Biztonságosan a Felhőben. A publikus felhők biztonsági kérdései

Rubóczki Edit

Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

edit.ruboczki@rubedi.hu

Absztrakt: Cikkemben elsősorban a felhővel, és a felhőszolgáltatásokkal foglalkozom. Részletesen bemutatom, miért előnyös a felhőszolgáltatásokat igénybe venni, milyen előnyökre tehetünk szert, ha az IT környezetünket, vagy annak csak egy részét felhőbe költöztetjük. A sok előny mellett bemutatom a hátrányokat, azokat a funkciókat, amiket elveszítünk felhőszolgáltatások igénybevételekor, vagy a vállalati környezetünkre negatív hatást mérünk a használattal. Összefoglalom azokat a biztonsági kérdéseket, melyek minden felkészült IT szakember fejében is megfordulnak akkor, amikor az a kérés érkezik feléjük, hogy: „Javasolja-e a számítási felhőre való átállást?" A válasz nem egyértelműen igen és nem egyértelműen nem. Szeretném felhívni a figyelmet arra, hogy ha körültekintően, a biztonsági előírásokat betartva járunk el, a felhő is lehet biztonságos – és sok esetben nyújthat nagyobb biztonságérzetet a felhasználónak.

Kitérek még a felhőszolgáltatásokra vonatkozó szabványosítási környezetre, ami védi, leírja és összefoglalja az IT biztonság felhőkre is vonatkozó részeit. Továbbá bemutatom, mire számíthatunk a következő évben, mi lesz a trend a felhős égbolton.

1 A felhő, mint szolgáltatás

Napjainkban az informatikai környezet és hálózatok mindenki számára elérhetővé váltak. Ez lassan, de biztosan jelenti azt, hogy az informatika és az internet közműszolgáltatássá válik. Különösen igaz ez az informatika azon területeire, amit minden felhasználó elér és „közösen" használ. Ezek a mindenki által elérhető szolgáltatások a felhőszolgáltatások, az informatika egyik legdinamikusabban fejlődő területe. Felhőszolgáltatások közül is többféle hozzáférésű architektúrát különböztetünk meg egymástól, nevezetesen a privát, a publikus és a hibrid kialakítású környezeteket. Cikkemben a publikus felhők biztonsági kérdéseivel foglalkozom.

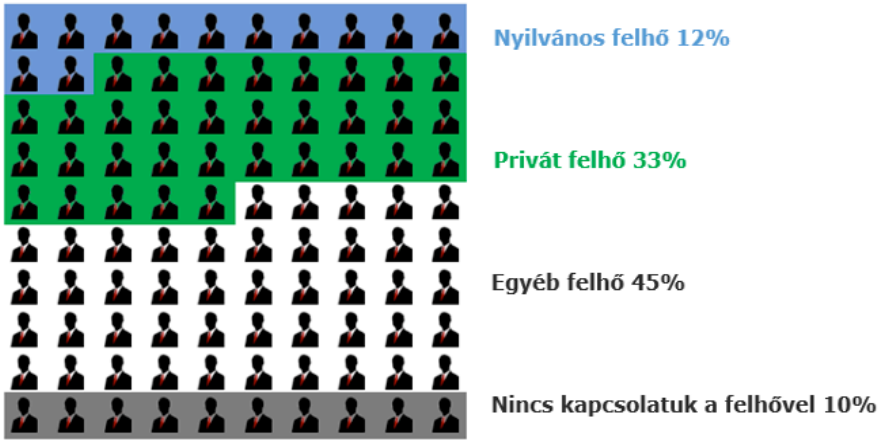
A felhőszolgáltatások hatalmas változást idéznek elő a piacon, általa az informatika minden eddiginél hatékonyabban szolgálja az üzleti fejlődést. A publikus felhőszolgáltatások olyan lehetőségeket nyújtanak az átlagfelhasználó

számára, amit csak egy jól szervezett és költséges nagyvállalati informatikai környezet biztosít munkavállalói részére. Mindezt természetesen „fillérekért" – havidíj ellenében, beruházási költségek nélkül veheti igénybe az előfizető. A „pay-as-you-grow" (felhasználás alapú fizetési mód) rendszereknek köszönhetően gyakorlatilag mindenki annyit és azt vesz igénybe, amire szüksége van – és csak annyit fizet érte, amennyit ténylegesen használ a publikus felhő szolgáltatásai közül.

