Műszaki Katonai Közlöny

XXII. évfolyam, 2012. 2. szám

Schubert Tamás[1], Póser Valéria, Ács Sándor,
Prém Dániel, Márton Judit, Kozlovszky Miklós

SZÁMÍTÁSI FELHŐ BIZTONSÁGI KÉRDÉSEI

Kivonat: A felhőszolgáltatások az informatika egyik legdinamikusabban fejlődő területévé váltak az utóbbi néhány évben. Az informatikai erőforrások és szolgáltatások igény szerinti, rugalmas, hálózaton keresztül történő igénybevétele jelentősen csökkenti a költségeket, ugyanakkor mind a szolgáltatás üzembiztonsága, mind az informatikai biztonság iránt fokozott igényeket támasztanak. Különösen igaz ez a felhőszolgáltatás kritikus informatikai környezetben történő alkalmazására. A „Számítási felhő biztonsági kérdései" c. TÁMOP kutatási projekt keretében feltárjuk az infrastruktúraszolgáltatást (IaaS) nyújtó felhők felhasználókat érintő biztonsági kérdéseket, kialakítunk az informatikai biztonságra (virtuális gépek, hálózatok, alkalmazások és tárolók) vonatkozó szolgáltatási szinteket. Cikkünkben rövid áttekintést adunk a felhőszolgáltatások jellegzetességeiről, az IaaS típusú felhők architekturális felépítéséről, a virtualizáció szerepéről a felhő megvalósításokban. Bemutatjuk egy széles körben használt nyílt forráskódú felhőszolgáltatás tulajdonságait. Végül a biztonság szolgáltatásként (Security as a Service – SECaaS) történő használatának lehetőségeit vázoljuk fel, ami várhatóan fontos szerepet kap a kutatási projektben.

Kulcsszavak: kritikus infrastruktúra, cloud, IaaS, számítási felhő, informatikai biztonság, SECaaS

Abstract: Cloud Computing has become one of the most dynamically developing area of the IT in the recent years. The on-demand and elastic use and the network access of the information resources and services significantly decreased the costs, but the expectations against such IT security criteria, as the availability of the services or the confidentiality of their data. This is especially true, when the clouds are used in critical IT environments. In the course of our TAMOP research project "Security issues of Cloud Computing", we disclose the security issues of the Infrastructure as a Service (IaaS) type clouds especially as far as the users are concerned. We work up information security service levels that include the virtual machines, networks, applications and storages. For a concrete cloud implementation, we develop such framework that automatically builds the security elements into the runtime system correspond to the security service level in question. In our paper, we describe the characteristics of cloud services, the architectural build up of the IaaS type clouds and the role of virtualization in the cloud implementations. We introduce the features of a widely used open source cloud implementation. Finally, we demonstrate the potential, how to use the security as a service (SECaaS), which will probably play an important role in our research project.

Keywords: critical infrastructure, cloud, IaaS, information security, SECaaS

1. Bevezetés

A felhőszolgáltatások az informatika egyik legdinamikusabban fejlődő területévé váltak az utóbbi néhány évben. A felhőszámítás (Cloud Computing) paradigma, ötvözi több technológia /elsősorban a virtualizáció, valamint grid (grid computing) és fürt (cluster computing) számítási koncepciók/ előnyös tulajdonságait. Mára minden technikai akadály elhárult az elől, hogy az informatika is - az áram- vagy a vízszolgáltatáshoz hasonlóan - szolgáltatássá váljék. A felhőszámítás jelenleg elsősorban a gazdasági szféra számára biztosít költséghatékony, megbízható, több rétegű szolgáltatási rendszert (a tudományos világ még mindig a grid-ek, illetve szuperszámítógépek erősen zárt világait használja, bár már itt is megfigyelhető növekvő intenzitású elmozdulás a felhő alapú megoldások irányába). A beruházási költségek a korábbinál sokkal kisebb mértékben merülnek fel az egyéni és a vállalati

[1] Óbudai Egyetem, Neumann János Informatikai Kar
schubert.tamas@nik.uni-obuda.hu, poserne.valeria@nik.uni-obuda.hu, acs.sandor@biotech.uni-obuda.hu, prem.daniel@nik.uni-obuda.hu, marton.judit@biotech.uni-obuda.hu, kozlovszky.miklos@nik.uni-obuda.hu

felhasználóknál. A publikus felhők esetében a szolgáltatásokért bérleti díjat kell fizetni. Az együttes bekerülési költség (CAPEX és OPEX) jelentősen csökken az erőforrások sokkal hatékonyabb kihasználása és az alacsonyabb üzemelési költségek miatt a szolgáltatóknál. Az erőforrások sokkal jobb kihasználása a kisebb energia felhasználás miatt jelentős környezetkímélő hatással is jár. Az utóbbi 5-7 évben a vállalatok felismerve a felhő infrastruktúrák által biztosított előnyöket (kisebb fenntartási költségek) egyre gyorsuló ütemben csökkentik saját infrastruktúra és ezekhez kapcsolódó szakértő humán erőforrás fejlesztéseiket és választják inkább a felhő infrastruktúrákat. A felhő rendszerek jelenleg egymástól elszigetelten, szigetszerű infrastruktúrákként működnek és az alábbi főbb szinteken biztosítanak szolgáltatásokat (a teljesség igénye nélkül):

- IaaS – infrastruktúra nyújtása szolgáltatásként (pl.: Amazon, Microsoft Azure, stb.)
- PaaS – platform nyújtása szolgáltatásként (pl.: Google, Microsoft Azure, Force.com, stb.)
- SaaS – alkalmazás nyújtása szolgáltatásként (pl.: SalesForce, a legtöbb WEB2 alkalmazás, online szoftverek, stb.)
- NaaS – hálózat nyújtása szolgáltatásként (pl.: Cisco, stb.)

Az egyes szigetszerű felhő rendszerek esetében általánosan elmondható, hogy közöttük az átjárás nehezen megoldott. A publikus felhőket használni szándékozó vállalatok jelenleg súlyos döntési helyzetben vannak és valójában a kedvező pénzügyi konstrukciók, vagy a biztonság között kell választaniuk. A felhő infrastruktúrába átültetett (virtualizált) alkalmazások, valamint a vállalatok belső adatainak felhőben történő tárolása csak akkor kivitelezhető, ha a vállalatok megbízhatnak az adott szolgáltatóban. A versenyképesség, megbízhatóság és bárhonnan/bármikor/bárhogyan történő elérhetőség érdekében a vállalatoknak el kell fogadniuk/hinniük, hogy a felhőszolgáltató megfelelően biztonságos, és adataik nem kerülhetnek illetéktelen kezekbe. A felhő szolgáltatóknak ehhez ugyanolyan vagy magasabb szolgáltatási minőséget kell garantálniuk, mintha a felhasználók saját informatikai kapacitással (hardver, szoftver, szakértelem) rendelkeznének. A szolgáltatási minőség az informatikai biztonságot is magába foglalja, melynek problémakörét célzottan kutatja jelen kutatási projektünk is. Távlatban olyan információ kritériumok teljesítésének vizsgálatával fogunk foglalkozni, mint az IT rendszerek rendelkezésre állása, bizalmassága, integritása, megbízhatósága, törvényeknek való megfelelése, hatékonysága, és célravezető minősége (COBIT 2007). Ez az általános értelmezés már közvetlenül támogatja az intézmények irányítását és működésének kiválóságát. Új kritériumokat is alkalmazunk majd. Ilyenek lehetnek például a dokumentáció, amely megköveteli, többek között, a változáskezelést és a konfigurációkezelést, vagy a funkcionalitás, amely a vállalati stratégiát az üzleti célokon keresztül támogatja (Szenes 2011).

A felhő infrastruktúrák és ezeken definiált szolgáltatások napjainkban már lehetővé teszik akár komplett cégek virtualizált üzemeltetését is, ahol nem csak a számítógépes programok, számítógépek, szerverek, de még maga a hálózat, sőt az adatközpont is teljes egészében virtualizált. A felhő infrastruktúrák teljes helyfüggetlenséget biztosíthatnak, ami egyik oldalról gyors és hatékony adatmigrációt, dinamikus erőforrás allokációt tesz lehetővé, másik oldalról azonban bizalmas adatok esetében problémát jelenthet a nemzeti határok és az adatintegritás garantálása. A felhőszolgáltatások eleinte csak a kisebb, erősen innovatív, korai elfogadó stratégiát követő cégek esetében voltak megfontolandó lehetőségek, azonban ez mára teljesen megváltozott, az utóbbi években már az összes nagyobb cég, sőt a web-es felhasználók többsége, sokszor tudtán kívül használ felhő infrastruktúrán működő szolgáltatásokat. Kritikus nagyvállalati, illetve kormányzati szintű infrastruktúrák esetében, amikor a kiemelt biztonságot igénylő alkalmazások adatainak nyílt felhőben való tárolása vagy a számítási erőforrások esetleges kiesése nem megengedhető, a nyilvános felhőszolgáltatás (public cloud) helyett adott adatközpontokban megvalósított magán felhőszolgáltatás (private cloud) biztosíthat hatékony megoldást. A kétféle szolgáltatás alap filozófiája és használt technológiája azonos, alkalmazható kibervédelmi megoldásaik jól átfedik egymást.

