Paper 07 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

IT Felhők Biztonsága

Albini Attila

Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 1034 Budapest, Bécsi út 96/b

Abstract. One of the latest and leading branches of information technology is cloud computing. Although it is only an eight years old technology, anyone can use these services nowadays. The first clouds were used in big companies to serve themselves. These were private systems with unique implementation and security system. Over time development enabled the standard and service oriented usage, so economic services could appear. The leaders of small companies are often not aware that the use of smart devices is based on the service provider's cloud technology. However, larger companies planned to use these services to implement business processes, taking into account the opportunities, risks and cost demands. So the service provider vital interest to achieve safer operation level. This includes topics of availability, capacity, performance , flexibility, measurability.

Keywords: cloud; safety; building; architecture; technology

Absztrakt. Az információs technológia egyik új és vezető területe a felhő-technológia. Bár ez csak egy nyolc éves technológia, bárki használhatja ezen szolgáltatásokat manapság. Az első felhőket nagy cégek alkalmazták saját maguk kiszolgálására. Ezek privát rendszerek voltak egyedi megvalósítással és biztonsági rendszerrel. Idővel a fejlődés lehetővé tette az egységes és szolgáltatás-központú használatot, így megjelenhettek az üzleti szolgáltatások. A kisvállalatok vezetői gyakran nincsenek tudatában, hogy okos eszközeik használata a telekommunikációs szolgáltató felhő-technológiáján alapszik. Viszont a nagy cégek tudatosan használják ezeket a szolgáltatásokat az üzleti folyamatok megvalósítása érdekében, számításba véve a lehetőségeket, kockázatokat, költségigényeket. Tehát a szolgáltató alapvető érdeke a magasabb biztonsági szint elérése. Ebbe beletartoznak a rendelkezésre állás, kapacitás, teljesítmény, rugalmasság és a mérhetőség témakörei.

Kulcsszavak: felhő; biztonság; építés; architektúra; technológia

Paper 07 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

1 Bevezetés

A felhőbiztonság témájában fellelhető dokumentációk nagy része a felhasználói adatintegritás vagy a törvényi felügyelet nézőpontjából vizsgálja a felhőszolgáltatást, s elsősorban a felhő határvédelmi és külső kommunikációs problémáit feszegeti. A felhőn belül alkalmazott logikai szintű biztonsági megoldásokról viszont nagyon kevés leírás található. A hiány megléte miatt választotta kutatási területének a szerző a felhőbiztonság technológiai oldalát. E területet körülhatárolván jelen írásban megemlítődnek elsősorban biztonsági szempontból: a felhő meghatározásának aspektusai, a felhő követelményei, építési technológiák, a felhő architektúrája, a felhő biztonsági modellezése.

2 A felhő elmélete

2.1 A felhő meghatározásainak bevezetése

Arra a kérdésre, hogy mi a felhő, jelenleg nincs egzakt megfogalmazás. Felhőszolgáltatás igénybe vételekor a szokásos három szereplő érintett: a szolgáltatás szállítója, megrendelője, valamint a szolgáltatás kereteit szabályozó szervezet. Ennek megfelelően a kérdés megválaszolásához másképp áll hozzá a felhasználó, a technológia előállítója, illetve független félként annak szabályzója. Ugyanakkor a megrendelő és a szállító közös szándékának kinyilvánításaként létrejön egy szerződéses keretrendszer, mely a szabályzó kereteken belül működik. Így a felhő meghatározását többféle aspektusból érdemes megtenni:

- független,
- felhasználói (megrendelői),
- szerződéses,
- technológiai (szállítói).

Az egyes nézőpontokban az alábbi faktorok a fontosak:

- a független szabályozás a rendszer viselkedésén keresztül közelíthető meg,[1]
- a megrendelő szemszögéből a gazdaságosabb üzleti megvalósítás a lényeges,
- a szolgáltató oldaláról a technikai jellegű paraméterek a fontosak,

- kettejük viszonyában a szerződésben kiköthető paraméterek a mérvadóak.

2.2 A felhő követelményeinek vizsgálata

A technológia vizsgálatakor kiderül, hogy a felhő legfontosabb tulajdonságai közé tartozik a megbízhatóság, a komponensek variálhatósága, változtathatósága, illetve a szolgáltatás mérhetősége is. Ezek alapján a kompetens technológiai követelményeket a következő témakörök köré lehet gyűjteni:

- Rendelkezésre állás – a rendszer létezése (lét),
- Erőforrások virtualizációja – a rendszer legalsó szintje (ismeret),
- Szolgáltatások virtualizációja – a rendszer legmagasabb szintje (cselekvés),
- Rugalmasság – a rendszer változtathatósága (Szabályzás és változás).