A felhőszolgáltatások leginkább a gazdasági szféra szereplőit, azon belül is a KKV szektor igényeit képes kielégíteni, általában azon a biztonsági szinten, ami a KKV szektorban lévő vállalkozások számára elég és elfogadható. Ezeknek a vállalkozásoknak nyújt megbízható (sok esetben 99,9%-os rendelkezésre állású), költséghatékony és könnyen skálázható, többrétegű szolgáltatásokat a felhőt üzemeltető. A nagyvállalatok általában rendelkeznek saját, testreszabott, egyéni igényeket kielégítő informatikai infrastruktúrával vagy ehhez tartozó szigorú biztonsági folyamatokkal, szabályozásokkal, amit jelenleg a publikus felhőt üzemeltető szolgáltatók még nem, vagy csak többletköltségek árán tudnak testre szabni. A felhők előnyeit azonban a nagyvállalatok is élvezni kívánják, az ő részükre privát felhő vagy hibrid felhő megoldásokat alakítanak ki informatikusaik vagy az erre a célra kiválasztott szolgáltató, aki képes az általuk előírt szabályzatok betartására.

A leendő felhasználók, az informatikáért felelős szakemberek és a kis-és középvállalkozások vezetői azonban még mindig tartózkodnak a felhőszolgáltatásokat igénybe venni, és csak részben, egyes szolgáltatáselemeket, általában a levelezést, az adattárolás egy részét engedik felhőbe helyezni. Ennek oka, hogy még mindig nem bíznak a számítási felhő biztonságában, az ott tárolt adataik sérthetetlenségében.

A Gartner elemzése szerint az általuk megkérdezettek az alábbi arányban használnak felhőmodelleket:



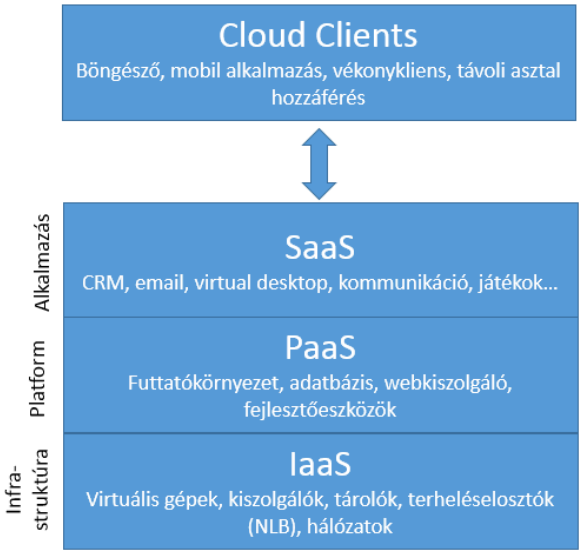
Forrás: Gartner-2012

2 Mit értünk felhő alatt?

A felhő nem más, mint egy speciális módon kialakított szolgáltatás, amely szolgáltatásai meghatározott feltételekkel, megadott SLA-jú rendelkezésre állás szerint, mérhető, elszámoltatható és egyszerűen kalkulálható felhasználói költségmodell (árlista) szerint működik. A felhő felhasználói internetkapcsolaton keresztül – jellemzően szélessávon – érik el azokat a szolgáltatáselemeket, amit a felhőszolgáltatójuk nyújt – és amikre nekik ezek közül a kínált szolgáltatások közül szükségük van.

A felhő elnevezést először Eric Schmidt, a Google CEO-ja használta a 2007-es Google Konferencián San Jose-ban, és alkotta meg a „Cloud Computing" vagyis a Számítási felhő fogalmat. Ugyanebben az évben, még a konferenciát megelőzően dobták piacra a Google Docs alkalmazásukat, ami később meghatározó mérföldköve lesz az irodai alkalmazások felhőben való elhelyezésének.

