogy a szá-

mítástechnika, kilépve az egyetemi, kutatóintézeti, és a természetesen katonai alkalmazások köréből, képes lesz komoly üzleti, gazdasági feladatok megoldására is, előre vetítette a technológia széles körű elterjedésének lehetőségét. McCarthy víziójától még jelenleg is messze vagyunk, de az informatika közművesedése belátható távolságra került.

Az 1960-as évektől kezdve, amikor megkezdődött a számítógépek elterjedése az üzleti szférában is, a fejlődésnek két, egymással párhuzamosan futó komponensét figyelhetjük meg: az egyik a *technológia*, a másik a használati, *üzemeltetési modellek* fejlődése. A két tényező közül az egyik hol megelőzi a másikat, hol egy kissé lemarad mögötte, de már néhány év távlatában is a két faktor felzárkózik egymáshoz. Az 1960-as években és a 70-es évek elején az üzleti szférában a fizikailag is nagy terjedelmű, „komoly" számítógépek voltak a jellemzők, amelyekre a programokat a cég programozói írták, a gépeket speciálisan kiképzett operátorok működtették. Az egy-egy alkalmazáshoz szükséges adatokat fizikailag is önálló lemezeken vagy szalagokon tárolták, ezeket egy-egy program futásakor az operátorok cserélgették. A rendszerszervezők, programozók, adatrögzítők, operátorok külön kasztot alkottak egy-egy nagyobb vállalatnál, a rendszereket testre szabták, minden cégnek önálló informatikája volt.

Ez a működési modell a gépek elterjedésével egyre komolyabb fejlesztői és üzemeltetői szakemberigényt teremtett, ezzel a képzés egyetlen országban sem tudott lépést tartani. A vállalatok pedig csak kényszerűségből vállalták fel az alapvető üzleti tevékenységüktől merőben eltérő kultúrájú és működésű informatikai részlegek felállítását, és amelyek irányítása, az ott dolgozó szakértőkkel való kommunikáció sok problémát okozott. Erre a problémára mind a technológia, mind a működési modellek fejlődése kínált megoldásokat.

A számítógépgyártók egyre nagyobb hangsúlyt fektettek előbb a programok „hordozhatóságához" szükséges technikai feltételek, szabványok és eszközök kidolgozására, a kezelhetőség – mai szóval – felhasználóbarátságosság – megteremtésére, Ross Perot pedig 1962-ben megalakította az Electronic Data Systems (EDS) nevű céget, amely más vállalatok számára kívánt számítástechnikai szolgáltatásokat nyújtani. Perot koncepciója az volt, hogy ha azok a szervezetek, amelyeknek a számítógépek kezelése, a rendszerek fejlesztése és azok üzemeltetése nem a fő profiljuk (nem core business), kihelyezik ezeket a tevékenységeket egy olyan cégbe, amelynek ez a core business-e, határozottan jól járnak. Mert igaz ugyan, hogy a kihelyezett informatika folyamatos költséget jelent, de a cég mentesül a speciális szakértelmet kívánó beszerzésektől, a gépek üzemeltetésétől, a fejlesztések megtervezésétől és finanszírozásától, ehelyett szolgáltatást vásárol.

Érdekes módon az 1962-től létező (pontosabban az USA-ban létező) outsourcing-modell sokáig nem talált komoly piacra, de az okok feltárása nem ennek a cikknek a tárgya. Az outsourcing igazi nagy fellendülése a 70-es évek végén, a 80-as években következett be az USA-ban. Ezt Európa tíz év késéssel követte, Magyarországon a 90-es évekig az állami tulajdon dominált, és az állam által létrehozott Számítástechnikai és Ügyvitel-szervezési Vállalat (SZÜV) volt az outsourcing-kínálat. A piaci körülmények a 90-es években alakultak ki Magyarországon. A 90-es évek informatikája az alábbi főbb tényekkel jellemezhető:

- beszerezhetővé válnak a korábban nem importálható legkorszerűbb számítógépek, szoftverek és alkalmazások,
- általánossá válik a távoli hozzáférés a számítógépekhez,
- szervezeteken belül működő adatátviteli hálózatok épülnek ki,
- a hazai telekommunikáció felzárkózik a fejlett világ színvonalára és a hálózat alkalmassá válik a szervezetek közötti rendszeres adatkommunikációra,
- az évtized végén általánossá válik a 64-128 Kbit/sec sávszélességű internet, ekkortól beszélhetünk tényleges üzleti, illetve közigazgatási alkalmazásokról a hálózaton.

Az 1990 utáni másfél évtized az outsourcing-modell töretlen fejlődésének korszaka volt. 2000 és 2005 között az IBM, a legnagyobb outsourcing-vállalat néhány megaüzletet kötött, az IBM informatikai szolgáltatási üzletágának a csúcson, 2004-ben, a bevétele 13,1 Mrd USD volt (IBM global outsourcing revenues rise, 2005). Az AmEx-szel négymilliárd USD-s, a Deutsche Bankkal 2,5 Mrd USD-s, többéves szerződést kötöttek 2002-ben (Greenemeier, 2002).

A számítási felhő üzleti modellje

A számítási felhő mint működési modell sajátosságainak megértéséhez a továbbiakban elemezzük az outsourcing-modellt.

Az outsourcing lényege az, hogy a szervezet (vállalkozás, igazgatási szerv stb.) informatikai rendszereit részben vagy egészben egy szerződéses partner, az outsourcing-partner üzemelteti. Az eszközök tulajdonjoga e tekintetben nem lényeges, de a jellemző az, hogy a hardver és a szoftverek, vagy ezek egy része, az outsorcingpartner tulajdonában vannak. Az üzemelte-

tést és szolgáltatást végző szakemberek az outsourcing-partner alkalmazottai.

Az outsourcingcégek – minthogy ez a core üzletük, akkor tudnak gazdaságosan működni, ha egyszerre több ügyfelet szolgálnak ki. Az outsourcing fénykorában – a felmerülő biztonsági aggályok eloszlatására – bevezették a „Kínai Nagy Fal" fogalmát, amely azt jelentette, hogy egy outsourcing-szolgáltató telephelyén a különböző partnerek rendszerei, és sokszor az azokat kiszolgáló személyek is teljes mértékben elkülönültek egymástól.

Az outsourcingpartner bevonásának számos üzleti előnyével lehetett számolni, a leglényegesebbek az informatikai üzemeltetés professzionalizmusa, a beszerzési, üzemeltetési fejlesztési és a munkaerőköltségek csökkenése a méretgazdaságosság következtében. Meg kell említeni még egy, a gazdasági mutatókban nehezen kifejezhető előnyt, az informatika átláthatóbbá vált a gazdasági vezetés számára. Az outsourcing-partnerrel a megfelelő szakértelemmel megkötött szerződés tartalmazta mindazokat a minőségi és mennyiségi mutatókat, amelyek a partner teljesítményét mérték, és amelyek alapján a díjfizetés történt. Ezek a mutatók a szervezeten belül sokszor követhetetlenek voltak.

Az outsourcing fejlődési ütemét sok helyen természetesen lassította az a körülmény, hogy a kiszervezés általában ellentétes volt a szervezet informatikusainak szakmai meggyőződésével és érdekeivel, a költségek tervezhetősége, a szolgáltatás mennyiségének és minőségének mérhetősége, a skálázhatóság együttesen azonban olyan előnyt jelentettek, amelyek általában legyőzték az outsourcinggal szembeni fenntartásokat.

A fentieken kívül még további, nehezen számszerűsíthető, de a vállalati vezetők számára igencsak fontos előnyök is jártak az informatika kihelyezésével. A nagyvállalatokra, különösen a nyilvános tőzsdei cégekre jellemző, hogy a tulajdonosok erőteljesebben korlátozzák a beruházási (CAPEX), mint a működési (OPEX) költségeket. Ugyancsak erős korlátokat határoznak meg az alkalmazottak létszámára – érthető okokból. Az informatika kihelyezése ebből a szempontból ideális, mert lehetővé teszi a CAPEX és a munkaerő egy részének átterhelését a partnerre, ez utóbbinál egy jogutódlási szerződés keretében még az egyébként felmerülő végkielégítések is elkerülhetők.

Az outsourcing-szerződésekre jellemző, hogy a szolgáltató a szolgáltatás nyújtásához hardver- és szoftvereszközöket vásárolt, ezért a szerződéseket 5-7 évre, legalább az eszközök megtérülési idejére kötötték. A hosszabb szerződési idő lehetőséget adott arra is, hogy a felek olyan díjfizetési ütemezésben állapodjanak meg, amely a megrendelő pillanatnyi pénzügyi helyzetét pozitívan befolyásolta.