2.3 Felhőépítési technológiák vizsgálata

A rendelkezésre állás növelésére számos gyártói megvalósítás látott napvilágot, de működési elvüket tekintve csupán néhány fő technológia köré csoportosíthatók. Mindegyik technológia alapja a rendszerbe iktatott redundancia, azaz az erőforrások többszörözése. Az alaptechnológiák az alábbiak:

- Klaszter-technológia: a klaszter-technológia lényege, hogy több komponens végezheti ugyanazt a tevékenységet, de kívülről nézve egyetlen egységes szolgáltatásnak látszik. Demokratikus irányítás jellemzi, azaz a klaszter elemei egymással egyenrangú kapcsolatot tartanak fenn. Meghibásodás esetén a továbbra is használható komponensek közösen eldöntik, hogy milyen belső konstellációban folytatják a szolgáltatás biztosítását.[2][3].

- Grid-technológia: A grid-technológia alkalmazásakor a klaszterhez hasonlóan több komponens végezheti ugyanazt a tevékenységet és kívülről nézve egyetlen egységes szolgáltatásnak látszik. Azonban a klaszterrel szemben az irányítás itt autokratikus. Egy kontroller komponens vezérli a grid működését, kezeli annak belső adminisztrációját, elosztja a műveleteket a tagok közt, s végzi a szolgáltatások prezentálását.[4]

- Virtualizáció: A virtualizáció lényege, hogy a virtualizált architekturális réteg vagy rétegek tényleges erőforrásai el vannak fedve, s ezekből csak a szükséges mennyiségű és minőségű kapacitás van prezentálva a magasabb rétegek felé a számukra szükséges módon. Ez a technológia tette lehetővé a klaszter- és grid-technológiák továbbfejlődését, s a felhő-technológia kialakulását. [5]

- Split-technológia: A nagy adatközpontok megjelenése és a rendelkezésre állás növelésének szándéka következtében megfogalmazódott az igény arra, hogy a teljes telephely használhatatlanná válásával járó kockázatokat is a minimálisra lehessen csökkenteni. A megvalósítás alapeleme egy alacsony architektúra rétegben elhelyezkedő splitter komponens, amely a magasabb rétegek felől érkező kommunikációs forgalmat egyszerre több irányba továbbítja. Ezáltal lehetővé válik, hogy a rendszer sokad-példányai jelen lehessenek más-más fizikai helyeken is. Így adott telephely kiesésekor egy másik telephelyen indulhatnak el a rendszer komponensei.[3][6]

3 Általános felhő-architektúra szintézise

A Felhő általános architektúrájának szintézisét a vizsgálati alapelvek lefektetésével érdemes kezdeni. Mint minden más rendszert, e szerveződéseket is többféle aspektusból lehet vizsgálni. Ennek megfelelően az architektúra ábrázolása is többdimenziós lehet. A főbb felhőkomponensek gyártóinak (Cisco, Computer Associates, Dell, EMC, Fujitsu-Siemens, Hewlett-Packard, Hitachi, IBM, Microsoft, Oracle, VMware) megoldásaiban rejtező, egymást kiegészítő elemeket szintetizálva, az egyező elemeket általánosítva a kétdimenziós mátrixszerű ábrázolás tűnik kézenfekvőnek.

A vertikális dimenzió léptéke az egymásra épülés szerinti vizsgálat eredménye által létrejövő rétegstruktúra szintjei, mely megegyezik az emberi modellalkotás lényegi szintjeivel. Minden réteg a közvetlenül alatta és felette levő rétegekkel kommunikál, s egy adott réteg az alatta lévő réteg felhasználója, illetve a felette lévő réteg kiszolgálója. Felfelé haladva az egyes rétegek a következőek:

- Fundamentális réteg – az energiakezelés rétege,
- Hardver réteg – a fizikai megjelenés rétege,
- Virtualizációs réteg – a modellalkotás rétege,
- Műveleti réteg – a modell működési rétege,
- Menedzsment réteg – a rendszer időbeli működésének kezelése,

A horizontális dimenzió pedig az információelméleti paradigma elemei alapján történő taglalás a rendszer dinamikájának figyelembe vételével:

- Tárolás – a filozófiai Tulajdonság megnyilvánulása (adat),
- Átalakítás – a filozófiai Dolog megnyilvánulása (feldolgozás),

- Közvetítés – a filozófiai Viszony megnyilvánulása (kommunikáció),
- Statogenezis – az elsőrendű rendszerváltozások (szabályzás),
- Morfogenezis – a másodrendű rendszerváltozások (változásmenedzsment).