A felhő rendszerek jelenleg egymástól elszigetelten, szigetszerű infrastruktúrákként működnek és az alábbi főbb területeken biztosítanak szolgáltatásokat:



- IaaS – infrastruktúra nyújtása szolgáltatásként, amikor a felhőszolgáltatók az infrastruktúrát nyújtják, mint szolgáltatáselemet. Virtuális gépet, szervert, vagy tárolót adhat a felhasználónak, mint pl. a Microsoft Azure szolgáltatása.
- PaaS – platform nyújtása szolgáltatásként, amikor a szolgáltató a környezetet biztosítja, úgymint az adatbázis, a fejlesztőkörnyezet vagy futtatókörnyezet, amit a felhasználók igénybe vehetnek. (Pl. az Amazon)
- SaaS – alkalmazás nyújtása szolgáltatásként, amikor csak meghatározott szolgáltatásokat nyújt a szolgáltató, az általa meghatározott lehetőségek szerint. Ilyen a Google Drive, vagy a Microsoft Office 365 szolgáltatása.

Azt nevezzük felhőszolgáltatásnak, ami rendelkezik mind a hat alapkritériummal:

1. Adatkapcsolaton keresztül érhető el (internet)
2. Az előfizető önkiszolgáló portálfelületet használ
3. Skálázható: a felhasználó annyit vesz igénybe, amennyire szüksége van.
4. Az árazása felhasználás-alapú: a "pay as you grow" elv alapján mindig csak annyi kapacitás után fizetnek, amennyire a méretük, működésük alapján szükségük van
5. Automatizált folyamatok működtetik a szolgáltatást
6. Egységesített szolgáltatás elemekből kialakított csomagolt megoldást nyújt

A felhőszolgáltatások használatának legfontosabb előnyeit és hátrányait az alábbi táblázat foglalja össze:

Előnyök:

- Előfizetéses vagy felhasználási alapú árazási modell
- Alacsony költség - az ügyfélköltségek csökkenése
- Célzott felhasználási lehetőségeket nyújt
- A felhasználók keveset vesznek észre abból, hogy felhő szolgáltat-e nekik, vagy helyi szerver
- Minden működik és gyors
- Egy új informatikai alkalmazás beindítása pillanatok alatt lehetséges
- Kevesebb karbantartást igényel
- Skálázható
- Információhoz való szabad hozzáférést biztosít
- A környezeti igénybevétel csökkenését eredményezi
- Rugalmas – a változó körülményekhez alakítható
- A területhasználat minimalizálására törekszik
- Csak az adatközpontokban kell a szervereket hűteni (környezetvédelem)
- Szokványos internet technológiák alkalmazásával kínálják

Hátrányok:

- Meg kell oldani az adatokhoz való hozzáférés kontrollálását
- A felhő tömeges használata feltétlenül olyan új vadászterületet hoz létre, amelyet a bűnözők a megfelelő elterjedés esetén azonnal kihasználnak
- Kritikus üzleti alkalmazásokhoz még mindig nem javasolják
- Jogi eltérés: ÁSZF van egyedi szerződés helyett
- A nyilvános felhő szolgáltatások nem köthetők egyik felhasználói csoporthoz sem (nem egyedi)
- Az adatokat titkosított adatcsatornákon, SSL kapcsolaton keresztül irányítják a felhőbe
- Az adatokat már a keletkezés helyén titkosítani kell
- Meg kell bízni a szolgáltatóban

- A felhasználók bizalmát erősíteni kell a szolgáltató felé
- A felhasználókban tudatosítani kell a biztonsági korlátokat

3 Veszélyforrások, kockázatok

Amikor a számítási felhő mellett érvelünk, elsődlegesen a rendelkezésre állása (sokszor 99,9%), a skálázhatósága, az alacsony környezeti terhelése, a költségek csökkentése és tervezhetősége merül fel. Amit véleményem szerint fontos még megemlíteni, hogy a felhőrendszerekben kialakított szabályok mindenkire egyformán érvényesek. Tehát egy vállalkozás tulajdonosára, vezetőjére, informatikusára, és az asszisztenciájára egyformán – ellentétben egy saját tulajdonban lévő informatikai környezettel, ahol a biztonsági rést legtöbbször maga a vezető vagy az informatikus nyitja meg. [1]

Ugyanakkor a számítási felhő erősebb biztonsággal rendelkezik az alábbi területeken:

1. Fizikai hozzáférés
2. Beléptetés és adatkezelés– a szolgáltatók sokkal többet költenek ezek felügyeletére, fejlesztésére és karbantartására, mint magára az adatok tárolására
3. Biztonsági Menedzsment– úgymint a patching, az updating, és az alacsony illetve magas kockázatú munkafolyamatok kialakítása során

Ha azt vesszük alapul, hogy egy felhőszolgáltató egyszer fizeti meg a fentiek költségét, érezhető az, hogy erre sokkal több energiát, időt és pénzt áldozhat, ugyanakkor a fajlagos költsége mégis nagyságrendekkel alacsonyabb lesz.