1.1. Kritikus infrastruktúra védelmi kutatások (TÁMOP-4.2.1.B-11/2/KMR) 2. alprojekt

1.1.1 Célja

A kutatási alprojekt célja az infrastruktúraszolgáltatást (IaaS) nyújtó felhők felhasználókat érintő biztonsági kérdéseinek feltárása, az informatikai biztonságra vonatkozó szolgáltatási szintek kialakítása, amelyek magukban foglalják a felhasználók virtuális gépeit, ezek hálózatait, alkalmazásait, tárolóit. Továbbá egy konkrét felhő implementációra olyan keretrendszer fejlesztése, amely a biztonsági szinteknek megfelelő biztonsági elemeket automatikusan beépíti a futtató környezetbe.

1.1.2 Célcsoportjai

A projekt keretében végzett elemzés feltárja a felhő infrastruktúrák jelen implementációiban fellelhető, felhasználókat érintő biztonsági hiányosságokat, biztonsági szolgáltatási szintekre tesz javaslatot, majd egy keretrendszerre épülő konkrét implementációt ad. Az Óbudai Egyetem az oktatáson keresztül is tervezi hasznosítani a projekt eredményeit, hiszen a kutatási eredmények egyes részei többek között az Informatikai biztonság szakirány tananyagának részévé is válnak.

1.1.3 Az alprojekthez kapcsolódó K+F+I tevékenység

A kutatási alprojekt keretében alapvetően infrastruktúraszolgáltatást (IaaS) nyújtó felhők felhasználókat érintő biztonsági kérdéseivel foglalkozunk. Ennek vonatkozásai:

- Védelem külső kibertámadások ellen IaaS felhőszolgáltatást használók számára;
- Sebezhetőség vizsgálat, adott virtuális gépek esetén a gépek biztonsági szintjének ellenőrzése, sebezhetőség vizsgálata;
- Felhasználók adatainak védelme;
- A virtuális gépek közötti biztonságos, titkosított kommunikáció a felhasználó szempontjából transzparens módon;
- A virtuális gépeken, illetve a tároló hálózaton elhelyezett adatok titkosítása a felhasználó szempontjából transzparens módon;
- Adatok áramlásának földrajzi korlátozása, ami nemzetközi infrastruktúrák esetén gyakran törvényi előírás;

A kutatási alprojekt várható eredményei:

- Az IaaS típusú felhőszolgáltatások használóit érintő veszélyforrások módszeres feldolgozása, dokumentálása;
- Az IaaS típusú felhőszolgáltatásoknál alkalmazott virtualizált infrastruktúrák biztonsági szintjének automatikus ellenőrzése, sebezhetőségük vizsgálata;
- A veszélyforrások elhárítását szolgáló automatizmus kidolgozása, és életképességének bizonyítása egy tesztkörnyezetben vizsgált minta-implementációban.

1.2. Mit értünk kritikus informatikai infrastruktúrán?

A nemzetközi gyakorlatnak megfelelően azokat az infrastruktúrákat tekintjük kritikusnak, melyek működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez, mint például az energiaellátó rendszerek, banki és pénzügyi rendszerek, közlekedés és szállítás, egészségügyi rendszer, kormányzat, kommunikáció- és információtechnológia, stb.

A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló Zöld Könyv alapján „kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak, stb.)”. (Green Paper 2005)

A kritikus informatikai infrastruktúrával szemben mind a szolgáltatás üzembiztonsága, rendelkezésre állása, mind az informatikai biztonsága iránt fokozott igényeket támasztanak. Ezeknek a fokozott igényeknek a kielégítése többnyire csak együttessen valósítható meg.

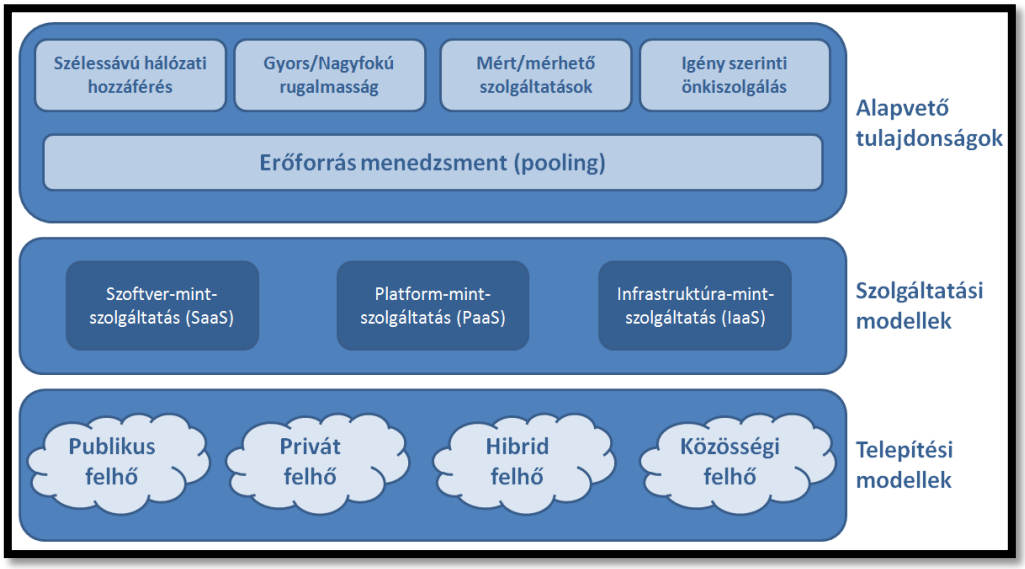
A rendelkezésre állást számszerűsíteni kell (pl.: öt kilences – five nines). Az informatikai biztonsággal szemben támasztott elvárásoknak egyen szilárdságúaknak kell lenniük a teljes infrastruktúrában.

A rendelkezésre állás és az informatikai biztonság paramétereit szolgáltatási-szint szerződésben (Service Level Agreement – SLA) kell rögzíteni, és mind a szolgáltatónak, mind az előfizetőnek/bérlőnek figyelemmel kell kísérnie.

2. A felhőszámítás meghatározása, jellemzői

A felhőszámítás - Cloud Computing meghatározásakor az *Institute for Standards and Technology (NIST) Information Technology Laboratory* definícióját szokás idézni, miszerint:

„A Cloud Computing olyan modell, amely lehetővé teszi konfigurálható számítási erőforrások (pl.: hálózatok, kiszolgálók, tárolók, alkalmazások és szolgáltatások) osztott készletének kényelmes, igény szerinti, hálózaton keresztül történő elérését, melyek gyorsan, kevés felügyeleti ráfordítással és szolgáltatói beavatkozással munkába állíthatók és eltávolíthatók. Ez a cloud modell öt lényeges tulajdonsággal rendelkezik, három szolgáltatási- és négy telepítési modellből áll (1. ábra)" (Mell és Grance 2011).



1. ábra Felhőszámítás – cloud computing vizuális definíciója (Mell és Grance 2011)

A felhőszolgáltatások keretében egyéni, kis- és nagyvállalati igényeket egyaránt kielégítő informatikai szolgáltatások érhetők el az interneten. Szabványos és testre szabható szolgáltatások, tetszőleges számú és teljesítményű számítógép és tárterület bérelhető előre megkötött szerződések szerint, vagy az igény felmerülésekor. Mindezt a világszerte kiépített hatalmas adatközpontok, a hálózati sávszélesség növekedése, a virtualizáció, az infrastruktúrát kezelő szoftverháttér, és új alkalmazásfejlesztő eszközök teszik lehetővé. A számítási felhő vagy Cloud Computing az informatikai szolgáltatások bérleti rendszerű igénybevételével szükségtelenné teszi az infrastruktúra helyi kiépítését. Az informatikai szolgáltatások olcsóbbá válnak, mivel az adatközpontok kihasználtsága többszöröse is lehet a helyi infrastruktúra kihasználtságánál. A vállalati informatikai beruházások a korábbinak töredékére esnek vissza, a bérleti költségek az igénybe vett szolgáltatással arányosan folyamatosan merülnek fel. A felhőszolgáltatás azonban számtalan kérdést vet fel a rendelkezésre állás és az informatikai biztonság szempontjából.

A kiemelt biztonságot igénylő vállalati alkalmazások esetén nem engedhető meg az adatok felhőben való tárolása vagy a számítási erőforrások esetleges kiesése, ezért a nyilvános mellett létrejött a vállalati adatközpontban megvalósított magán felhőszolgáltatás.

A felhőszolgáltatás öt lényeges jellemzője (Hurwitz et al. 2010):

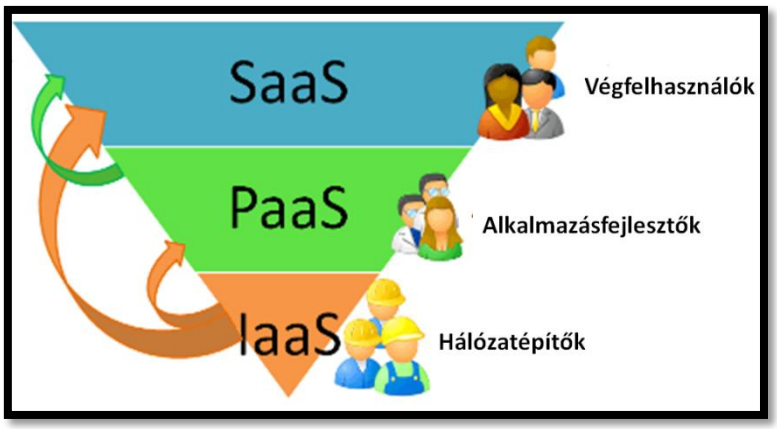
- **A szolgáltatás igény szerinti használata (On-demand self-service)**. A felhasználók egyoldalúan és emberi beavatkozás nélkül foglalnak számítógépi erőforrásokat (szerver idő, CPU teljesítmény, memória, hálózati tárolókapacitás).