A skálázhatóság (leegyszerűsítve, amikor a lineáris igénynövekedéshez lineáris, vagy annál kisebb meredekségű költséggörbe tartozik) az outsourcing esetén nem volt magától értetődő, hiszen a szolgáltatónak nem volt érdeke, hogy a szerződésben rögzített teljesítmény eléréséhez szükségesnél magasabb kapacitásokat vásároljon saját kockázatra. Ehhez vagy előre kellett látni és szerződésben rögzíteni az üzlet 5-7 éves növekedési pályájához szükséges informatikai szolgáltatás mennyiségét, vagy a felek megegyezésére volt szükség a szerződéses idő alatti bővítések finanszírozási kérdéseiben. Az outsourcing-modell a skálázhatóság problémáját a technológia térferéről áttette a szolgáltatási szerződés térfelére. Tekintettel arra, hogy a szolgáltató igényt tartott az adott szerződés teljesítése érdekében vásárolt eszközeinek megtérülésére, a díjazás döntően csak fix áras lehetett, ami megnehezítette a lefelé való skálázás lehetőségét.

A felsorolt – elsősorban gazdasági – tényezők, a problémák ellenére egyértelműen motiválták a szervezeteket az informatika kiszervezésére. A vezetés számára erős érv volt a kiszervezés mellett a szabványosítás és egységesítés, amely általában az informatikai üzemeltetés „legjobb gyakorlatának" bevezetését, és ezzel költségcsökkenést jelentett a szervezetekben.

A pozitív érvek mellett számos, az outsourcinggal szembeni érv is megfogalmazódott. Ezek közül a leglényegesebbek az elköteleződés egy szolgáltató irányában, a kontrollálhatóság kérdése, a biztonság és az adatvédelem.

Az elköteleződés (lock-in) az outsourcing kapcsán kétségtelenül fennáll, de elsősorban nem technológiai, hanem üzemeltetés és folyamatszintű. Az alkalmazott technológiák túlnyomóan szabványosak, az alkalmazott hardver- és szoftvereszközök a megrendelő számára ismertek, így a rendszerek és az adatállományok viszonylag gyorsan és kevés költséggel áttelepíthetők egy másik szolgáltató hasonló eszközeire. Az üzemeltetési politika, a folyamatok és az árazás azonban egy másik szolgáltatónál lényegesen különbözhet az előzőtől, így szolgáltatóváltásnál gyakorlatilag újra kell gondolni az üzleti modellt és a folyamatokat. Például az első outsourcing-szolgáltató nem virtualizált környezetben működött, és az árazásában az egyik fő tétel az eszközök fizikai megtérülése volt, míg az újabb szolgáltató virtualizált eszközökkel működik, és a fizikai gépek megtérülése nem közvetlen.

A biztonság kérdése az informatika kihelyezésénél nem különbözik lényegesen a belső informatikai biztonságtól, leszámítva azt a tényt, hogy a statisztikák szerint a biztonság elleni támadások legnagyobb része a szervezeten belülről indul. A hagyományos

outsourcing-szerződések keretében fizikailag behatárolható, megtekinthető és a szerződésben foglaltak szerint auditálható rendszereket használnak, a megrendelő meghatározhatja a számára megfelelő biztonsági politikát és szabályozást, beleértve az azonosítást, jogosultságkezelést és elszámoltathatóságot (AAA – authentication, authorization, accountability). Az auditok (pl. COBIT, SOX megfelelőség stb.) általában ugyanúgy végrehajthatók, mint a szervezet saját maga által üzemeltetett rendszerein.

Az adatvédelmi kérdések elemzésénél a kiindulópont az egyes országok saját jogi szabályozása. Ellentétben a biztonsági kérdésekkel, ahol nemzetközileg elfogadott szabványok és kritériumok léteznek, de azt, hogy egy gazdasági szervezet mely kritériumoknak, illetve szinteknek felel meg, maga a szervezet dönti el üzleti érdekei alapján, az adatvédelmet minden szervezetre kötelező törvények definiálják. E tekintetben az Európai Unió élenjáró, az 1995-ben megjelent Adatvédelmi irányelv (Adatvédelmi irányelv, 1995) máig a személyi adatok védelmének legkorszerűbb elveit rögzíti. A magyar adatvédelmi törvény (1992. évi LXIII. Törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról) teljes egészében az EU-s irányelvre épül. Itt az adatvédelem azon kérdéseit emeljük ki, amelyek az outsourcing szempontjából érdekesek. Adatvédelmi kérdések természetesen csak abban az esetben merülnek fel, ha a szervezet saját dolgozóinak, vagy ügyfeleinek, partnereinek személyes adatait a kihelyezés keretében tárolja vagy feldolgoztatja. Az EU-s Adatvédelmi irányelv és az EU-tagországok nemzeti jogszabályai erre a helyzetre kellő eligazítást adnak, szétválasztva az adatkezelő és az adatfeldolgozó szerepét és felelősségét, meghatározzák a személyek tájékoztatásának kötelezettségét, amennyiben az adatkezelő más adatfeldolgozónak adja át a személyi adatokat. Az irányelv rendelkezik arról az esetről is, amikor az outsourcing-szolgáltató nem EU-tagországban, vagy nem az EU-s Adatvédelmi irányelvet alkalmazó jogrendű országban működik, vagy ilyen országon keresztül továbbít személyes adatokat. Az EU tagországaiban létrejött olyan informatikaifeladat-kihelyezések, amelyekben személyes adatokat is kezeltek, döntően EU-s telephelyű cégekkel, európai országokban valósultak meg, így az Adatvédelmi irányelv előírásainak betartása és ennek ellenőrzése nem okozott különösebb gondot.

Az outsourcing előnyei az informatikai szolgáltatások és költségek tervezhetőségében, az erőforrások bizonyos fokú skálázhatóságában, a beruházások és emberierőforrás-költségek működési költséggé konvertálhatóságában és az informatikai professzionalizmusban foglalhatók össze. Hátrányai a kismértékű skálázhatóság (főként a csökkenés irányában), a szállítói elköteleződés és a rugalmatlanság.

Az outsourcing-modell a továbbiakban összehasonlítási alapul szolgál majd a számítástechnikai felhő modellek elemzéséhez.

A XXI. század első évtizedének végére a technológia fejlődése új helyzetet teremtett az informatika és a kommunikáció alkalmazásában. Az új helyzet főbb attribútumai az alábbiak:

- az adattárolás költsége igen alacsony: egy gigabájt adat fillérekért tárolható,
- az adatfeldolgozási kapacitás – köszönhetően a processzorok teljesítmény/ár arány gyors növekedésének – olcsóvá vált,
- a telekommunikációs fejlesztések és a szolgáltatók erős versenye nagyon lecsökkentette az adatátviteli költségeket, egy gigabájt átvitele néhány forintba kerül,
- a szabványos és felhasználóbarát megoldások egyre nagyobb szerepet kapnak az informatikában,
- a korszerű szoftverek költsége nem csökken és növekvő arányt képvisel az informatikai rendszerekben,
- a nagy tudású, professzionális szakemberek költsége folyamatosan nő.

A számítástechnikai felhő mint szolgáltatási modell lényegében az új technológiai üzleti feltételrendszerhez jól illeszkedő szolgáltatási modell.