Amikor felhőről beszélünk, megváltozik a fizikai biztonság értelme, ugyanis a felhő nem működik virtualizáció nélkül.

Lényegéből fakad, hogy olyan környezetben találhatók a szolgáltatások, ahol a virtualizáció adja a rendszer stabilitását, könnyű konfigurálhatóságát, mindazt, ami a felhőben jó. Ebben a rendszerben a programkörnyezet fájlként jelenik meg, ami - bizonyos megkötések mellett - szabadon másolható. A lemásolt rendszer azután szabadon vizsgálható, a tartalma megfejthető, módosítható. [3], [2]

3.1 Legfőbb félelmeik:

1. Felhőszolgáltató megbízhatósága, úgymint
   A. Biztonság / adatvédelem – ez a legnagyobb félelem
   B. Rendelkezésre állás / megbízhatóság – Elegendő-e a 99,9%? (Ez egyébként 8,76 óra kiesést jelent éves szinten)

C. Irányítás, kockázat és a megfelelés-kezelés (GRC) - túlélne-e egy auditot?

D. Hibák kijavítása - szankciók meg nem felelés esetén

2. Adathordozhatóság - a szolgáltató hibája esetén
3. Adatok elhelyezkedése - hozzáférhetnek-e az adatokhoz a nyomozó hatóságok?
4. Integráció és hibrid környezetek - problémák többféle környezet esetén
5. Az infrastruktúra felkészültsége - megfelelő-e ez az átjáró?
6. Licencelés - BYOL és más verziók
7. Adózási következmények - CAPEX vs. OPEX
8. Szakismeret rendelkezésre állása és munkahelyi kultúra - legfőbb IT akadály

3.2 A felhőszolgáltatások felhasználóit az alábbi fenyegetések érhetik:

1. Adatok megsértése

Minden olyan számítógépes rendszerhez, amely az internethez csatlakozik, gyakorlatilag bárki hozzáférhet. Ezáltal a felhőszolgáltatók fenyegetésnek vannak kitéve a képzett hackerek rosszindulatú szándékai által. 2012-ben a bejelentett szerver feltörések száma 200 fölött volt, amely mintegy 9 millió adatállomány elvesztését eredményezte.

2. Adatvesztés

Az adatvesztés a másik komoly fenyegetés, amivel a felhőszolgáltatóknak komolyan foglalkozniuk kell, és amit nem feltétlenül tudnak megelőzni. Amennyiben a szolgáltatónak nagyobb adatmennyiséget kell kezelni, az adatvesztés még nagyobb mértékben jelentkezhet. Ahogy a felhőszolgáltatások népszerűsége nő, növekszik a szolgáltató felé érkező érzékeny adatok mennyisége is – ahol azonban az adatvesztés, az adatok elvesztése vagy véletlen törlése, esetleges meghibásodása már nem elfogadható a felhasználó felől.

3. Felhasználó eltérítés (account hijacking)

A vállalat jogosult személyeinek általában engedélyezve van távolról hozzáférni a felhő adatokhoz mobil eszközökről vagy távoli számítógépekről. A potenciális előfizető- vagy adateltérítések száma akkor növekedhet, amikor a munkavállalók távoli felületeken keresztül férnek hozzá bizalmas információkhoz, amelyek nem rendelkeznek feltétlenül olyan szintű védelmi mechanizmussal, mint a munkahelyi számítógép.

4. Bizonytalan alkalmazásprogramozási felületek (API-k)

Az API-k biztosítják a programok egymás közötti kommunikációját és biztonságuk nem mindig teljesen garantált. A rossz szándékú embereknek ezek a biztonsági kiskapuk adják meg a lehetőséget a kommunikációs csatornán áthaladó adatokhoz való hozzáférést.