- **Hálózati elérés**. A szolgáltatások távolról, hálózaton keresztül érhetők el a legkülönfélébb eszközök segítségével (PC, laptop, vékony kliens, mobil telefon, PDA).
- **Erőforrás készlet kialakítása**. A szolgáltató számítógépi eszközparkot hoz létre, amelynek erőforrásait a felhasználók dinamikusan, az igényeiknek megfelelően vehetik igénybe. A pillanatnyilag igénybe vett erőforrások helyére vonatkozóan a felhasználóknak általában nincs információjuk, bár egyes megoldásokban bizonyos absztrakciós szinten (pl. ország, adatközpont) lehet választásuk. Az erőforrás alatt többnyire tárolót, processzort, memóriát, hálózati sávszélességet és virtuális gépet értenek.
- **Rugalmasság (elasticity)**. Az erőforrások gyorsan, rugalmasan és gyakran automatikusan rendelkezésre bocsáthatók vagy visszaadhatók (quick scale out and scale in). Az elérhető erőforrások mennyisége a felhasználók számára gyakran korlátlannak tűnik, és bármikor bármilyen mennyiségben igénybe vehető.
- **A szolgáltatás mérése**. A felhő automatikusan vezérli és optimalizálja az erőforrások felhasználását, amelyet a szolgáltatás típusának megfelelő absztrakciós szinten (tároló, processzor, sávszélesség, stb.) méri. Az erőforrások felhasználását a felhő a szolgáltató és a felhasználó számára átlátható módon monitorozza, szabályozza, és dokumentálja.

Felhőszolgáltatások használata kritikus alkalmazási környezetben (pl.: közigazgatás, államigazgatás, honvédelem, stb.) is lehetséges, csak az adott környezetben elvárt SLA-t (rendelkezésre állás és biztonság) a szolgáltatónak (public, hybrid, private, community) garantáltan biztosítania kell. A felhőszolgáltatások használata kritikus alkalmazási környezetben is szükséges lehet, hiszen a felhőszolgáltatás fent vázolt öt lényeges jellemzője olyan előnyöket biztosít, amely csak extrém elvárások esetén szabad mellőzni.

2.1. Felhő szolgáltatási modellek

A 2. ábra szerint az egyes szolgáltatások közvetlenül más szolgáltatásokra épülnek, de nem minden esetben van ez így. Előfordul, hogy egy adott szolgáltatás típust olyan architektúrában valósítanak meg, hogy az igénybe vett szolgáltatások önálló szolgáltatásként nem jelenhetnek meg.



2. ábra Felhő szolgáltatási modellek

Infrastruktúra-mint-szolgáltatás (Infrastructure as a service - IaaS) Az infrastruktúra szolgáltatásként történő használata alatt szűkebb értelemben fizikai vagy virtuális számítógépeket értenek, tágabb értelemben a tárolókapacitások, a hálózati infrastruktúra vagy akár egy teljes virtuális adatközpont önálló használataként is értelmezik. Mivel a tágabb értelmezés fenti esetei önálló névvel is rendelkeznek, az IaaS jellemzőit a szűkebb értelmezéshez adjuk meg.

- A szolgáltatók a számítógépi erőforrásokat platform/szerver virtualizációs környezetben bocsátják az előfizetők rendelkezésére, bár igény szerint fizikai számítógépek használatát is lehetővé teszik;

- Az előfizetőknek nem szükséges az eszközöket (számítógépek, tárolók, hálózati berendezések, szoftver licencek, stb.) megvásárolniuk és üzemeltetniük;
- Az előfizetők az erőforrásokat kihelyezett szolgáltatásként vásárolják meg;
- Csak a ténylegesen használt erőforrásokért kell fizetni (pl. óránként);
- A szolgáltatás minősége (QoS) az SLA-ban rögzíthető;
- A szolgáltatás az internet segítségével érhető el;
- Ma már számos szolgáltatás vehető igénybe (pl. Amazon EC2, Amazon S3).

2.1.1 Platform-mint-szolgáltatás (Platform as a service - PaaS)

A Platform magában foglalja a felhő alkalmazás fejlesztésének, tesztelésének, telepítésének és üzemeltetésének teljes életciklusát, valamint sok esetben az ezekhez alkalmazható fejlesztői és üzemeltetői keretrendszereket. A teljes életciklus a felhőszolgáltatásra épül.

A PaaS jellemzői, előnyei:

- A felhőalkalmazások fejlesztését, tesztelését, telepítését, futtatását és felügyeletét ugyanaz az integrált környezet látja el (költségek csökkennek, minőség és rendelkezésre állás nő);
- A felhasználói kényelemet, a megfelelő válaszidőt, és a minőséget kompromisszum nélkül biztosítani kell (a hagyományos alkalmazásokéval azonos elvárások);
- A méretezhetőség, a megbízhatóság, és a biztonság járulékos fejlesztés, konfigurálás és költség nélkül biztosítható. Több bérlő kiszolgálása (multi-tenancy) automatikusan biztosítva van. Az adatok tárolásának, továbbításának és a pénzügyi tranzakcióknak biztonságosnak kell lenniük az alkalmazás teljes életciklusában;
- A Web szolgáltatások és adatbázisok elérése eleve alapértelmezett szolgáltatásként biztosított (távoli szolgáltatások és adatok elérése);
- Fejlesztők és fejlesztői csoportok támogatása biztosított. Az együttműködést a platformnak az alkalmazás teljes életciklusában külön konfiguráció nélkül biztosítania kell;
- Az alkalmazásba beépülő mélységi monitorozás segítségével a felhasználók aktivitását, a hibákat és a teljesítmény problémákat rögzítik. Ez az információ segíti a fejlesztőket az alkalmazásaik javításában és a felhasználók újabb elvárásainak megismerésében.

2.1.2 Szoftver-mint-szolgáltatás (Software as a service - SaaS)

A SaaS jellemzői, előnyei:

- Az alkalmazások az internet segítségével érhetők el és felügyelhetők;
- Az alkalmazások kizárólag internet böngészővel érhetők el, helyi installálás nem szükséges;
- Az alkalmazás adatstruktúrája (distributed model) és a program architektúrája lehetővé teszi az alkalmazás egyidejű használatát sok felhasználó számára (multi-tenancy);
- Uniformizált alkalmazások könnyen átültethetők a felhőbe. Az SaaS alkalmazásoknak kellően általánosnak kell lenniük, hogy sok felhasználó is használni tudja;
- Az alkalmazások testre szabása programozás nélkül, kizárólag paraméterezéssel elvégezhető;
- A kommunikáció biztonsága SSL használatával érhető el;
- A felhasználóknak nem kell szoftver licenceket vásárolniuk, kizárólag a szolgáltatásért fizetnek (pl. havidíj vagy felhasználónkénti díj);
- A SaaS alkalmazásoknak rendelkezniük kell mérő és monitorozó szolgáltatással, hogy az előfizetőknek csak a tényleges használatot számítsák fel;
- A SaaS alkalmazásoknak beépített számlázási szolgáltatással kell rendelkezniük;
- A SaaS alkalmazásoknak nyilvános fejlesztői/kapcsolódási felülettel és ecosystem partnerekkel kell rendelkezniük, akik kibővíthetik az előfizetők körét és az alkalmazás piaci részesedését;
- A SaaS alkalmazásoknak biztosítaniuk kell, hogy az ügyfelek adatai és speciális konfigurációi biztonságosan elkülönüljenek más ügyfelek adataitól és konfigurációitól;

- Az SaaS alkalmazások többnyire kifinomult üzleti folyamat konfigurátort biztosítanak az ügyfelek számára;
- A SaaS alkalmazásoknak állandóan új szolgáltatásokkal és képességekkel bővülhetnek;
- A SaaS alkalmazásoknak biztosítaniuk kell az ügyfelek adatainak integritását;
- A szoftver licenceket a szolgáltatók kezelik;
- A költség sok ügyfél között oszlik el;
- A szoftverkarbantartást a szolgáltató végzi;
- A verziókövetést a szolgáltató végzi;
- Az ügyfél hardver költségei csökkennek;
- Tömeges használat esetén a hardver méretezhetősége a szolgáltatónál könnyebben kézben tartható.

Lehetséges hátrányok:

- Hálózati problémák;
- Biztonsági hiányosságok;
- Szolgáltató függőség;
- Korlátozott testre szabhatóság.

Megjegyezzük, hogy a szolgáltatási modellek bemutatásakor csak a hagyományos (SPI modellek – Software, Platform, Infrastructure) megoldásokra tértünk ki. Terjedelem korlátok miatt nem foglalkoztunk az újabb keletű Service Broker-ek által nyújtott lehetőségekkel, melyek közvetítő, integrációs, monitorozó és irányító szolgáltatásokat biztosítanak.

2.2. Felhő telepítési modellek és szolgáltatásaik

A szolgáltatási modellektől (IaaS, PaaS, SaaS) függetlenül négy telepítési modellt dolgoztak ki, melyek mind különböző speciális felhasználói igényeket elégítenek ki.