A számítási felhő működési modelljei

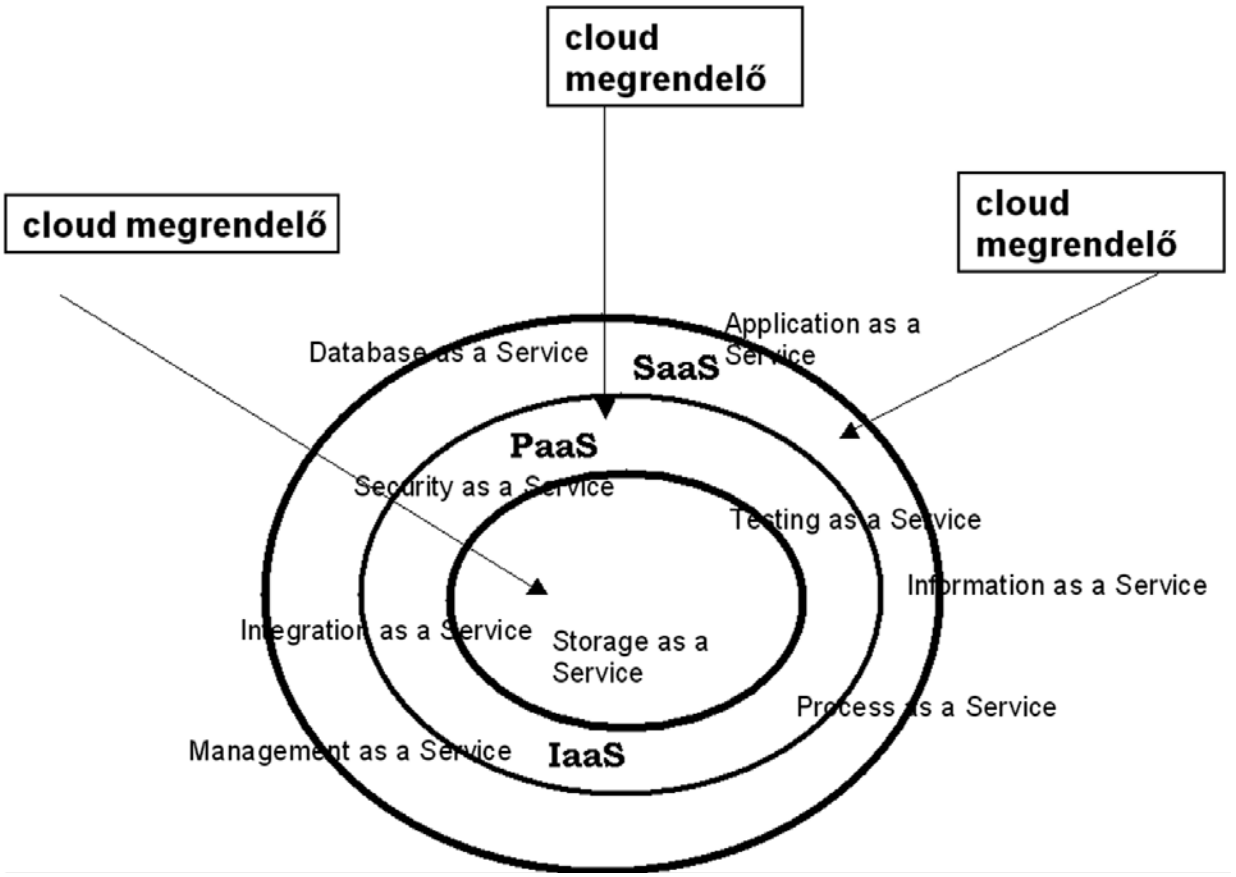
A számítási felhőre számos meghatározás létezik, a leginkább „hivatalos” a NIST (az USA Nemzeti Szabványosítási és Technológiai Intézete) alábbi definíciója:

A cloud computing olyan, a hálózatot és a hálózatra csatlakozó, könnyen konfigurálható, megosztott erőforrások (pl. hálózat, szerverek, tárolók, alkalmazások és szolgáltatások) igény szerinti elérését felhasználóbarát módon biztosító modell, amely gyorsan bevezethető és a lehető legkevesebb menedzsmenttevékenységet és a szolgáltatásszállító minimális beavatkozását igényli (Mell – Grance, 2009).

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 szakirodalomban ezeket a

1. ábra

Az XaaS különböző fajtái



modelleket XaaS (X as a Service, ahol X sokféle jelentéssel bírhat) modelleknek nevezik. Az 1. ábrán látható három alapvető modell az IaaS, vagyis infrastruktúra mint szolgáltatás, a PaaS, platform mint szolgáltatás és az SaaS, szoftver mint szolgáltatás.

Az IaaS-re jellemző példa az Amazon EC2 (Elastic Cloud Computing) szolgáltatása, ahol virtuális számítógépeket vehetünk igénybe igen rugalmas konfigurációban, a Microsoft elsősorban a .Net platformon kínál szolgáltatásokat (PaaS), míg a Google a vállalati levelezést, irodai munkát támogató eszközöket, dokumentumtárolást és szerkesztést kínálja szolgáltatásként (SaaS). A többi cloud-szolgáltató ugyanezeket a modelleket alkalmazza jelenleg. A szolgáltatások közös jellemzői az alábbiak:

- a megrendelő igen tág határok között adhatja meg, hogy milyen mennyiségű szolgáltatást szeretne igénybe venni,
- nincs lehetőség arra, hogy a megrendelő meghatározza, hogy az általa igénybe vett szolgáltatásokat milyen eszközökről és a világ mely részéről kapja,
- kizárólag az igénybe vett szolgáltatásokért kell fizetni, előre meghatározott egységárak alapján (pay per use).

A számítási felhő megértéséhez példaként nézzünk meg egy IaaS, egy PaaS és egy SaaS konstrukciót. Jelenleg a piacon nincs akkora cloud-kínálat, hogy ezeket a konstrukciókat cégektől függetlenül, típusszolgáltatásként jellemezhessük, így nem tudunk eltekinteni a szolgáltatók nevének említésétől.

Az Amazon EC2 IaaS jellemzői

Virtuális számítógépes környezet választható operációs rendszerrel, alkalmazásfejlesztő szoftverekkel, jogosultságkezelő rendszerrel, a programok futtatása tetszőleges számú virtuális rendszeren, a megrendelő által feltöltött futtatási környezetben. Létrehozható egy virtuális gép saját alkalmazásokkal, könyvtárakkal, adatokkal, konfigurációval. Használhatók a különböző menedzsmenteszközök, többféle helyszínen lehet futtatni, lehetőség van statikus IPO-címek használatára.

A szolgáltatásért csak a felhasznált erőforrások után kell fizetni. Példaként megemlítjük, hogy egy közepes kategóriájú PC-nek megfelelő teljesítményt Linux operációs rendszerrel óránként 0,085 USD-ért lehet megvásárolni. A kínálat valóban rugalmas, a kis teljesítménytől a nagyon nagy teljesítményig lehet választani, az alkalmazott alap- és egyéb szoftverek kínálata lefedi a piacvezető termékeket. A gépek kiválasztásánál figyelembe vehetjük, hogy inkább számításigényes, vagy inkább tárigényes faladatokat szeretnénk futtatni. Ismeretes, hogy munkahelyeken használt saját szerverek kihasználtsága a világon nem éri el a 8%-ot – ugyanis ezeket a gépeket általában a ritkán szükséges csúcsterhelésekre méretezik –, a személyi számítógépek kihasználtsága a 30%-ot. A szerverek esetén a működtetési költségek függetlenek a kihasználtságtól, így nem nehéz kiszámítani, hogy a „pay-per-use" modell költsége lényegesen alacsonyabb a saját üzemeltetésű infrastruktúra költségeinél.

A Microsoft Azure PaaS jellemzői

A cég virtuális gépeken a saját szoftvereinek szolgáltatásait (.Net, SQL, Sharepoint Server, CRM, Live Services stb.) és ezek integrációjának lehetőségét adja, a saját platformján. A kínált rendelkezésre állás 99,95%-os (évi 4 óra állásidő). A virtualizált gépeket számos konfigurációban lehet használni, az igényeknek megfelelően. Fizetni csak a tényleges processzor- és tárhasználatért, az adatátvitelért és a szoftverekért kell. Tekintettel az igénybe vehető szolgáltatások komplexitására, nehezen hasonlítható össze a szolgáltatásért fizetendő díj a saját beruházásban megvalósított rendszerek árával. A cég – a számítást egy webes TCO-kalkulátorral (Microsoft TCO-kalkulátor) segíti. A próbaszámítások szerint a cloud-szolgáltatással 40-50%-os TCO-megtakarítás érhető el.

A Google SaaS jellemzői

A kínálat biztonságos vállalati levelezés, 25 GB tárterület, spamszűrés, naptárkezelés, dokumentumkezelés, webhelyek, videomegosztás, ügyfélszolgálat, néhány egyéb kiegészítő szolgáltatás 99,9%-os rendelkezésre állás mellett évi ötven USD díjért. Egy kkv, sőt egy nagyvállalat sem képes ezeket a szolgáltatásokat ezzel a költséggel nyújtani. A 99,9%-os rendelkezésre állás évi maximum 8 óra állásidőt jelent, amit egy saját számítóközpont csak ezeknél a szolgáltatásoknál nem indokolt mértékű redundancia mellett képes biztosítani. Az XaaS szolgáltatások általános jellemzője az egyszerű elérhetőség, vagy böngészőből, vagy egy letölthető, könnyen kezelhető interfész segítségével használhatók.

A fenti példákból kiindulva összegezhetjük a számítási felhő mint szolgáltatás igénybevételének nyilvánvaló előnyeit:

- jelentős TCO-csökkenés,
- csak azért fizetünk, amit használunk,
- skálázhatóság felfelé és lefelé,
- nem szükséges kezdeti beruházás (CAPEX, ingatlan, EF),
- kis és nagy kapacitásokat egyaránt tudunk használni,
- mindig a legkorszerűbb technológiát vehetjük igénybe az átállás nehézségei nélkül,
- az egészen kis vállalkozások is olyan alkalmazásokat használhatnak, amelyek méretük miatt korábban a nagyok privilégiumai voltak (pl. CRM),
- a döntéstől a rendszer használatbavételéig eltelt idő lényegesen, hónapokról napokra csökkenhet,
- a szolgáltatóval kötött szerződés időtartama rugalmas.