5. Szolgáltatás megtagadása

Bár nem befolyásolja súlyosan a felhő szervein tárolt adatok integritását, a szolgáltatás megtagadása átmenetileg megakadályozhatja a jogosult felhasználók adatokhoz való hozzáférését.

6. Adatok kezelése

A technológia és erőforrások megosztása több különböző szervezet között mindig kockázatot jelent az adatok kezelését illetően. Néha a felhő szerverek úgy vannak beállítva, hogy több ügyfél is tudjon az adatokkal dolgozni. Ha egy eltérő követelményekkel rendelkező kliens adatai bekerülnek a rendszerbe, az adatok sértetlenségét és a felhasználók izolációját a szolgáltató nem tudja biztosítani.

4 Eszközök és módszerek a kockázatok csökkentése érdekében

Az érzékeny adatokat csak titkosítással lehet kellőképpen megvédeni. A különféle vállalati auditok során (pl. PCI DSS) előírt követelmény az adatok titkosítása a tárolási helyükön. Ezt a távoli eléréssel is meg kell oldaniuk a szolgáltatóknak, hogy az üzleti felhasználóik üzleti célra is alkalmazhassák a felhő szolgáltatásait. Sok esetben azonban nem elég a felhőben kialakítani a titkosítást, azt sokkal korábban, az adatkapcsolat titkosításával (SSL) is meg kell tenni, sőt, akár a keletkezési helyükön. Az egyes felhasználók tárhelyeit, alkalmazásait, postafiókjait külön jelszavas védelemmel kell ellátni. Az adatok biztonságát és a rendelkezésre állást a szolgáltatók az adatközpontok számának növelésével érik el. Több szolgáltató rendelkezik georedundáns adatközpontokkal, ami azt jelenti, hogy az adatközpontok egymástól meghatározott távolságra helyezkednek el, és az adatokat ennek megfelelően elosztva tárolják. Számos lépést lehet tenni a felhő biztonságának fokozása érdekében. A világ egyik vezető cége az információs adatvédelem és vírusirtás terén, a Symantec négy fő ajánlást készített el ezzel kapcsolatban egy 2013-ban készült felmérés alapján: [4]

- Irányelvek fókuszálása az információkra és az emberekre, a technológia vagy a platform helyett
- Irányelvek tanítása, figyelemmel kísérése és érvényesítése
- Olyan eszközök megragadása, amelyek platform agnosztikusak
- Deduplikált adatok a felhőben.

Ugyanakkor ez a nyitott tér, ez a mindenki által használható és használt platform csábító terület a rosszakaratú felhasználók számára. A felhasználók részére most már egyre népszerűbb MDM (Mobile Device Management) lehetőséget nyújtani, mely segítségével a szolgáltatásba bevont mobileszközön lehet távoli törlést

végrehajtani, ha az eszköz rosszakaratú személy birtokába kerül. A publikus felhőszolgáltatást nyújtó szolgáltatók elsődleges feladata a felhasználóik adatainak megvédése, a felhő biztonságos kialakítása. A biztonság az egyik olyan legnagyobb aggasztó tényező, ami miatt a vállalatok hezitálnak a felhőbe való kiszervezéssel kapcsolatban, és ez a tényező a legnagyobb veszély a felhő számára. [5]

5 A felhőt minősítő szabványok

A felhőszolgáltatásokat leginkább minősítő szabvány az ISO 27001 – ami az alkalmazott információbiztonság megfelelően magas szintjét hivatott tanúsítani. 2013 őszén (2013. október 1.) jelent meg a szabvány legújabb verziója (ISO/IEC 27001:2013), mely új lendületet ad az információbiztonsággal irányítási rendszer szintjén foglalkozó szervezetek információbiztonsági törekvéseinek.

Az ***ISO/IEC 27001:2013*** szabvány az információbiztonsági irányítási rendszerek követelményszabványa, és mint ilyen ez képezi az ún. harmadik fél általi tanúsítások alapját. Szabályozni kell az adatok hozzáférésének jogosultságát, ahogyan az adatok sértetlenségét is, valamint biztosítani kell a rendelkezésre állást. A három területen tett erőfeszítések pedig kockázatelemzési szempontok alapján ki kell értékelni.