2.2.1 Nyilvános felhő infrastruktúra (Public cloud)

A nyilvános felhő infrastruktúra a nagyközönség vagy egy nagyobb felhasználói csoport számára nyújt szolgáltatásokat, és a szolgáltatást nyújtó szervezet tulajdonában van.

A felhőszolgáltató vállalatoknak és magánszemélyeknek egyaránt kínál szolgáltatásokat.

Néhány példa, amikor a nyilvános felhő a legjobb választás:

- Sokak által használt szabványos szolgáltatás, pl. e-mail;
- Alkalmazások fejlesztése és tesztelése;
- Vállaltok által igénybe vett fokozottan biztonságos SaaS alkalmazás;
- Extra számítási kapacitás igénybe vétele csúcs időben;
- PaaS fejlesztő környezet használata.

2.2.2 Magán felhő infrastruktúra (Private cloud)

A magán felhő infrastruktúra kizárólag egyetlen szervezet számára nyújt szolgáltatásokat, melyet maga a szervezet vagy egy másik fél üzemeltet, és a szolgáltatást igénybevevő szervezet telephelyén vagy azon kívül helyezkedik el.

A magán felhő infrastruktúra használatának leggyakoribb okai:

- A titkossággal és a biztonsággal szemben támasztott fokozott elvárások;
- Irányítási és megfelelőségi követelményekhez történő igazodás;
- A vállalatok már rendelkeznek megfelelő infrastruktúrával, de jobb kihasználásra törekednek;
- A vállalatok a teljesítménnyel és rendelkezésre állással szemben fokozott követelményeket támasztanak;
- Bizonyos esetekben az erőforrások kihasználása elérheti a 90%-ot is.

2.2.3 Közösségi felhő infrastruktúra (Community cloud)

A közösségi felhő infrastruktúrán több szervezet osztozik, és valamilyen közös vonatkozással, érdeklődéssel bíró közösség számára nyújt szolgáltatást. Az üzemeltetést végezheti maga a szervezet vagy egy másik fél, és a szolgáltatást igénybevevő szervezet telephelyén vagy azon kívül helyezkedik el.

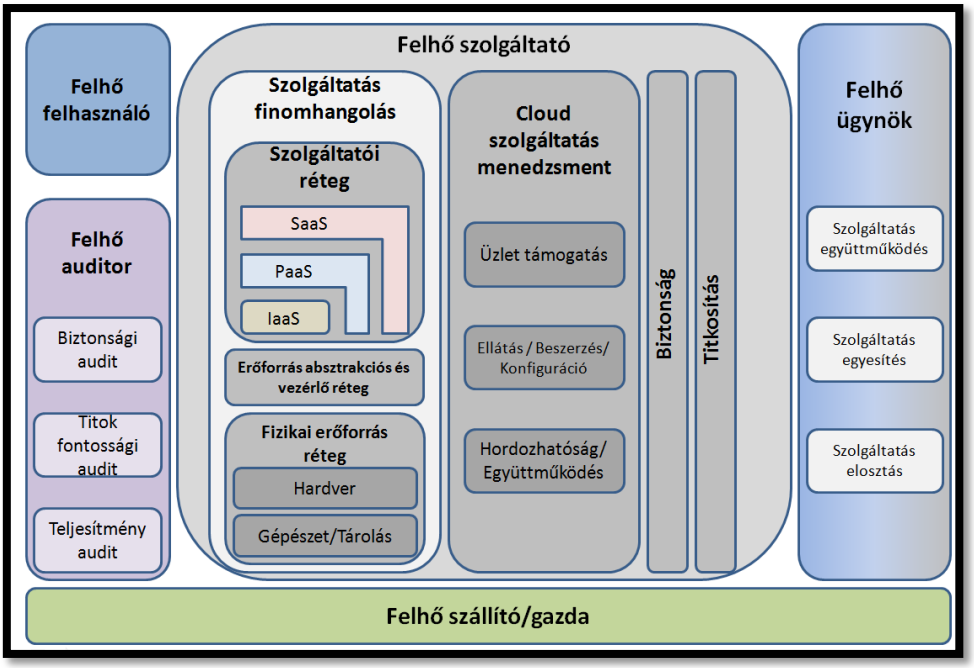
2.2.4 Hibrid felhő infrastruktúra (Hybrid cloud)

A hibrid felhő infrastruktúra két vagy több, más telepítési modellbe tartozó felhő kompozíciója, amely egyetlen felhőként jelenik meg. Az összekapcsolt felhők olyan szabványos vagy gyári protokollal vannak összekapcsolva, amely biztosítja az adatok és az alkalmazások mozgását/ hordozhatóságát.

A nyilvános és magán felhőszolgáltatás esetében alkalmazott technológiák jórészt azonosak. A magán felhőszolgáltatás esetében a beruházási költségek a vállalatnál merülnek fel, az erőforrások jobb kihasználása azonban csökkenti a fajlagos beruházási költségeket. A hibrid felhő a magán felhő összekapcsolása a nyilvános felhő infrastruktúrával.

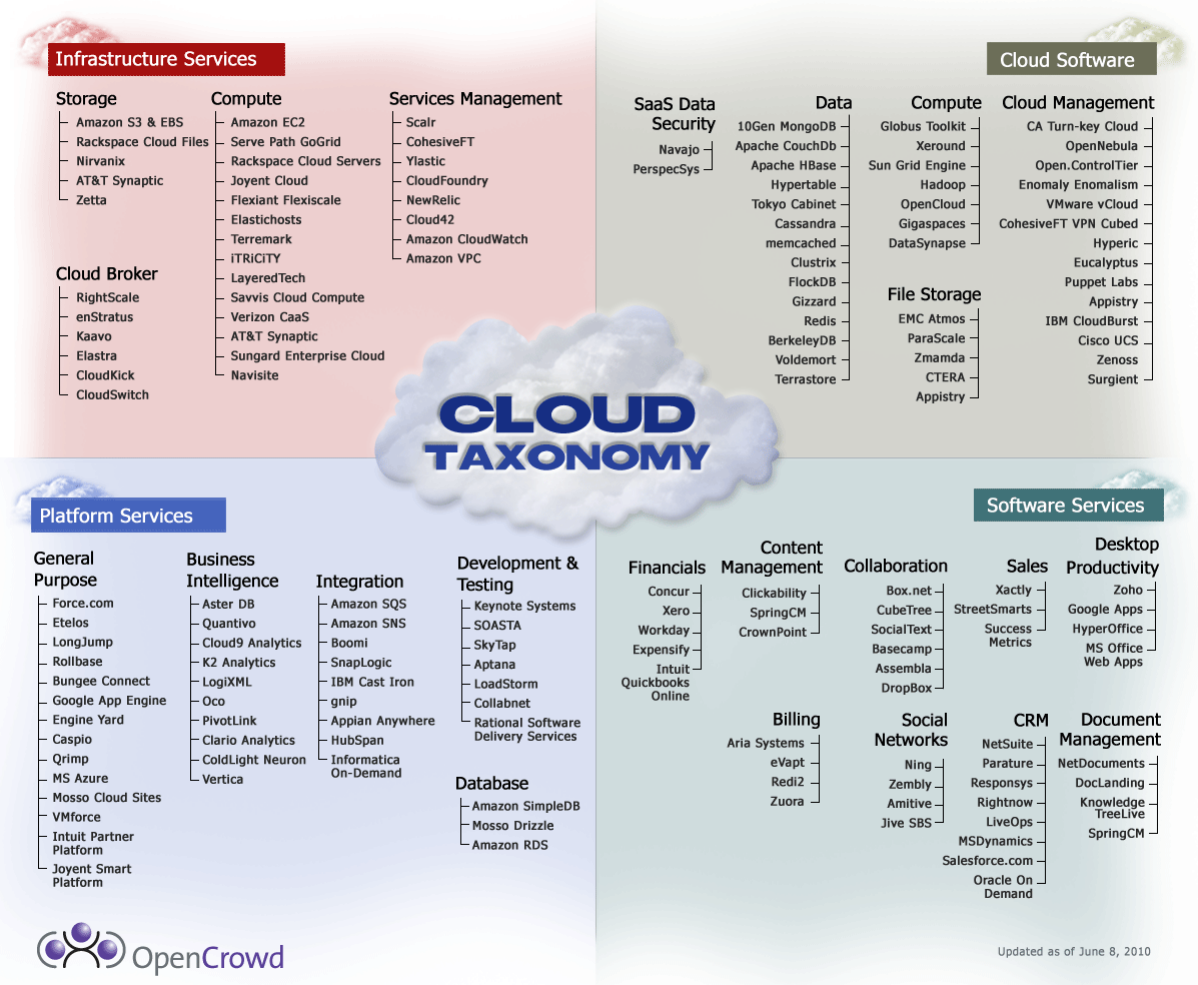
2.3. A felhő referencia modellje, taxonómiája

A NIST felhő számítási referencia modellje azonosítja a felhő főbb szereplőit, tevékenységeiket és feladataikat.



3. ábra A felhő számítás elvi referencia modellje (Liu et al. 2011)

A felhők szolgáltatásait, szolgáltatóit, eszközeit és fejlesztőit foglalja össze az OpenCrowd cég felhő taxonómiája. A taxonómiát az idők folyamán többször is frissítették, de sosem lehet teljesen naprakész a terület sokszínűsége és gyors fejlődése miatt. Készítésének célja, hogy párbeszédet nyisson a felhőszolgáltatások szállítói, üzemeltetői, fejlesztői és előfizetői között, és ezáltal előmozdítsa a felhőalkalmazások és szolgáltatások jobb megértését, könnyebb befogadását, és a teljesebb tájékozódást.