Alacsony költségek, alacsony belépési korlát, gyors használatbavétel, rugalmas használati feltételek – mi tartja vissza az üzleti és az informatikai vezetőket, hogy azonnal szerződjenek egy cloud-szolgáltatóval?

A számítási felhő problémái

A számítási felhő nem outsourcing. Nem tudjuk, hol tárolódnak az adataink, nem tudjuk, hol vannak azok a számítógépek, amelyeken a feldolgozások futnak, nem tudjuk, kik a „társbérlőink" abban a virtuális környezetben, ahol a rendszereink futnak. A Google számos telephelyén több mint egymillió szervert üzemeltet, évi százötvenezer terabájtnyi új adattárolót épít be rendszereibe. A feldolgozást automatikus elosztó és menedzselő rendszerek irányítják, ha ezt a szolgáltatást használjuk, nincs mód arra, hogy akár földrészpontossággal behatároljuk adataink elhelyezését.

A számítási felhő abban is lényegesen eltér az outsourcingtól, hogy nem a megrendelő határozza meg a technológiát, kizárólag a szolgáltató kínálatából választhat. Minthogy az erőforrások virtualizálása a felhőben általános, a fizikai hardver és az alap operációs rendszereket a megrendelő nem is látja.

Ha a megrendelőnek a gazdálkodásában speciális megfelelőségi kritériumoknak is eleget kell tennie, vagy saját belső pénzügyi ellenőrzési rendszere megköveteli az informatikai rendszerek auditját, a felhőben ezt nem minden esetben tudja megtenni.

A számítási felhő alkalmazása nem teszi lehetővé a feleslegessé vált informatikai üzemeltető munkaerő

áthelyezését a szolgáltatóhoz, mint az outsourcing-szerződések esetén ez sokszor történt.

Az eszközök és a helyszín virtualizálódása számos biztonsági és adatvédelmi kérdést is felvet, ezekre a későbbiekben részletesen kitérünk.

Az Európai Unió a cloud alkalmazásának terén ugyanabban a helyzetben van, mint bármelyik vállalati vezető. Egyrészt a cloud alkalmazását a versenyképesség egyik jelentős mozgatóerejének tartják, másrészt viszont nem szeretne visszalépni az adatvédelem terén elért eredményektől (Kroes, 2011).

Az Enisa (European Network and Information Security Agency) mint az EU hivatala 2009-ben kutatást folytatott a vállalkozások körében a cloud kockázatainak feltérképezésére. A megjelent tanulmány (Enisa Report, 2009) összegzi azokat a kockázati tényezőket, amelyekkel a számítási felhő esetleges alkalmazásakor számolni kell.

Az Enisa jelentése a kockázatelemzést az ISO/IEC 27005: 2008 „Információs biztonság kockázatmenedzsment" szabvány szerint végzi. Az alábbiakban röviden leírjuk a kockázatok jellegét.

A szolgáltatás felhő jellegéből fakadó üzleti kockázatok

Kötődés a szolgáltatóhoz (lock-in)

Jelenleg a számítási felhő szolgáltatás kevéssé szabványos, nincsenek a szolgáltatók által egységesen alkalmazott cloud-szabványok, sokszor a rendszerek egyedi platformokra készülnek, és azokon futnak. Ezért a szolgáltató váltása hosszú, bonyolult és költséges folyamat. A „pay-per-use" árazás azt sugallja, hogy ha egy szolgáltatóval nem vagyunk elégedettek, akár másnap átmehetünk egy másikhoz. A cloud-szolgáltatók jelenlegi kínálata és a technológiák közötti különbségek ezt azonban nem teszik lehetővé.

Az irányítás elvesztése

Elvész a rendszerek feletti irányítás lehetősége. Nem mindig tisztázott a felelősségek kérdése a megbízó és a szolgáltató között. A megrendelő és a szolgáltató saját belső folyamatai, előírásai eltérőek lehetnek. A szerződések nem mindig rögzítik az SLA-szinteket és ezek mérési módszereit. A futó alkalmazások ellenőrzése sokszor nem lehetséges, így a megbízó joggal úgy érzi, hogy elveszti az ellenőrzést a rendszerei felett.

A megfelelőség biztosítása

A megfelelőség (compliance) biztosítása és az ezzel kapcsolatos minősítések szigorú ellenőrzési folyamatokat kívánnak meg (l. később). Ezek végrehajtása nem minden cloud-konstrukcióban lehetséges.

Rossz szomszédság

A virtualizáció következtében ugyanazon a hardver- és szoftverplatformon olyan felhasználók rendszerei is futhatnak, amelyek a megrendelő számára nem kívánatosak, pl. üzleti versenytársak, esetleg üzleti adatainkat féltjük tőlük.

Cloud-szolgáltatás megszűnése

A jelenlegi szolgáltatók esetében a piacról való kivonulás nem valószínűsíthető feltételezés, de ha a cloud-piac megfelelően fejlett lesz, akkor egyes cégek törvényszerűen tönkre is fognak menni.

A szolgáltatót felvásárolják

A szolgáltató harmadik fél által történő felvásárlása a megrendelő számára nem mindig elfogadható, például, ha ezt a megrendelő egy piaci versenytársa teszi. Nem egyértelmű, hogy ebben az esetben a szolgáltatónak mikor és hogyan kell tájékoztatnia a felvásárlásról a megrendelőt, van-e a megrendelőnek ebbe beleszólása, illetve ha szolgáltatót szeretne váltani (ha ez egyáltalán lehetséges), ki fizeti ennek költségeit.

Az ellátási lánc nem működik

A cloud-szolgáltató egyes feladatokat, pl. a jogosultságkezelést saját outsourcing-partnerének is kiadhatja. A harmadik fél – akinek létezéséről a megrendelőnek esetleg nincs is tudomása – teljesítménye befolyásolhatja a szolgáltatást.

A szolgáltatás felhő jellegéből fakadó műszaki kockázatok

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 cloud-szolgáltatók erőforrásai igen jelentősek, ez a kockázat sem zárható ki.

Hibás 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 cloudszolgáltató biztonsági eszközeiben bízhat, amelyekre semmilyen befolyása nincs.

Belső támadás

Hogyan védi meg megrendelőit a cloud-szolgáltató a saját munkatársai részéről történő adatlopástól vagy adatmanipulációtól? Erre sincs befolyása a megrendelőnek.

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.

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.

Nem biztonságos vagy nem hatékony az adatok törlése

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.

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.

Kriptográfiai kulcsok elvesztése

Ha a megrendelő adatainak védelmében kriptográfiai eszközöket használ, és kódolt adatokat tárol a felhőben, a kriptográfiai kulcsok elvesztése egyenértékű az adatok megsemmisülésével.

Szkennelés

A cloud-szolgáltatónak meg kell akadályoznia, hogy hackerek kitapogassák rendszereinek támadhatósági pontjait.

A szolgáltató központi eszközeinek meghibásodása

A virtualizációs szoftver mint központi elem elromlása a szolgáltatást lehetetlenné teszi.

Konfliktus a megrendelő biztonsági folyamatai és a cloud között

Ha a szolgáltató biztonsági politikája, szabályzata és folyamatai nem egyeznek meg a megrendelőével, például a szolgáltató nem ugyanazokat a biztonsági kritériumokat alkalmazza, akkor a megrendelő biztonsági előírásainak teljesülését nem lehet hitelt érdemlően ellenőrizni.

Számítógépek lefoglalása

Előfordulhat, hogy két cloud-megrendelő közül az egyik a közös fizikai eszközökön futó virtuális gépeit illegális tevékenységre, pl. illegális fájlcserére használja, és a rendőrség ezért lefoglalja a fizikai gépet. Ez esetben a legális tevékenységet folytató megrendelő adatait és alkalmazói rendszereit is lefoglalhatják.

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 (erre a kérdésre még részletesen visszatérünk).

Licencelés

A szolgáltató feladata, hogy minden általa adott szoftver jogtiszta legyen és a megfelelő számú licenceket beszerezze. Amennyiben ezt nem teszi meg, a megrendelőnek erről esetleg nincs is tudomása, a felelősség azonban esetenként őt terhelheti.

Nem cloud-specifikus kockázatok

A nem cloud-specifikus kockázatok minden, hálózaton működő információs rendszer jellemzői, például a hálózat vagy a hálózatmenedzsment hibája, a hálózat túlterhelése, hackertámadások, a hozzáférési jogosultság kezelésének hiányosságai, a naplófájlok elvesztése vagy kompromittálódása, a backup állományok elvesztése vagy megsemmisülése, a rendszerhez való illetéktelen hozzáférés, a gépek ellopása, természeti katasztrófák. Ezek a kockázatok és kezelésük minden informatikai alkalmazás szükséges velejárói, itt nem részletezzük.