4 Biztonsági térmodellezés

Hatékony kockázatelemző, és ezen belül veszélyforrás elemző módszerek a kritikus rendszerek vizsgálatának kedveznek. E rendszerek alrendszerei a szűk keresztmetszet elvén egyforma prioritást élveznek, hiszen bármelyik alrendszer meghibásodása kritikus hatással van a rendszer egészének működésére.

A szerző által összeállított és bevezetett modellezés hatékonyabbá tudja tenni az olyan rendszerek vizsgálatát is, melyeknél az egyes alrendszerek prioritása, fontossága, kihatása eltérő, s elősegíti e rendszerek veszélyforrásainak egyszerűbb megtalálását. Ezen rendszerek lehetnek mechanikai, informatikai, de akár társadalmi rendszerek is. A modellezés célja a rendszerek biztonsági vizsgálatának elősegítésére egy olyan procedúra bevezetése, melynek végrehajtása után a folyamat produktuma a vizsgálandó rendszer releváns biztonsági aspektusrendszere. Vagyis a modellezés végén olyan aspektusrendszer áll elő, amely szerint érdemes megvizsgálni a rendszert a veszélyforrások elemzése érdekében. A relevancia és a vizsgálati spektrum határának kijelölése a vizsgálatot végző feladata.

4.1 A térmodellezés alapelve

A modellezéshez olyan nézőpont-rendszert kell keresni, amely minden rendszerben jelen van, értelmezhető. Bármilyen élő és élettelen, létező és elvont dolog egységes tárgyalására a vizsgálandóhoz kapcsolódó tudományágak szemléletrendszere lenne ideális. Ha olyan vizsgálati módszer kidolgozása a cél, amely független a dologhoz kapcsolódó tudományágaktól, akkor a filozófiai elemzés segíthet.

Az elemzés célja első lépésben tudományágak paradigmális alapjain keresztül megmutatni azt a sejtést, hogy a tudományágak paradigmális rendszerei egymás és a filozófiai alapparadigma analógiái. A sejtés logikai alapja az, hogy az összes jelenlegi tudományág a filozófiából alakult ki.[7]

Továbbá érdemes megmutatni, hogy a statikus paradigmák kiegészítése a rendszerváltozások időbeli vizsgálatával ismét filozófiai alapkérdések tárgyalásához vezet. S ezek után a modellezést a filozófiai alapkérdések köré érdemes szervezni.

4.2 A biztonsági térmodellezés fő lépései

1. A vizsgált rendszer általános modelljének elkészítése.
2. A támadás modelljének elkészítése.
3. Az általános modell és a támadás modelljének egyesítése révén alakul ki a biztonsági térmodell.
4. A modellezés alkalmazása után előáll a rendszer biztonsági aspektusrendszere.

4.3 Biztonsági térmodellezés alkalmazása a felhő-architektúrára

A szerző a bevezetendő térmodellezési eljárását alkalmazni fogja a felhő-architektúrára oly módon, hogy az már tartalmazza a humán erőforrással kapcsolatos aspektusrendszert is. Ebben az esetben a felhő-architektúra műveleti- és menedzsment rétege közé beékelődik az emberi tudás és pszichés kivetülését jelképező réteg. Továbbá a támadás modellezésénél is megjelenik ennek az új rétegnek a hatása.

Hivatkozások

[1] Mell, Peter - Grance, Timothy: The NIST Definition of Cloud Computing. Weboldal. USA. National Institute of Standards and Technology. 2011.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (Letöltve: 2016.09.15)

[2] Hewlett-Packard Development Company, L.P.: Managing Serviceguard Twentieth Edition. eBook. 2011. 407 p. HP Part Number: 5900-1869.

http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c02985067-1.pdf (Letöltve 2016.09.15)

[3] McCabe, John: Introducing Windows Server 2016 Technical Preview. First Printing. Redmond. Microsoft Press. 2016. 176 p. ISBN:978-0-7356-9773-7

[4] International Business Machines Corporation: Introduction to Grid Computing with Globus. Second Edition. New York. IBM Redbooks. 2003. 296 p. ISBN:0738427969

[5] Savill, John: Microsoft Virtualization Secrets. Indianapolis. John Wiley & Sons, Inc., 2012. 552 p. ISBN:978-1-118-29316-4

[6] EMC Corporation: Information Storage and Management: Storing, Managing, and Protecting Digital Information. Indianapolis. John Wiley & Sons, Inc., 2010. 480 p. ISBN:978-0-470-61833-2

[7] Dörömbözi János: A filozófia alapjai. Budapest. Nemzeti Tankönyvkiadó. 2011. 224 p. ISBN: 9789631964653