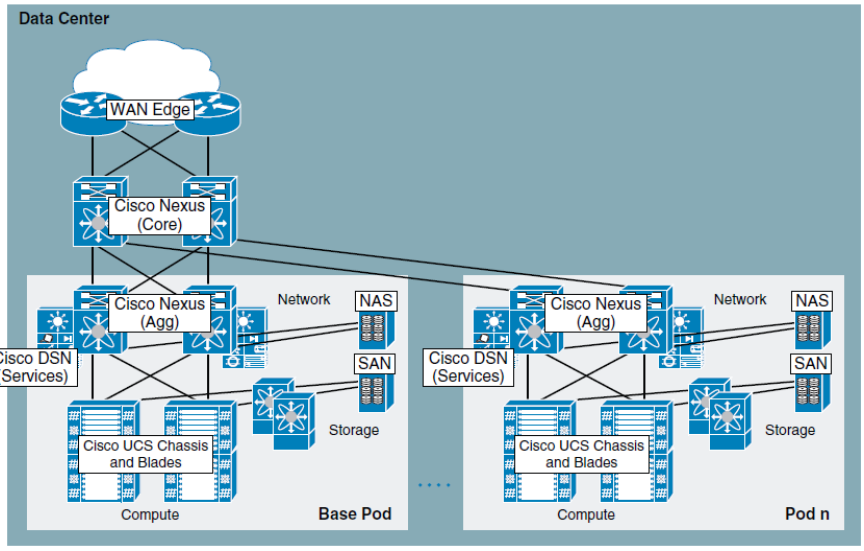
4. ábra Felhő taxonómia (OpenCrowd 2010)

2.4. Az IaaS típusú felhők általános architektúrája

Az IaaS szolgáltatói modell megvalósítása jelenleg gyártófüggő. A szabványosítási törekvéseket azonban jól mutatja, hogy számtalan nemzeti és nemzetközi testület, munkacsoport, egyesület, szabványosítási szervezet (ISBN 9781743041451) foglalkozik a felhők különböző aspektusainak szabványosításával. Példaképpen az *Open Cloud Consortium*-ot (OCC) említjük, amely a felhők és a felhők közötti együttműködés keretrendszerével kapcsolatos szabványok fejlesztését támogatja, benchmarkokat fejleszt a felhők vizsgálatára, és segíti referencia implementációk létesítését.

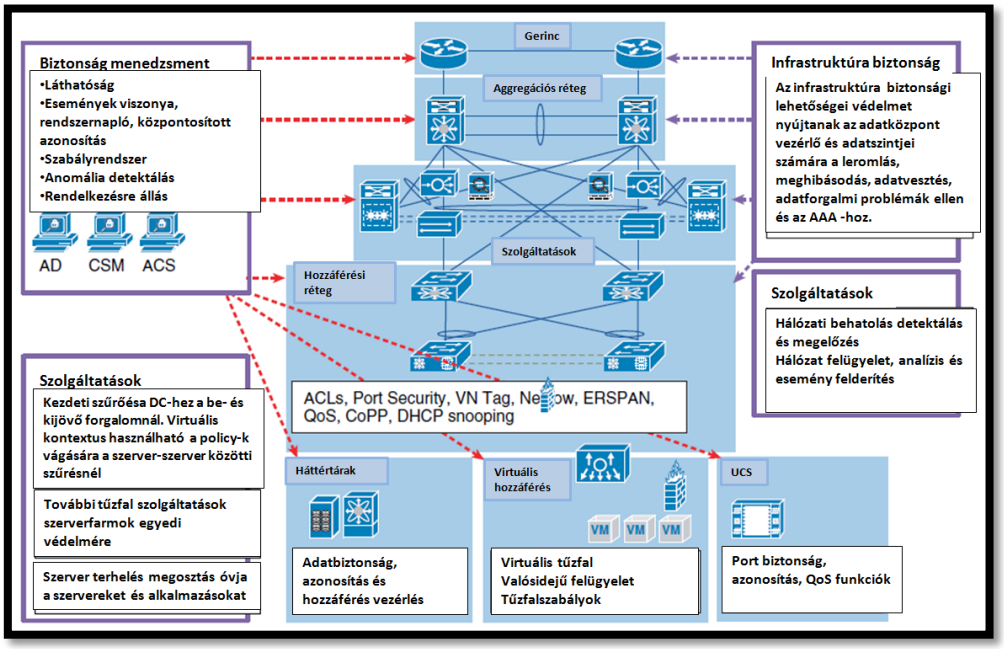
Az alábbiakban összefoglaljuk azon követelményeket, amelyeknek a mai IaaS implementációknak eleget kell tenniük:

- **Az IaaS keretében igénybe vehető szolgáltatások (Cisco 2012)**: számítási és tároló kapacitás, hálózati szolgáltatás és kiegészítő szolgáltatások (DHCP, DNS, terhelés elosztók, tűzfalak, NIDS/NIPS, stb.). E szolgáltatások a hagyományos adatközpontokhoz hasonló virtuális topológiában összeállíthatók és integrált szolgáltatásként nyújthatók (Virtual Multi-Tenant Data Center – VMDC). Az erőforrások közvetlenül fizikai eszközökkel vagy virtualizálva biztosíthatók.
- **Flexibilitás.** A felhő moduláris építőkockákból (point of delivery – pod) áll, amelyek számítási, tároló, hálózati, és egyéb standard elemekből épülnek fel. A felhő ilyen moduláris építőkockákkal bővíthető (5. ábra).



5. ábra Méretezhető adatközpont felépítése moduláris építőelemek segítségével (Cisco 2011)

- **Több bérlő támogatása (Multi-Tenancy)**. A szolgáltatást igénybe vevő bérlők adatainak, számítási erőforrásainak és hálózati forgalmának teljes elkülönítése.
- **Szolgáltatás megkülönböztetés**. A szolgáltatás mennyiségi és minőségi jellemzőinek megadása: CPU teljesítmény, virtuális gépek száma és teljesítménye, tároló kapacitás és megbízhatósági és biztonsági jellemzői, hálózati szolgáltatások, mint például VLAN szegmens hozzárendelés, minőségi paraméterek (QoS), biztonság, katasztrófatűrés, üzletfolytonosság, és más alkalmazás szintű tulajdonságok.
- **Rétegszerkezetű biztonság**. A felhő infrastruktúráját alkotó adatközpont a szokásos rétegstruktúrát (access, aggregation, core) követi. A virtualizált adatközpont minden rétegében megfelelő szintű biztonsági elemek vannak beépítve (6. ábra).



6. ábra A Cisco VMDC architektúra biztonsági keretrendszere (Cisco 2011)

- **Magas rendelkezésre állás (High Availability)**. A megfelelő szintű rendelkezésre állás a bérlők/előfizetők által igénybe vett valamennyi erőforrásra kiterjed és egyen szilárdságú. A HA biztosítása automatizált.
- **Széleskörű szolgáltatás menedzsment**. A szolgáltatás építőkockákból és a szolgáltatás biztosítás alrendszere biztosítja az automatikus konfigurálást és végrehajtást a szolgáltató és a bérlő számára egyaránt. Az önkiszolgáló, portál alapú modell lehetővé teszi a szolgáltatás minden részletre kiterjedő kiválasztását. Minden installálási és konfigurálási feladatot a rendszer automatikusan elvégez.

2.5. A virtualizáció szerepe a felhő infrastruktúrákban

A számítógép virtualizáció hatékonyabbá és olcsóbbá tette, valamint felgyorsította az alkalmazások és szolgáltatások telepítését és futtatását. Az operációs rendszer és futtató hardver elkülönítésével egy nagyon rugalmas modell jött létre. Ez a modell a fizikai számítógépeket egy általános erőforrás készletnek tekinti, a virtuális számítógépek pedig ebből az erőforrás készletből nyerik az erőforrás szükségletüket. Teljesítményük (CPU, memória) rugalmasan (elasztikusan) alkalmazkodhat a szükségleteihez. Akár futás közben is szabadon mozgathatók a fizikai számítógépek között. (Nicira 2012)

A tároló virtualizáció azt jelenti, hogy a fizikai vagy a virtuális számítógépek tetszőleges méretű és teljesítményű tárolót (logikai egység LU, kötet) vehetnek igénybe hálózaton keresztül függetlenül attól, hogy a tárolók hol helyezkednek el, a kötetek milyen szegmensekből tevődnek össze, a tároló milyen technológiára épül, és ki gyártotta. A kötetek mérete rugalmasan követheti az igényeket. Az elvárt szintű rendelkezésre állás megvalósítása transzparens a számítógépek számára. A tároló virtualizáció a tároló hálózatok (Storage Area Network – SAN és Network Attached Storage – NAS) megjelenésével vált elérhetővé. A tároló hálózatok nélkül lehetetlen lenne a virtuális számítógépek mozgatása a fizikai számítógépek között anélkül, hogy a virtuális gépekkel együtt ne lenne szükséges a tároló egység egyidejű mozgatása is. A hibatűrő rendszerek alkalmazásának szintén feltétele a tároló hálózatok használata.