Az ISACA (Information Systems Audit and Control Association, a világ legnagyobb informatikai audit és kontroll szakmai szervezete) kiadványa, az (ISAKA: „Cloud Computing Management") számos nem cloud-függő, és több cloud-függő kockázatot is megjelöl. A cloudfüggetlen kockázatokat itt nem ismertetjük, ez nem tárgya a jelen cikknek. A cloud-függő kockázatok típusai:

Jelentős függőség harmadik féltől:

- külső interfészek támadhatósága,
- az adatközpontok aggregáltsága önmagában kockázat,
- a szolgáltatók esetleges fejletlensége,
- nagymértékű függőség külső tanúsítási folyamatoktól.

A törvényeknek és szabályozásoknak való megfelelőség komplexitása:

- az adatvédelmi kockázat lényegesen megnő,
- a személyes adatok országhatárokon keresztül közlekednek,
- a szerződésben rögzített megfelelőség kockázata.

Az internet mint elsődleges eszköz a szervezet adatai szempontjából kockázati tényező:

- fellépnek a nyilvános környezet biztonsági kockázatai,
- probléma az internetkapcsolat rendelkezésre állása.

A számítási felhő dinamikus jellegénél fogva:

- az adatfeldolgozás helyszíne a terheléselosztás függvénye,
- a feldolgozást végző eszközök más országban is lehetnek,
- a használt eszközökön esetleg a szervezet a versenytársával osztozik,
- a feldolgozás helyszínéül szolgáló ország jogszabályi környezete (felelősség, tulajdonlás kérdése stb.) kockázatot jelenthet a szervezet adatvagyona számára.

Látható, hogy a tipikusan európai megközelítést alkalmazó Enisa-jelentés és az ISACA kiadványa között nagy az átfedés. A továbbiakban elemezzük, hogy egy informatikai vezetőnek mely szempontokat célszerű figyelembe venni a cloud-kockázatok kezelésénél.

Az üzleti és műszaki kockázatok kezelése

Az üzleti jellegű kockázatok kezelése

Az üzleti kockázatok alapvető oka a számításifelhő-piac éretlensége, és ebből következően alacsony szintű szabályozása. Jelenleg még nem léteznek sem cloudspecifikus szabványok, sem erre vonatkozó jogi szabályozás. Amellett, hogy a biztonsági szabványok és az egyes országok információs rendszerekre vonatkozó jogszabályai természetesen a számítástechnikai felhőre is érvényesek, az új szolgáltatási modell jelentősen megnehezíti ezek alkalmazását. Ahogyan Neelie Kroes, az EU-bizottság alelnöke kijelentette (Kroes, 2011): a nemzetközi szabványosítási folyamatnak nagy jelentősége lesz a számításifelhő-fejlődés szempontjából. Az egységes, valóban kompetitív digitális piacon „a cloud-szolgáltató váltásának olyan gyorsnak és egyszerűnek kell lennie, mint a mobilvagy internetszolgáltatók közötti váltásnak". Kroes nagy szerepet tulajdonított a SIENA- (Standards and Interoperability for e-Infrastructure Implementation Initiative) kezdeményezésnek, amely kijelöli „a cloud és grid computing szabványosítási útvonalát az e-tudományban és azon túl" (SIENA Roadmap).

A SIENA törekvése elsősorban a cloud-szolgáltatások interoperabilitásának megteremtése az alkalmazások hordozhatóságát biztosító virtualizációs formátum, a cloud computing interfész IaaS környezetben, valamint az adatkezelési interfész szabványosításával. A SIENA-kezdeményezés együttműködik az USA NIST intézetével a cloud computing területén, így várható, hogy a szabványosítás befejezésekor egységes világszabvány vonatkozik majd erre a területre.

A számítási felhő nyitottságát, azaz a szolgáltatóválasztás és -csere, valamint a több szolgáltatóval való együttműködés lehetőségét tűzte zászlajára egy több száz, kisebb és nagyobb szolgáltatót és felhasználót tömörítő szervezet, amely Open Cloud Manifesto címen jelentette meg elképzeléseit (Open Cloud Manifesto). A kiáltvány létrehozói a cloud-szolgáltatók együttműködésétől várják az egyszerű szolgáltató-váltás, a portabilitás és az interoperabilitás lehetőségének megteremtését.

Véleményünk szerint a cloud-piac jelenlegi, kevéssé fejlett állapotában nincs olyan üzleti kényszer, amely a nagy szolgáltatókat azonnali együttműködésre késztetné. A piac érettségének növekedésével ez az együttműködés majd be fog következni, mint az például a távközlési szektorban a piaci verseny erősödésével meg is történt.

A szolgáltatóhoz való kötődéssel mint kockázattal szemben a legjobb védelem a szabványos, interoperábilis megoldások alkalmazása lenne. Ez – szükség esetén – megkönnyítené az elszakadást a szolgáltatótól, az irányítás sem esik ki teljesen a megrendelő kezéből. Jelenleg, 2011-ben azonban a rendszerek hordozhatósága a Neelie Kroes által vizionált szinten nem lehetséges, ezzel – a teljes interoperabilitást lehetővé tevő szabványok létrejöttéig – várni kell.

Ugyanakkor az egyéb üzleti kockázatok jelentős része a megrendelő és a szolgáltató együttműködésével, a megfelelő, közösen kialakított szabályzatokkal és technikai eszközökkel elfogadható szintre csökkenthető, a felelősség és az esetleges anyagi kár a szerződésben megosztható. Erre természetesen csak akkor van lehetőség, ha a szolgáltató cloud-politikája olyan, hogy hajlandó egyedi szolgáltatási szerződéseket kötni, vagy a megrendelő képes a szolgáltatónál egyedi feltételeket elérni. Meg kell jegyezni, hogy a nagy cloud-szolgáltatók üzleti filozófiája ebben eltérő, vannak, akik készek egyedi szerződéses feltételeket elfogadni, míg mások a szolgáltatást „as is", nem változtatható

formában értékesítik. Megegyezés tárgya lehet a az adatok fel-, illetve letöltésének és tárolásának formátuma, az alkalmazott programfejlesztési módszerek és a programok szabványai, a dokumentáció, a biztonsági eszközök és biztonsági szabályok, a megfelelőséghez kapcsolódó minősítési rendszerek, az autentikációs és autorizációs eljárások, a tranzakciók operatív naplózása, a biztonsági naplók és az ellenőrzési naplófájlok, készítése és formátuma stb.

A szolgáltató piacról való távozását vagy harmadik fél részéről történő felvásárlását a megbízó gyakorlatilag nem akadályozhatja meg. A szerződésben kiköthetjük a tájékoztatási kötelezettséget, esetenként a szerződés azonnali felbontásának lehetőségét és a migráció költségeinek megtérítését.

Ismét megjegyezzük – és ezt az Enisa-jelentés is hangsúlyozza – a kockázatok csökkentése érdekében a megrendelőnek olyan erős pozícióval kell rendelkeznie, hogy a szolgáltatóval a saját érdekeit érvényesítő egyedi szerződést tudjon kötni. Ellenkező esetben el kell fogadnia a szolgáltató általános szerződéses feltételeit.

A műszaki jellegű biztonsági kockázatok kezelése

A cloud-szolgáltatók igen nagy erőfeszítéseket tesznek az informatikai biztonság érdekében, alighanem jóval többet, mint egy átlagos megrendelő. Az Amazon például saját biztonságerősítő tevékenységéről információs anyagot is összeállított (AWS, 2010), amelyből kiderül, hogy félévente a SAS 70 (Statement on Auditing Standards No. 70) II. típusú auditot végeztet egy független szervezettel. Az audit keretében ellenőrzik a biztonság szervezését, az alkalmazottak jogosultságkezelését, a logikai és fizikai biztonságot, az adatkezelés biztonságát, a változásmenedzsment-folyamatot, az adatok sértetlenségét és visszakereshetőségét, valamint az eseménykezelést. Az Amazon a biztonságért való felelősség kérdését megosztja a szolgáltatás, valamint a megrendelő között, mindenki felel a saját erőforrásai és eszközei biztonságáért.

A kockázatmenedzsment a szolgáltatók részéről általában a COBIT keretrendszer szerint történik, és megfelel az ISO/IEC 27000-es szabványsorozatnak. Általánosan jellemző, hogy a biztonságot szerves egészként kezelik, nemcsak a kész rendszereket auditálják, hanem alkalmazzák a „security by design" elvet, azaz a rendszerek tervezési fázisában, a tervek és az elkészült programok biztonsági vizsgálatával igyekeznek elkerülni azt, hogy a kész rendszerek biztonsági réseket tartalmazzanak.

Általánosan megállapíthatjuk, hogy a cloud-szolgáltatók a rendszereik biztonságára a legtöbb megrendelőnél sokkal több erőforrást fordítanak, és az általuk alkalmazott szakértői gárda és eszköztár is magasabb szintű, mint a legtöbb cloud-felhasználóé.