SLA - Nyilvános felhő esetén biztonsági felügyeletet a szolgáltatási szerződésben rögzített mértékig igényelhetjük. Itt csak olyan szintű monitorozást kérhetünk, amit a szolgáltató bevezetett, annál jobbat, alaposabbat, részletesebben ellenőrzőt nem, vagy csak igen jelentős költségtöbblettel. A szolgáltató ugyanis egyetlen ügyfél kedvéért csak jelentős többletért tud bevezetni új szolgáltatásokat.

6 Mikor biztonságos a felhő alkalmazása?

A versenyképes felhőszolgáltatók – lehetőleg az ISO 27001-es szabványoknak megfelelő, rendszeres auditálással – igazolni tudják, hogy adatközpontjaik fizikailag biztonságosak. A versenyképes felhőszolgáltatók jelenléti pontjainak korszerű, a legújabb hozzáférés-szabályozási és adatvédelmi technológiákat alkalmazó adatközponti létesítményeknek kell lenniük. A többéves és igazolható informatikai és adatvédelmi tapasztalatnak kiemelkedő jelentősége van, mivel nem csak a szolgáltató telephelyein működő hardverek biztonságára, hanem a szoftverbiztonságra – többek között a kötetek adattitkosítására, a kiszolgálói és adathozzáférés átfogó szabályozására és a részletes naplózásra – is ki kell terjednie. Az identitáskezelés talán a legfontosabb felhővel kapcsolatos biztonsági

kérdés. Azzal, hogy a felhasználók közvetlenül, önkiszolgáló portálokon keresztül érhetik el az informatikai erőforrásokat, az identitáskezelés szerepe minden eddiginél fontosabbá vált. [6]

7 Aktuális felhő trendek 2015-ig

A formális döntéshozatali keretrendszerek elősegítik a felhő befektetések optimalizálását.

- A hibrid számítási felhő elkerülhetetlen
- A felhőszolgáltatás brókerek megjelenése előmozdítja a felhő felhasználást
- A felhő központú tervezés szükségszerű lesz
- A számítási felhő hatással lesz a jövőbeli adatközponti és üzemeltetési modellekre

Sok magyar vállalat küzd azzal a problémával, hogy az egyszeri nagyobb méretű beruházási költséggel járó IT fejlesztést a szűkös anyagi feltételek miatt tolják maguk előtt. Ez akár éveket is jelenthet, magyar vállalatok szép számmal rendelkeznek már lejárt vagy a közelben lejáró szerver- operációs rendszer- vagy szoftverliszenszekkel. A válság miatt a felhő használata jó lehetőség az IT fejlesztésre, mivel fejlesztési költség, egyszeri beruházás nincs, csak a döntést kell meghozni, hogy felhőt használjanak. Az évekig halogatott IT fejlesztés így mégiscsak elérhető lenne. [7]

A felhőszolgáltatások használatát nem fogjuk tudni elkerülni. Az IT ezen az úton halad, a szolgáltatók nagyon sok pénzt és energiát fektetnek a számítási felhő megfelelő kialakításáért, fenntartásáért, és működtetéséért. De nekünk, felhasználóknak a felelősségünk az, hogyan használjuk, hogyan óvjuk meg adatainkat a veszélyektől, hogy ami rajtunk múlik, azt megtegyük annak érdekében, hogy biztonságot teremtsünk egy változó világban.

Referenciák

[1] https://www.microsoft.com/hun/megoldas-magazin/felho/biztonsag-es-megfeleloseg-a-felhoben/

[2] http://index.hu/tech/biztonsag/2012/08/06/veszelyes_felhoben_tarolni_az_adatokat/

[3] http://servira.com/tm/4.gyik/opengyik=first

[4] http://www.biztonsagosinternet.hu/tippek/szamitasi-felho

[5] http://hadmernok.hu/2011_4_kovacsz.pdf

[6] Zoltan Rajnai: Planification of a Transmission Network, In: Tibor Farkas, András Tóth New Trends in Signal Processing. Liptovsky Mikulas: Armed Forces Academy of General Milan Rastislav Štefánik, 2012. pp. 134-141.

[7] Bleier Attila – Dr. Rajnai Zoltán: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23.