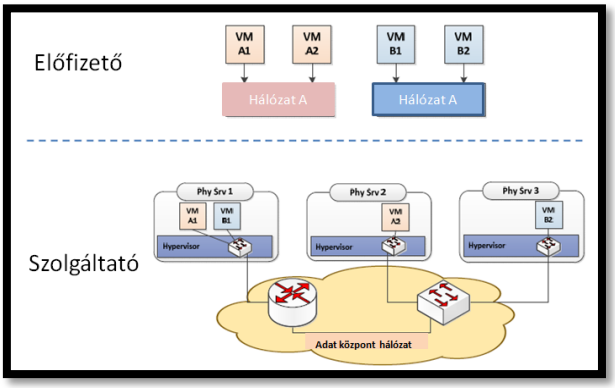
A számítógép és a tároló virtualizáció mintául szolgál arra, hogyan kell és érdemes átfogóan gondolkodnunk a teljes informatikai infrastruktúráról. A hálózat virtualizációjával kiegészül az informatikai infrastruktúra teljes virtualizációja. Ennek eredményeképpen bármely alkalmazás bárhol futhat, ami az automatizáció révén csökkenti a működési költségeket, az eszközök uniformizálása és konszolidációja révén pedig a beruházási költségeket.

A hálózat virtualizálása elkezdődött, de még nem fejeződött be. A hagyományos hálózati architektúrákkal és technológiákkal a hálózati virtualizáció meglehetősen nehézkes, jelentős terhet ró a hálózati rendszergazdákra és nehezen automatizálható.

A hálózati virtualizációval szembeni elvárások az alábbiak szerint foglalhatók össze (Josyula et al. 2012):

- Multi-tenancy (több bérlő): a felhő infrastruktúráját alkotó adatközpontnak több virtuális adatközpontot (Virtual Multi-tenant Data Center – VMDC) kell magában foglalnia, kiszolgálnia. Az adatközponti hálózatban az egyes virtuális adatközpontokhoz tartozó hálózati forgalmat teljesen el kell különíteni. Ehhez számtalan technológia és protokoll áll rendelkezésre (VLAN, Virtual Routing and Forwarding – VRF, többféle VPN, és számos újabb keletű, szabványosítás alatt álló megoldás). Ennek ellenére még homogén eszközkészlettel felépített adatközpontok esetén is csak az eszközök egyedi konfigurálásával lehet elvégezni a virtuális adatközpontok kialakítását. A feladat nehezen automatizálható, és a változtatás is nehézkes, időt rabló, és számtalan hibalehetőséget rejt magában.
- A virtuális adatközpont virtuális hálózatában biztosítani kell a megfelelő rendelkezésre állást, az elvárt minőségű hálózati szolgáltatást (QoS), és az IT biztonságot.

- A fizikai hálózat és virtuális hálózat felügyeletét el kell különíteni. A fizikai hálózat felügyeletét a felhő szolgáltatója (adatközpont üzemeltető), a virtuális hálózat felügyeletét pedig a bérlő látja el.
- A virtuális számítógépek egymás közötti forgalmát virtuális kapcsolók látják el, amelyek gyakran nem nyújtanak olyan biztonsági (magán VLAN, ACL, stb.) és egyéb szolgáltatásokat, mint a hagyományos hardver kapcsolók. A virtuális gépeknek a fizikai számítógépekhez hasonlóan a kapcsolt hálózat részévé kell válnia.
- Az azonos bérlőhöz tartozó virtuális gépeknek ugyanazon a Layer 2-es hálózaton kell lenniük, és nem keveredhetnek más bérlők virtuális gépeivel, függetlenül attól, hogy azonos fizikai számítógépen több bérlő virtuális gépei is futhatnak. Vagyis a hálózat fizikai (szolgáltatói) nézete és a virtuális (bérlői) nézete teljesen elkülönül. Ha ez az elvárás megvalósul, a virtuális hálózat ugyanúgy működik, mintha a bérlő egy dedikált hálózattal rendelkezne. A szórásos és a többes címzésű üzenetekre, valamint az IP címzésre vonatkozó szabályok továbbra is érvényesek. Tehát a címtérnek is virtualizáltnak kell lennie. A fizikai számítógépek címtere elkülönül a virtuális számítógépek címterétől. Ez a megoldás lehetővé teszi azt is, hogy a különböző bérlők IP címterei átfedésben legyenek, így a virtuális gépek szabadon mozgathatók egyik fizikai gépről a másikra.
  A fenti feladat megoldására számos megoldást dolgoztak ki (VLAN-VRF, nvGRE, VxLAN, stb.).



7. ábra A szolgáltató és az előfizető másként látja a hálózatot (Orlando 2012)

- Az adatközpontok méretezhetősége a virtualizációval szintén új megvilágításba kerül. Egy több bérlős adatközpontban, ahol egy-egy fizikai számítógép hypervisora 20-80 VM-et is futtat, a virtualizációnál használt technikák könnyen méretkorlátokba ütköznek. A VLAN-ok maximális száma 4096, a VRF táblák, MAC-címtáblák mérete, és a használható ACL-ek száma szintén erősen korlátos.
- A hagyományos adatközpontokhoz hasonlóan a virtuális adatközpontok is integrált szolgáltatásokkal egészülnek ki. Ilyen szolgáltatások például a DHCP és DNS, az alkalmazás szintű tűzfalak, a mélységi forgalomelemzők, a behatolás érzékelők (IDS/IPS eszközök), a szerver terheléselosztók. E szolgáltatásokat megvalósíthatják kapcsolókba épített vagy önálló virtualizált hardver eszközökkel, külön virtuális gépen alkalmazott szoftver modulokkal, vagy a hypervisorba integrált szoftver modulokkal. Az előbbi két esetben meg kell oldani a forgalom átirányítását a szolgáltatást ellátó eszközbe, az utóbbi esetben a szolgáltatás a hypervisort futtató fizikai számítógép erőforrásait veszi igénybe.
- A hálózat virtualizációját teljesen automatizálni kell, hiszen virtuális adatközpontok létrejönnek, megszűnnek, topológiájuk átalakul, változik a hálózathoz tatozó virtuális gépek száma, változik a terhelésük, ezzel változik a virtuális hálózati összeköttetések sávszélesség igénye. E változásokat dinamikusan követni kell úgy, hogy közben ez ne befolyásolja az adatközpont többi bérlőjének munkáját.

3. Nyílt forrású felhő infrastruktúrák

Léteznek nyílt forrású felhő megoldások, amelyek abban különböznek a kereskedelemben kapható felhő implementációktól, hogy a szoftver teljes verziója és annak forráskódja szabadon elérhető, módosítható és felhasználható. Az első széles körben elterjedt szabad forrású felhő megoldás az Eucalyptus volt, amely az Amazon EC2 és S3 szolgáltatásait és interfészeit vette példaként. Az Eucalyptus sikere után számos nyílt forrású felhő fejlesztése kezdődött, de ezek közül elterjedtsége és támogatottsága miatt az OpenNebula és az OpenStack emelkedik ki.

3.1. Az OpenNebula felhő

A nyílt forráskódú OpenNebula szoftver segítségével ipari felhasználásra alkalmas számítási felhő építhető komplex és heterogén rendszerekből. Az OpenNebula project célja, hogy a legújabb technológiákat alkalmazó, jól méretezhető, minőségi és megbízható szoftver eszközkészletet nyújtson felhő infrastruktúrák menedzseléséhez. A szoftver fejlesztése egy 2005-ben indult kutatással kezdődött, melynek témája az elosztott rendszereken futó virtuális gépek hatékony és méretezhető menedzselése volt. Az első hivatalos kiadás 2008-ban jelent meg (az aktuális verzió: 3.6).

Az OpenNebula segítségével helyi erőforrásokból privát felhők alakíthatóak ki, de alkalmas publikus és hibrid felhő infrastruktúra (mint az Amazon EC2 rendszere) építésére is. Az alkalmazás számos innovációt elősegítő nyílt rendszert és kutatást szolgál ipari és akadémiai közegben egyaránt.

3.2. Az OpenNebula infrastruktúra tulajdonságai

Az OpenNebula a tervezési elvek alapján és az ipari szintű használhatóság érdekében a következő tulajdonságokkal rendelkezik:

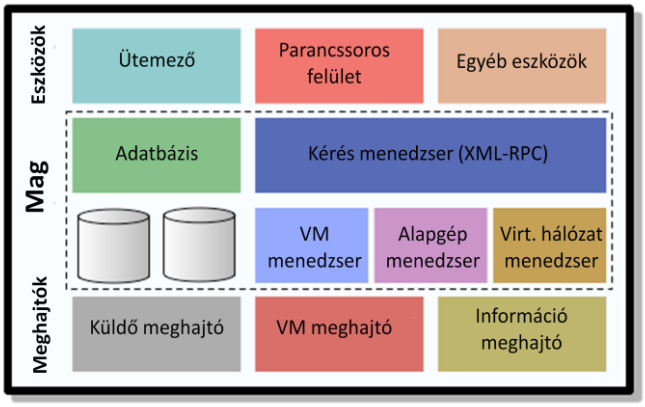
- **Nyílt.** Architektúrája, felülete és kódja szabadon hozzáférhető, felhasználható, továbbfejleszthető;
- **Biztonságos.** A rendszert használók feljogosítása jelszón, RSA[2] kulcspáron, LDAP[3]-on vagy SSL[4] csatornával biztosított külső forráson alapul;
- **Alkalmazkodó.** Képes különböző hardver és szoftver eszközök integrálására;
- **Együttműködő és hordozható;**
- **Stabil.** Ipari használatra is alkalmas;
- **Nagy teljesítményű;**
- **Méretezhető.** Nagy kiterjedésű infrastruktúrák létesítésére is alkalmas;
- **Megbízható;**
- **Szabványos.**

A szoftver három virtualizációs technológiát támogat: Xen, KVM, VMware.