Természetesen a biztonság kérdése a megrendelőre is tartozik, az ő közreműködése nélkül a szolgáltató egyedül nem képes garantálni a magas biztonsági szintet. A megrendelő feladata a saját jogosultságkezelési rendszerének menedzselése, amelyben bele kell érteni a megrendelő teljes AAA folyamatát. Az adatok kódolt átvitelét és tárolását a szolgáltatónak és a megrendelőnek együtt kell rendeznie, célszerűen valamely szabványos megoldás alkalmazásával.

Nem tartozik szorosan a műszaki biztonság körébe a rosszindulatú, vagy illegális tevékenységet folytató társbérlő kérdése, de jelenlétük igen komoly kockázatot jelent a megrendelőnek. Ugyanakkor a megrendelőnek nincs lehetősége arra, hogy megválogassa a társbérlőket, erre vonatkozóan a szolgáltatónak kell megadnia a megfelelő garanciákat.

A számítási felhő alkalmazása során a fentieknél nehezebben kezelhető kérdések a megfelelőség bizonyítása és az adatvédelem terén jelentkeznek.

Megfelelőség a számítási felhőben

A vállalatoknak és egyéb szervezeteknek minden szektorban és gazdálkodási rendszerben meg kell felelniük az érvényes pénzügyi-gazdálkodási és adatvédelmi előírásoknak, szabványoknak és törvényi szabályozásnak. Az előírásokat részben jogszabályok, részben a szervezet belső szabályzatai tartalmazzák. Példaképpen megemlítjük az ISO/IEC 27000-es nemzetközi szabványokat, amelyek az informatikai biztonság kérdését szabályozzák megfelelő részletességgel.

A továbbiakban a jogszabályoknak való megfelelőség elemzésére helyezzük a hangsúlyt, de a belső szabályozásra is ugyanazok a kritériumok vonatkoznak a számítástechnikai felhőben, csak utóbbiak menedzselése a szervezet belügye, míg a jogszabályoknak való megfelelés hiánya törvényi következményekkel jár.

A pénzügyi-gazdálkodási megfelelőség

A pénzügyi-gazdálkodási megfelelőség kérdése 2001-ben került a nemzetközi figyelem fókuszába, amikor az USA egyik legnagyobb energiaszolgáltatójának vezetősége kreatív könyvelési technikákat alkalmazva eltitkolta valós gazdasági helyzetét, félrevezette a részvényeseket és csődbe vitte a céget. Az USA kongresszusa a hasonló esetek megelőzésére elfogadta az ún. SOX- (Sarbanne-Oxley) törvényt, amely a tőzsdei cégek számára kötelezővé teszi a pénzügyi előírásoknak való megfelelőség (compliance) ellenőrzését, a pénzügyi jelentésrendszer pontosságát és az ellenőrzés

bizonyíthatóságát. A megfelelőségért a szervezet vezetői büntetőjogi felelősséggel tartoznak.

Az SOX szerint a szervezeteknek biztosítaniuk kell a megfelelő pénzügyi belső ellenőrzési folyamatokat, ki kell dolgozni a belső ellenőrzés mérhető hatékonysági kritériumait, a menedzsmentnek évente értékelnie kell a belső ellenőrzési rendszer hatékonyságát és nyilvánosságra kell hozni a gyenge pontokat.

Az SOX bevezetése ezeknél a szervezeteknél számos szervezési feladattal járt, például a legtöbb érintett vállalatnál megfelelőségi vezetői pozíciót hoztak létre azzal a feladattal, hogy a vállalat megfelelőségét vezetői szinten biztosítsák.

Az SOX-on kívül más megfelelőségi rendszereket is alkalmaznak a különböző szektorokban. Az USA egészségügyében általános követelmény a HIPAA-(Health Insurance Portability and Accountability Act) megfelelőség. A HIPAA az USA egészségügyi rendszerében alkalmazott elektronikus tranzakciók szabványa, amely többek között előírja az egészségügyi adatok védelmét is. Az EU-ban nincs önálló általános szabályozás az egészségügyi adatok kezelésére, de az EU Adatvédelmi irányelveivel harmonizáló nemzeti jogszabályok természetesen itt is kötelezőek. Emellett egyes országok további nemzeti előírásokat és szabványokat léptettek életbe az elektronikus adatok kezelésének szabályozására. E területen Magyarországon még van teendő.

Az USA pénzügyi intézményeinek szabályozásával kapcsolatos az 1999-ben elfogadott GLBA törvény (Gramm–Leach–Bliley Act), amely – sok egyéb más intézkedés mellett – kötelezővé teszi az intézmények számára az ügyfelek személyes adatainak védelmét. A törvénynek való megfelelőség a menedzsment kötelessége.

Az USA-ban ugyancsak megfelelőségi követelmény a Federal Information Security Management Act of 2002 („FISMA") megfelelőség, amely információs rendszerek biztonságára vonatkozó előírásokat tartalmaz.

Az EU tagországaiban a megfelelőség kicsit komplexebb, mint például az USA-ban. Más, informatikailag fejlett országokkal, mint például Ausztráliával, Japánnal, Kínával, Oroszországgal, Dél-Koreával stb. itt nem foglalkozunk, a legtöbb helyen az USA-hoz hasonló megfelelőségi filozófiát alkalmaznak.

Az EU azon vállalatai számára, amelyeket az USA tőzsdéin jegyeznek, kötelező az SOX-megfelelőség. Magyarországon például anyavállalatán keresztül ebbe a kategóriába esik több nagyvállalat is. Ezenkívül egyes EU-s tagországok bevezették az SOX saját megfelelőjét. Az Egyesült Királyságban a Londoni Tőzsde szabályai a mérvadóak, Franciaországban meg kell felelni a French Association of Private Enterprises (AFEP) és a French Employers' Federation (MEDEF) Corporate Governance Code-nak a pénzügyi jelentések összeállításakor. Németországban a Federal Institution for Supervision of Financial Services irányítja a pénzügyi szektor ellenőrzési gyakorlatát stb. Minden EU-s tagországra jellemző az informatikai biztonsági szabványoknak, a pénzmosás elleni jogszabályoknak, a pénzügyi ellenőrzési követelményeknek való megfelelés kötelezettsége a nem nyilvános tőzsdei cégek esetén is.

A megfelelőségi előírások nemcsak a szabályoknak való megfelelésre, hanem az ellenőrzési és dokumentálási módszerekre is vonatkoznak.

Az információs rendszerek biztonsági auditját jellemzően a COSO (Committee of Sponsoring Organizations) és a Control Objectives for Information and Related Technologies (COBiT) módszertanok alkalmazásával hajtják végre. Az ISACA hivatkozott anyagában részletes ajánlást dolgozott ki a cloud-környezetben végrehajtott COSO/COBiT biztonsági auditra, amely a megfelelőségi kritériumok ellenőrzésének is eleget tesz. A végrehajtáshoz ugyanakkor a cloud-szolgáltató teljes együttműködésére van szükség. Például az audit-ajánlás az irányítási modell ellenőrzéséhez előírja, hogy meg kell győződni arról, hogy a szervezet összes szerződéses cloud-szolgáltatójának biztonsági rendszere megfelel-e a szervezet biztonsági politikájának, és megfelelően kezeli-e a cloudban való feldolgozás kockázatait, az irányítás és a biztonságért való felelősség megosztása megfelelő és megfelelően dokumentált. Előírja a szolgáltató összes belső biztonsági folyamatának és gyakorlatának áttekintését, az adattárolás megfelelőségét a helyi jogi környezetnek, általában a jogi megfelelőséget stb. Megköveteli a szolgáltató és a megrendelő adatvédelmi felelősségének világos elkülönítését, az ISO 27001-es biztonsági szabványnak való megfelelőséget és az erről szóló tanúsítványt. Külön részt szentel a portabilitás ellenőrzési kérdéseinek.

A teljes ellenőrzést meghatározó célok közül kiragadott fenti példák érzékeltetik, hogy az audit kizárólag a szolgáltató teljes együttműködésével valósítható meg. Az audit feltételeit a cloud computing szerződésben kell rögzíteni, azonban a szerződés megkötése előtt célszerű megvizsgálni a szolgáltató saját biztonsági és ezzel összefüggő üzleti politikáját, szabályzatát és folyamatait.