3.3. Az OpenNebula architektúra

Az OpenNebula architektúrája három rétegre bontható (8. ábra). Az Eszközök-réteg feladata, hogy menedzsment eszközöket nyújtson a mag felületéhez. A Mag-réteg tartalmazza a központi virtuális gépet, tárolóeszközt, virtuális hálózatot és az alapgép menedzsment komponenseit. A Meghajtók-réteg felel a különböző virtualizációs technológiák, tárolók, monitorozó eszközök és felhőszolgáltatások Mag-réteghez való csatlakoztatásáért.

2 RSA: Ron Rivest, Adi Shamir és Leonard Adleman által kifejlesztett nyílt kulcsú (vagyis „aszimmetrikus") titkosítás
3 LDAP (Lightweight Directory Access Protocol): Könnyűsúlyú Címtár-Hozzáférési Protokoll
4 SSL (Secure Socket Layer): Protokoll réteg, amely a kliens és szerver közötti kommunikáció biztonságáért felel



8. ábra: Az OpenNebula architektúrája

A rendszer használatához szükséges interfészek között található a felhasználók számára készült webes felületen kívül számos API és parancssoros eszköz, amelyek a nyílt és szabványos OCCI interfészen kívül a de facto szabvánnyá vált EC2 interfésszel is kompatibilisek.

4. Security as a Service (SECaaS) alkalmazása biztonsági szempontból kritikus környezetben

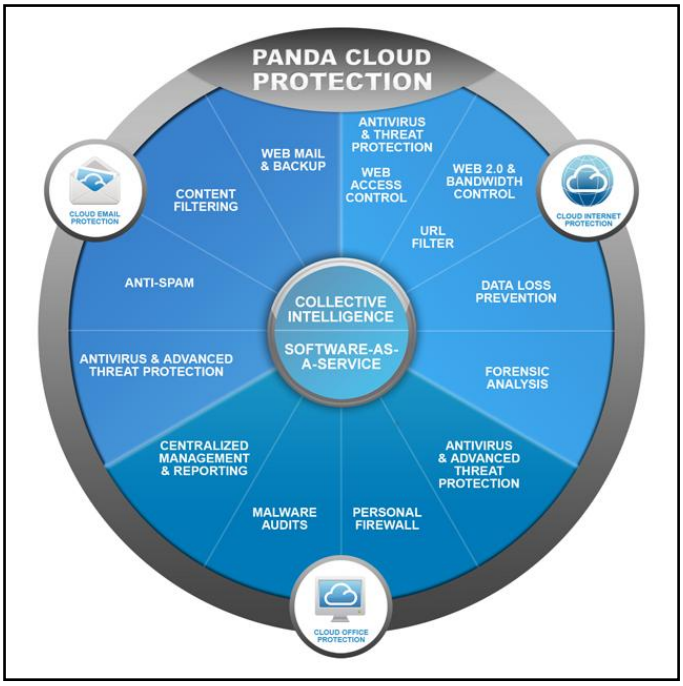
Az elmúlt években egyre több infrastruktúra esetében tudatosan alkalmaznak felhőszolgáltatásokat, de az is előfordul, hogy a felhasználók észre sem veszik, hogy felhő szolgáltat nekik, nem pedig egy helyi szerver. Leginkább azt tapasztalhatják, hogy minden jól és gyorsan működik. A felhő technológiák előnyeinek kihasználása céljából egyre több cég fordul az IaaS, a PaaS, a SaaS, vagy éppen a SECaaS megoldások felé annak érdekében, hogy csökkenteni tudja a vállalaton belül felmerülő költségeket. Bár sokan még kételkednek e technológiák biztonságos voltában, ennek ellenére egyre több informatikai biztonsági eszközöket gyártó cég (pl. McAfee, Panda Security, Symantec, stb.) fejleszt és kínál felhő alapú biztonsági szolgáltatásokat.

4.1. Mi is az a SECaaS?

A SECaaS egy olyan felhő alapú szolgáltatás, ami biztonsági alkalmazások és megoldások távoli igénybe vételét teszi lehetővé általában virtuálisan kiépített csatornán keresztül. Olyan felhő számítási modell, mely biztonsági szolgáltatásokat menedzsel az interneten keresztül. A SECaaS a Software as a Service (SaaS) modellen alapul.

Kezdetben a Security as a Service megoldásokban csupán áthelyezték a központosított irányítást a felhőbe, majd fokozatosan kiaknázták a felhőszolgáltatásban rejlő erősségeket. Például a Panda Security rengeteg helyi számítási erőforrást takarított meg azzal, hogy a rosszindulatú szoftverek vizsgálatát felhőben bonyolította ahelyett, hogy a vállalat asztali számítógépein egyenként tette volna ezt meg. Ennek eredményeképpen sokkal több kapacitást sikerült megtakarítani, mintha egyszerűen az ügyfél oldalon végezték volna a vizsgálatokat, valamint emellett lehetőség nyílt az egyes számítógépeken felfedezett veszélyekhez kapcsolódó információk összegyűjtésére, könnyen átlátható, fenyegetésekre vonatkozó halmazba integrálására is. (Matt 2012)

A rosszindulatú szoftverek elleni védelem mellett természetesen más szolgáltatás is rendelkezésre áll. Például a 9. ábrán láthatóak a Panda Security által kínált felhő alapú biztonsági szolgáltatások.



9. ábra: A Panda Security által kínált szolgáltatások (Panda Security 2012)

4.2. A SECaaS alkalmazásának előnyei és hátrányai

A SECaaS alkalmazásának előnyeit az alábbiakban foglaljuk össze:

- Nincs szükség hardverek vagy szoftverek vásárlására, karbantartására, a SECaaS szolgáltató biztosítja;
- Csökkentett sávszélesség használat;
- A felesleges e-mailek csak a felhőig jutnak el (a bejövő e-mailek legnagyobb része spam);
- Megbízható adatközpont rendelkezésre állás;
- Néhány vállalat SECaaS megoldással egyszerűen össze tudja kötni a vállalat infrastruktúráját és a biztonsági beruházásokat;
- Jellemzően gyorsabb kivitelezés és a külső forrású szakmai hozzáértés miatt rendkívüli mértékben csökken a kockázat;
- Könnyű méretezhetőség;
- Ugyanarra a problémára több szolgáltatás áll a megrendelő rendelkezésére;
- Igénybevétel szerinti költségek;
- A biztonsági feladatok kiszervezésével a szervezetek több időt fordíthatnak a fő feladatkörükre;
- IT-s szakembert nem feltétlenül igényel, nem szükséges a helyszínre küldeni, egyszerűen megoldható a felhő segítségével;
- Alacsony bevezetési költség és még alacsonyabb a használat során felmerülő költség a tulajdonos számára;
- A forgalmazót anyagi érdekeltség köti a megfelelő működéshez, mert, ha a szolgáltatás bevezetése nem sikeres, a szolgáltató elveszti az előfizetőt;
- Az adminisztratív feladatok pl. log fájlok kezelése külső helyen történik, ezáltal időt és pénzt takarítva meg és lehetőséget biztosítva, hogy több idő maradjon a fontosabb feladatokra;
- Folyamatos vírus definíciós frissítések;
- Nincs szükség felhasználói beavatkozásra;
- Web és e-mail biztonság. (Online-crm 2012)

Hátrányok:

- Egy szolgáltatás esetleges meghibásodása vagy feltörése esetén a felhő nagysága miatt dominó effektus alakulhat ki.
- A cégeknek aggodalomra ad okot egy más cégekkel közösen alkalmazott eszköz használata. Bizalmas információkat nem szívesen adnak ki.
- Bizonyos speciális üzleti területtel foglalkozó vállalatnak szüksége van az ahhoz kapcsolódó alkalmazásokra. Ezek az alkalmazások annyira speciálisak, hogy a SECaaS megoldásokban nem elérhetők vagy egyszerűen nem megoldható a működésük jelenleg.
- Sok SECaaS megoldás esetén még mindig szükséges egy-egy szoftver telepítése a vállalat összes számítógépén az automatikusan elvégezhető telepítések, illetve a frissítések miatt. (Online-crm 2012)

A SECaaS szolgáltatások biztosítása még nagyobb kihívás, mint a normál szolgáltatásoké:

- különböző architektúrák, funkciók és megvalósítások;
- nincs egy világszinten elfogadott keretrendszer kialakítva;
- a vállalatok nagy része még nem áll készen ilyen szolgáltatások biztosítására;
- a felhő sebezhetősége (felhő specifikus biztonsági rések):
  - adatok megőrzése;
  - fizikai hozzáférés ellenőrzés;
  - titkosítási kulcsok kezelése;
  - alacsony szinten vagy egyáltalán nem monitorozható az operatív hozzáférés és/vagy a szolgáltatás menedzsment;
  - a felhő környezet nem teszi lehetővé, megnehezíti vagy hatástalanítja a hagyományos ellenőrzési eljárásokat (Forensic, havi biztonsági audit, biztonsági értékelések, stb.);
  - a felhasznált felhő technológiák is okozhatnak sebezhetőséget: a technológia velejárói (pl.: virtual machine escape), a felhőbe implementálás következményei (pl.: session visszaélés/eltérítés).