A fenti követelményekből látható, hogy a hatékonyságot a központba helyező cloud-szolgáltatási modell és a szolgáltató üzleti modellje, valamint a megfele-

lőségi audit követelményei csak nagy erőfeszítésekkel egyeztethetők össze. A szolgáltató üzleti érdeke a terheléselosztás, akár országhatárokon át is, ahol más és más jogrendnek kell megfelelni. A szolgáltatónak nem feltétlenül érdeke a teljes átláthatóság biztosítása, hiszen ez üzleti szempontokat érinthet. A szolgáltató nem feltétlenül készít auditdokumentációt egy adott megrendelő tranzakcióiról, vagy nem a megrendelő által igényelt formában készíti. Minden, az audithoz szükséges „testreszabás" pluszköltséget jelent, amelyet vagy a megrendelőnek, vagy a szolgáltatónak kell megfizetni, rontva ezzel az alap cloud-modell hatékonyságát.

Összességében elmondhatjuk, hogy a számítási felhőben működő informatikai rendszerek megfelelőségi szempontból auditálhatók, ennek módszertana is létezik, ugyanakkor az auditok lefolytatásához a megrendelő és a szolgáltató közötti szerződésnek részletesen szabályoznia kell ennek folyamatát, a felek feladatait és felelősségét. Ehhez viszont (l. Enisa-jelentés) a megrendelőnek megfelelő tárgyalási pozíciókkal kell rendelkeznie a szolgáltatóval szemben.

Természetesen a szolgáltatóknak is érdeke a megrendelő megfelelőségi auditjainak segítése, ennek hiányában ugyanis sok szervezet nem köthet szerződést a szolgáltatásra. A következő néhány évben majd eldől, hogy a cloud-szolgáltatók milyen messzire mennek el az auditálhatóság tekintetében.

Az adatvédelem kérdése

Az Európai Unió az 1995-ös Adatvédelmi Irányelv megjelenése óta vezető szerepet játszik az adatvédelem területén (Kroes, 2011b). 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 cloud-szolgáltatás igénybevétele esetén is. Az irányelvet az egyes országok kisebb-nagyobb különbségekkel alkalmazzák, a számítási felhővel kapcsolatos adatvédelmi követelmények kisebb mértékben változhatnak az egyes országok között. Az adatvédelem jogi szabályozásában Magyarország az EU egyik élenjáró országa, a magyar adatvédelmi jogszabályok nem kevésbé szigorúak, mint bármely más EU-s tagországé, így az adatvédelem kérdését az EU-s irányelvek alapján vizsgálhatjuk Magyarországon is.

Az Adatvédelmi irányelv meghatározza a személyes adat, a különleges adat, az adatkezelés és adatfeldolgozás, valamint az adatkezelő és az adatfeldolgozó fogalmát. A számítási felhő alkalmazása esetén gyakran személyes adatokat kezelnek, ugyanis a szolgáltatásokat általában az e-mail, üzenetközvetítés, desktop, projektmenedzsment, bérelszámolási, könyvelési, pénzügyi, alkalmazásfejlesztési, telemedicinális, CRM, értékesítési, személyes adatfeldolgozási – beleértve a különleges adatokat is – számlázási stb. feladatok megoldására veszik igénybe. Az adatok alanyai alkalmazottak, ügyfelek, szállítók, páciensek, üzleti partnerek.

A továbbiak szempontjából lényeges az adatkezelő és az adatfeldolgozó szerepének pontos meghatározása, ezért ezt idézzük az irányelvekből:

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.

Adatfeldolgozó: az a természetes vagy jogi személy, igazgatási vagy egyéb szervezet, amely az adatkezelő megbízásából személyes adatot dolgoz fel.

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.

Tilos az adatok továbbítása azokba az országokba, ahol nincs megfelelő adatvédelem, kivéve, ha az alany ehhez előzetesen kifejezetten hozzájárul, vagy a harmadik ország megfelelő adatvédelmet tud biztosítani (pl. ha az adatokat az USA-ba továbbítják, akkor a „Safe Harbour Privacy Principles", amely szerint a részt vevő USA székhelyű vállalatok vállalják, hogy biztosítják az EU-nak megfelelő adatvédelmet).

Az EU tagállamai engedélyezhetik a személyes adatok olyan harmadik országba irányuló továbbítását, amely nem biztosít megfelelő szintű védelmet, amennyiben az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében; ilyen garanciát jelenthetnek elsősorban a megfelelő szerződési feltételek.

A fenti követelmények betartása – számos egyéb, nem cloud-specifikus adatkezelési előírás betartása mellett – az adatkezelő feladata.

Felmerül a kérdés, hogy cloud-szolgáltatás alkalmazása mellett ki az adatkezelő és ki az adatfeldolgozó. Minthogy a szolgáltatás megrendelője határozza meg az adatfeldolgozás célját és eszközeit, a cloud-szolgáltató pedig a megrendelő megbízásából feldolgozza a személyes adatokat, egyértelmű, hogy a megrendelő az adatkezelő, a cloud-szolgáltató pedig az adatfeldolgozó.

Az Adatvédelmi irányelveknek való megfelelésért elsősorban az adatkezelő felel. Műszaki és szervezési eszközökkel biztosítania kell, hogy az adatok ne veszhessenek el, ne változtassák meg őket, illetéktelenek ne férhessenek hozzá és ne történhessen semmiféle törvénytelen felhasználás.

Olyan adatfeldolgozót kell választania, amely megfelelően garantálni tudja azokat a műszaki és szervezeti feltételeket, amelyek biztosítják az irányelv szerinti feltételek teljesülését. Emellett az adatkezelőnek tájékoztatási kötelezettsége is van, kötelező tájékoztatni például a saját *ügyfeleit* arról, hogy adataikat feldolgozásra átadja egy harmadik félnek, a *cloud-szolgáltatónak*. Ez a tájékoztatási kötelezettség minden személyes adat alanyára vonatkozik, akinek az adatai átkerülnek a felhőbe. Tájékoztatni kell az alanyokat az átadás céljáról, okairól, a szolgáltató „minőségéről".

A cloud-szolgáltató a szolgáltatásba – üzleti tevékenysége körében – bevonhat EU-tagországot, vagy az EU-n kívüli országot is, ahol esetleg nem teljesülnek az EU-s irányelv előírásai. Ezért mindenképpen szükséges az adatkezelő ügyfeleinek megfelelő tájékoztatása és egyértelmű beleegyezése, vagy megfelelő szerződéses feltételek biztosítása, vagy a Safe Harbour alkalmazása az USA esetében. Az egyedi beleegyezés egyébként visszavonható.

A számítási felhő alkalmazásakor a fenti követelmények teljesítése nem egyszerű. Nem világos például, hogy adatvédelmi szempontból mi a teendő, ha a megrendelő az egyik cloud-szolgáltatótól átmigrál egy másikhoz, és az utóbbi egyik telephelye nem esik az EU-s szabályozása alá, ugyanakkor nem zárható ki, hogy az automatikus terheléselosztás eredményeképpen az adatokat éppen ebben az országban dolgozzák fel.

Az irányelv nem határozza meg pontosan az adatátvitel fogalmát, de nem számít az Adatvédelmi irányelv megsértésének, ha egy EU-tagországból az USA-ba (Safe Harbour) továbbítanak személyes adatokat, például Izlandon és Kanadán keresztül. Az interneten viszont az adatok útvonalai akár a terhelések függvényében is változhatnak, nem határozható meg egy rögzített útvonal.

Az irányelvek szerint az adatkezelő feladata, hogy biztosítsa a személyes adatok elérhetőségét és sértetlenségét. Ehhez a cloud megrendelőjének ellenőrizni kell tudnia a cloud-szolgáltató biztonsági politikáját, szabályzatát, azok betartását, az országban érvényes kötelező biztonsági előírásokat és meg kell győződni az azoknak való megfelelőségről.

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 bűnügyi szankciókkal járhat.

A cloud megrendelőjének saját felelősségét a cloud-szolgáltatóval kötött szerződésben célszerű részletezni, és ahol ez lehetséges, a szolgáltatótól garanciákat kérni arra, hogy az előírásoknak megfelel. Ehhez természetesen szankciókat kell társítani.

Az Enisa-jelentés szerint cloud-szerződésbe célszerű beiktatni egy adatvédelmi részt, amelyben rögzíteni kell, hogy

- a cloud-megrendelő az EU-irányelv szerinti adatkezelő, aki törvény szerint felel a tisztességes, törvényes stb. adatfeldolgozásért, meg kell jelölni, hogy e feltételeknek a megrendelő hogyan tud megfelelni,
- a cloud-szolgáltatónak tevékenyen együtt kell működnie a megrendelővel a megrendelő adatvédelmi jogainak biztosítása érdekében,
- a cloud-szolgáltatónak megfelelő biztonsági eljárásokat és eszközöket kell alkalmazni és a biztonság esetleges megsértése esetén haladéktalanul tájékoztatnia kell a megrendelőt és együtt kell működnie a probléma gyors megoldása érdekében,
- az adatvédelmi előírások megsértése milyen következményekkel jár a szolgáltatóra nézve, illetve a megrendelő megfelelő kártérítést kap-e ez esetben.

Önállóan kezelendő kérdés a személyes adatok továbbítása nem EU-s vagy nem EGT (Európai Gazdasági Tér) országokba. Ha a személyes adatokat olyan harmadik országba továbbítják, amely nem felel meg az irányelvekben megadott adatvédelmi követelményeknek, akkor ehhez vagy az érintett előzetes, egyértelmű hozzájárulását kell megszerezni, vagy az irányelvekben megadott egyéb módon kell biztosítani az adatvédelmet (az adatkezelőnek megfelelő garanciákat kell adnia, ilyen garanciát jelenthetnek elsősorban a szerződéses feltételek, illetve a Safe Harbour-elv a csatlakozó szervezetek esetén).

Az Enisa-jelentés szerint, ha a cloud-szolgáltató olyan, az Európai Gazdasági Térségen kívüli országban működik, amely nem biztosítja a megfelelő adatvédelmet, akkor a cloud-megrendelőnek célszerűbb az irányelvekben megengedett szerződéses feltételekre, vagy az USA esetében a Safe Harbour-elvre támasz-

kodni, mint az érintett ügyfelek beleegyezését megszerezni, ami bármikor visszavonható.

A cloud-szolgáltatások kivétel nélkül az interneten működnek, így az adatátvitel alapvető összetevője minden cloudnak. Sajnos az adatok átvitelének szabályozása még az EU tagországai között sem egyértelmű. Az irányelvek ugyan kimondják az adatok szabad áramlását, azonban az egyes országok eltérő szabályozása miatt a felelősség kérdése nem egyértelmű.

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. Nem véletlen, hogy a cloud alkalmazásának EU-s előrejelzései (hatmilliárd euró értékű cloudpiac 2013-ban) meglehetősen visszafogottak.

Az informatika és a távközlés fejlődése, a korszerű eszközök és üzleti modellek elkerülhetetlenné teszik az Adatvédelmi irányelvek áttekintését és pontosítását. 2010 novemberében megjelent a Bizottság közleménye (Európai Bizottság közleménye, 2010).

*A közlemény rámutatott, hogy „*az adatfeldolgozás növekvő mértékű – és igen gyakran az Unión kívülre történő – kiszervezése több problémát is felvet az adatfeldolgozásra alkalmazandó joggal és az ahhoz társuló felelősség megosztásával kapcsolatban. Ami a nemzetközi adattovábbítást illeti, sok szervezet szerint a jelenlegi szabályozások nem teljes mértékben megfelelők, ezért az adattovábbítás egyszerűsítése és nehézkességének csökkentése céljából felül kell vizsgálni és korszerűsíteni kell azokat.”

Emellett „A Bizottság mérlegelni fogja, hogy az új technológiáknak az egyének jogaira és szabadságaira gyakorolt hatását és a személyes adatok belső piacon való szabad áramlásának biztosítására vonatkozó célkitűzést szem előtt tartva hogyan biztosítható az adatvédelmi szabályok következetes alkalmazása”.

Ehhez – az Adatvédelmi irányelvek alapvető céljainak változatlansága mellett – konkrét szabályozást, kritériumrendszert, a nemzetközi adattovábbítás szabályozásának egységesítését és egyszerűsítését szeretnék végrehajtani. Az Adtatvédelmi irányelvek korszerűsítése valószínűleg még jó néhány hónapig el fog tartani, addig a jelenlegi szabályozást kell alkalmazni.

Összefoglalás

Cikkünk üzleti és műszaki áttekintést kívánt adni a számítástechnikai felhő üzemeltetési modell alkalmazásának vezetők számára fontos lehetőségeiről és kockázatairól. Lényegében arra kívántunk rámutatni, hogy bár az amerikai menedzsmentirodalom lelkes evangélistája ennek az új koncepciónak, és nyilván nem vitatható az, hogy ezzel egész új irányokat szab az információmenedzsment néhány területén, azért a jelenlegi európai és magyar infrastrukturális és szabályzási környezet miatt ezzel a lelkesedéssel megfontoltan kell bánnunk. Elemzésünk összegzéseként összefoglaljuk, hogy egy magyar (európai) vezetőnek milyen szempontokat kell figyelembe venni egy cloud-szolgáltatás igénybevételénél:

1) meg kell vizsgálni, hogy melyik szolgáltatási modell illeszkedik legjobban a szervezet üzleti stratégiájához (SaaS, PaaS, IaaS, esetleg ezek kombinációja),
2) ki kell választani az(oka)t a szolgáltató(ka)t -amelyek a megfelelő szolgáltatást nyújtják,
3) el kell végezni a cloud.szolgáltatás és az ugyanolyan funkcionalitású saját rendszer TCO-számítását, és mérlegelni kell a gazdasági előnyöket,
4) a cloud-szolgáltatóval együtt meg kell vizsgálni,(due diligence) hogy a szervezetre alkalmazandó megfelelőségi kritériumok auditját hogyan lehet elvégezni a cloud-környezetben, ebben a szolgáltató hogyan tud vagy akar közreműködni,
5) meg kell ismerni a szolgáltató biztonsági politikáját, előírásait, gyakorlatát, valamint minősítéseit (due diligence),
6) meg kell győződni arról, hogy a szolgáltató minden tekintetben képes megfelelni az EU Adatvédelmi irányelveinek,
7) meg kell győződni arról, hogy a szolgáltató a szokásos üzleti és szolgáltatási szint megállapodások mellett hajlandó szerződésben garantálni a megrendelő számára elengedhetetlen biztonsági és adatvédelmi követelményeket.

Érdemes megjegyezni, hogy egy oursourcing-szerződés megkötése előtt a due diligence vizsgálatot az outsourcing-szolgáltató végzi a megrendelőnél, a cloud esetén ez pont fordítva történik, a megrendelő vizsgálja a szolgáltatót, ugyanis megfordul a kockázatviselés terhe, a cloud esetén a nagyobb kockázatot mindenképpen a megrendelőnek kell vállalnia.

Lábjegyzet

* A kutatást a TÁMOP 4.2.1.B-09/1/KMR-2010-0005 projekt támogatta.

Felhasznált irodalom

Adatvédelmi irányelv (1995): Az Európai Parlament és Tanács 95/46/EC sz. 1995. október 24-i, a személyes adatok védelméről és szabad áramlásáról szóló irányelve (Az Európai Parlament és Tanács 95/46/EK irányelve (1995. október 24.)

AWS (2010): Amazon Web Services: Overview of Security Processes, August 2010 http://aws.amazon.com/security

Bőgel Gy. (2009): Az informatikai felhők gazdaságtana – üzleti modellek versenye az informatikában. Közgazdasági Szemle, LVI. évf., 2009. július–augusztus, 673–688. o.

Enisa Report (2009): Cloud Computing – Benefits, Risks and Recommendations for Information Security. Nov. 2009 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Az Európai Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának (2010): Az európai digitális menetrend Brüsszel, 2010. 8. 26.

Az Európai Bizottság Közleménye (2010): A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: „A személyes adatok Európai Unión belüli védelmének átfogó megközelítése" címmel. (Brüsszel, 2010. 11. 4. *COM*(2010 609 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_hu.pdf

Greenberger, M. (1962): Management and the Computer of the Future. MIT Press – John Wiley & Sons, Cambridge, New York

Greenemeier, L. (2002): American Express, IBM Sign $4B Deal: http://www.informationweek.com/news/software/productivity_apps/showArticle.jhtml?articleID=6500855

IBM global outsourcing revenues rise (2009) – newsrating.com 12/09/05

IDC on cloud computing (2009) http://www.idc.com/prodserv/idc_cloud.jsp

ISACA (2010): Cloud Computing Management Audit /Assurance Program. www.isaca.org, ISBN 978-1-60420-162-8)

Kroes, N. (2011a): European Cloud Computing Strategy Needs to aim high, Opening Speech of Microsoft Centre on Cloud Computing and Interoperability, Brussels, 22 March 2011.

Kroes, N. (2011b): European Cloud Computing Strategy Needs to Aim High: Brussels, March 22, 2011, Opening of Microsoft Center on Cloud Computing and Interoperability)

Mell, P. – Grance,T. (2009): The NIST Definition of Cloud Computing. http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc 2009. 10. 07

Microsoft TCO kalkulátor (2010) (https://roianalyst.alinean.com/msft/AutoLogin.do?d=176318219048082115)

OECD Key ICT Indicators (2010) www.oecd.org/sti/ICTindicators

Open Cloud Manifesto (2010) www.opencloudmanifesto.org

SIENA Roadmap (2010): European roadmap on Grid and Cloud Standards for E-science and Beyond, www.sienainitiative.eu)

Cikk beérkezett: 2011. 4. hó
Lektori vélemény alapján véglegesítve: 2011. 5. hó