4.3. A Cloud technológiák szabványosítása

Az előbbi hátrányokon kívül jelentős problémát jelent a SECaaS biztonsági szempontból kritikus környezetben történő alkalmazásában, hogy a felhő technológiákra vonatkoztatva nincs egységes előírás, a szabványosítás ezen a területen még gyerekcipőben jár. A felhő szabványokkal, ajánlásokkal több szervezet is elkezdett már foglalkozni (cloud-standards.org).

2010 tavaszán a Novell és a Cloud Security Alliance (CSA) meghirdette az iparág első szállító független, számítási felhőkre vonatkozó biztonsági tanúsítási programját (Trusted Cloud), melynek célja a szolgáltatók segítése az ajánlásoknak megfelelő, biztonságos és az ügyfelek meglévő informatikai rendszerével együttműködő megoldások kidolgozásában. Kiterjed a felhőalapú megoldások bevezetésekor kényes területnek minősülő személyazonosság-kezelési, hozzáférési és megfelelőségi megoldások konfigurációira.

Az USA kormánya kezdeményezte a felhő szolgáltatások megrendszabályozására alkalmas ajánlások kidolgozását (mik azok a biztonsági intézkedések, amelyeket egy szolgáltatónak foganatosítania kell, és melyek azok, amiket az előfizetők számon kérhetnek).

2011 februárjában a NIST kiadott egy dokumentumot (ajánlások), melynek célja a felhő számítási környezetek biztonsági követelményeinek meghatározása. Elsősorban a nyilvános felhő szolgáltatásokkal foglalkozik:

- Általános tudnivalók, megfelelőségi és felügyeleti kérdések, az architekturális követelmények.
- Külön foglalkozik az azonosság- és hozzáférés kezeléssel, az adat- valamint szoftverizolációval és az adatvédelmi nehézségekkel.
- Ajánlásokat tesz a rendelkezésre állással és az incidenskezeléssel kapcsolatban. (Kristóf 2012)

A Cloud Security Alliance ajánlásai a biztonság minden területére kiterjednek.

A CSA ajánlásai között szerepel többek között, hogy a biztonságnak és az adatvédelemnek már a rendszerek fejlesztési életciklusának tervezési szakaszában meg kell jelenniük (maximális hatékonyság és a minimális költségek), mert a megvalósítás után a biztonsági kérdések kezelése

nemcsak bonyolultabb és költségesebb, hanem kockázatosabb is. Továbbá, hogy a szervezeteknek olyan szolgáltatásokat kell választaniuk, amelyek a bevezetés, a konfigurálás és a felügyelet szempontjából is megfelelnek a biztonsági követelményeiknek. (Simmonds 2011)

5. Összefoglalás

Jelen cikkünk 1. fejezetében bemutattuk a számítási felhők (Cloud Computing) főbb jellegzetességeit, tulajdonságait, gyors elterjedésének okait, előnyeit és hátrányait. Meghatároztuk a cikk hátteréül szolgáló, a „Számítási felhő biztonsági kérdései" c. TÁMOP kutatási projekt (TÁMOP-4.2.1. B -11/2/KMR-2011) céljait, célcsoportjait és kutatási-fejlesztési feladatait.

A későbbiekben bevezettük a felhő szolgáltatás fogalmát, áttekintettük a felhők szolgáltatási és telepítési modelljeit, bemutattuk a felhők fejlesztők/gyártók/szolgáltatók funkcionalitás szerinti osztályozását (felhők taxonómiája). Ez az osztályozás jól mutatja a felhők várható fokozott térnyerését az informatikai szolgáltatásokban. Egy további tendencia is megmutatkozik, nevezetesen az informatika minden részfeladatának szolgáltatásként történő megjelenése, és ezek összekapcsolása komplex informatikai szolgáltatások nyújtásában.

A felhők elvi referencia modellje segítségével tekinthető át az IaaS típusú felhőszolgáltatás moduljainak egymáshoz kapcsolódása. Az IaaS típusú felhők architektúráját a Cisco cég által megvalósított Virtual Multi-tenant Data Center (VMDC) segítségével szemléltettük. A Cisco megoldása jól mutatja, hogy a hálózati biztonsági elemek hogyan épülhetnek be egy virtuális adatközpont topológiájába, és hogy a hálózati biztonság megteremtésében hogyan kaphatnak szerepet mind hardver mind pedig szoftver elemek. A virtualizáció az infrastruktúra minden elemét érinti, de kiemelten kezeltük a hálózat virtualizációját, mivel egy sokkal újabb keletű technikáról van szó, mint a számítógép, vagy akár a tároló virtualizációja. A hálózat virtualizációja teszi lehetővé virtuális topológia létesítését, és ezzel a bérlők forgalmának teljes elszigetelését, valamint a virtuális gépek és az alkalmazások szabad mozgatását a felhőben és a felhők között.

A 3. fejezetben egy széles körben használt nyílt forráskódú felhőszolgáltatás tulajdonságait mutattuk be. Ahogyan a világszerte működő felhő megvalósításokban, úgy a kutatási projektünkben is fontos szerep vár a nyílt forráskódú implementációkra, hiszen a fejlesztésükben résztvevő cégek és magánszemélyek komoly szellemi potenciált jelentenek, és olyan újszerű megoldások kerülnek ki a kezeik alól, amelyek a felhők további fejlődésére is hatást gyakorolnak. Másrészről a nyitottságuk teszi lehetővé, hogy a kutatási feladatunk számára megfelelő környezetet biztosíthassunk.

A 4. fejezetben a felhők biztonsági kérdéseivel foglalkoztunk, ennek is egy viszonylag újszerű megvalósításával az informatikai biztonság szolgáltatásként történő kezelésével (Security as a Service – SECaaS). Már ma is léteznek felhőből hagyományos infrastruktúra vagy felhő részére nyújtott biztonsági szolgáltatások, de a téma intenzív kutatás alatt áll, és még nem eléggé kristályosodott ki, hogy a biztonság mely területeit lesz képes meghódítani.

Köszönetnyilvánítás

A szerzők ezúton mondanak köszönetet a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások" projektnek a cikkhez végzet kutatások anyagi támogatásáért. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Irodalomjegyzék

Simmonds P., Rezek C., Reed A. Editors (2011) Seurity Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Josyula V., Orr M., Page G. (2012) Cloud Computing: Automating the Virtualized Data Centers, Cisco Press

Smoot S. R., Tan N. K. (2012) Private Cloud Computing; Consolidation, Virtualization, and Service-Oriented Infrastructure, Elsevier Inc.

Hurwitz J,. Bloor R., Kaufman M., Halper F. (2010) Cloud Computing For Dummies, Wiley Publishing, Inc.

Schulz G. (2012) Cloud and Virtual Storage Networking, CRC Press
Networking and Cloud (2011) An Era of Change, White Paper, Cisco Systems Inc., white_paper_c11-677946.pdf
Cisco (2011) Cisco Virtualized Multi-Tenant Data Center Framework, White Paper, Cisco Systems Inc., vmdcframework.pdf
Cisco (2012) Cisco Virtualized Multi-Tenant Data Center, Version 2.2 Design Guide, Cisco Systems Inc., vmdcDesign22.pdf
Nicira (2012) It's Time to Virtualize the Network. Network Virtualization for Cloud Data Centers., Whitepaper
Orlando, S. (2012) Quantum, Virtual Networks for Openstack, Quantum, 6th International Software Development Conference
Mell P., Grance T. (2011) The NIST Definition of Cloud Computing, NIST Special Publication 800-145, National Institute of Standards and Technology
OpenCrowd (2010) Cloud Taxonomy
http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png
Liu F., Tong J., Mao J., Bohn R., Messina J., Badger L., Leaf D. (2011) NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292, Recommendations of the National Institute of Standards and Technology
The Cloud Computing Standards handbook, ISBN 9781743041451
Matt Sarrel: Cloud Computing - Evaluating Security-as-a-Service, http://www.cioupdate.com/trends/article.php/3893521/Cloud-Computing---Evaluating-Security-as-a-Service.htm, 2012-04-21
Panda Security: Panda Cloud Protection, http://www.pandasecurity.com/enterprise/solutions/cloud-protection/, 2012-05-10
Online-crm: The Realities of CRM SaaS - Advantages and Disadvantages, http://www.online-crm.com/saas_advantages_disadvantages.htm, 2012-04-23
Kristóf Csaba: Iránymutatások a cloud computing védelméhez, http://computerworld.hu/iranymutatasok-a-cloud-computing-biztonsagosabba-tetelehez.html, 2012.05.10
Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final
Szenes, K.(2011): Supporting Applications Development and Operation Using IT Security and Audit Measures (Procds. of 5th IFIP TC2 Central and Eastern European Conference on Software EngineeringTechniques (CEE-SET'2011), Debrecen, Hungary, August 25-26, 2011), to appear in: e-Informatica Software Engineering Journal, http://www.e-informatyka.pl/wiki/e-Informatica
COBIT (2007): COBIT® 4.1 , Framework, Management Guidelines, Maturity Models, Copyright © IT Governance Institute® , 2007, editor: ISACA