Nemzeti
Közszolgálati Egyetem
Vezető-és Továbbképzési Intézet

DR. RACSKÓ PÉTER

A felhő alapú számítástechnika biztonsági kérdései a közigazgatásban

Budapest, 2014

A tananyag az ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel című projekt keretében készült el.

Szerző:
© Dr Racskó Péter 2014

Kiadja:
© NKE, 2014

Felelős kiadó:
Patyi András
rektor

TARTALOM

Kulcsszavak: számítási felhő, cloud computing, közigazgatási rendszerek, biztonság, adatvédelem, titkosítás, kilcsmenedzsment, adatátvitel, tárolás, informatikai infrastruktúra, szolgáltatási szint, költség-haszon elemzés, virtualizáció.

Összefoglaló:

A 21. század elejére végre megvalósult az informatika alkalmazóinak több évtizedes álma, arról, hogy egyes számítástechnikai szolgáltatásokat közműszerűen, a hálózatról vehessenek igénybe, a rendszerek használatához ne kelljen saját eszközöket vásárolni és üzemeltetni, és ne kelljen számos olyan számítástechnikai fogalmat, ismeretet és készséget elsajátítani egy egyszerű felhasználónak, szervezetnek, amelyre valójában semmi szüksége. A felhő alapú számítástechnika létrejöttével realizálható egyértelmű gazdasági előnyök számos, a versenyszférában működő szervezetet arra késztettek és késztetnek, hogy informatikai tevékenységeik egy részét vagy egészét "kihelyezzék a felhőbe". Ez a folyamat nem kerülte el a világ fejlett és fejlődő országainak közigazgatását sem. Több ország egyes közigazgatási informatikai rendszereit már a felhőben üzemelteti.

A tananyag célja:

A tananyagban leírjuk a felhő alapú számítástechika főbb jellemzőit, és kiemeljük az alkalmazással járó biztonsági és adatvédelmi kérdéseket, illetve ezek gyakorlati megoldásait. Külföldi példákon keresztül mutatjuk be, hogy egyes - a számítási felhő alkamazásában élenjáró - országok hogyan alakították át közigazgatási, közszolgálati információs rendszereiket és hogyan oldották meg, ill. hogyan kezelik a biztonsági és adatvédelmi kérdéseket. A biztonság jelenleg az informatika és távközlés egyik legfontosabb kérdése, a Stuxnet, a Mask[1] és más, hasonló, nagyon kifinomult és hatékony vírusok, valamint a Red October és a hasonló, összehangolt támadások korában mi legyen a helyes biztonsági stratégia, próbáljunk meg mindent saját kézben tartani, és magunk vegyük fel a harcot a támadókkal, vagy – éppen egy cloud alkalmazás kapcsán – ezt bízzuk a szolgáltatóra, akinek esetleg ehhez sokkal több erőforrás áll rendelkezésére. Ezt a döntést a szervezetnek magának kell meghoznia, mert a munkát ugyan kihelyezheti, de a felelősséget nem. Képletesen szólva, mely biztonsági paradigmát alkalmazzuk, ne tegyük az összes tojást egy kosárba, vagy tegyük az összes tojást egy kosárba, de arra nagyon vigyázzunk:

Oktatási célok:

- A hallgatók megismerik a felhő alapú számítástechnika működését, gazdasági és szervezeti előnyeivel.
- Megismerik az Európai Unió és a világ más országainak a számítási felhő közszférában történő alkalmazására vonatkozó álláspontját és törekvéseit.
- Megismerik a felhőspecifikus biztonsági kockázatokat és azok menedzselését
- Képesek lesznek megérteni a felhő alapú számítástechnikából eredő a közigazgatásban releváns biztonsági és adatvédelmi kérdéseket.

Bevezetés:

1961-ben egy informatikai konferencián merült fel először - akkor utópiaként [2]- hogy majd a számítástechnikai rendszereket közműszerűen lehet használni. Erre azonban még több, mint negyven évet kellett várni. Mi tette végül is lehetővé a közműszerű alkalmazást, illetve mi hiányzott ehhez évtizedeken keresztül?

Meglehetősen leegyszerüsítve azt mondhatjuk, hogy az informatika - és a távközlés- működését és alkalmazhatóságát három fő tényező határozza meg:

- feldolgozási (processzálási) kapacitás
- adattárolási (storage) kapacitás
- adatátviteli kapacitás (sávszélesség, bandwith).

1 Kaspersky: Unveiling "Careto" - The Masked APT February 2014.

2 Simson Garfinkel (3 October 2011). „The Cloud Imperative". Technology Review (MIT). Retrieved 31 May 2013.

Egy számítógép processzorának feldolgozási kapacitását az egy másodperc alatt elvégezhető műveletek számával, tároló kapacitását az egy tároló egységen, pl. mágneslemezen tárolható bájtok számával, vagy az egységnyi költségért tárolható bájtok számában, míg az adatátviteli kapacitást az egy másodperc alatt az egyik hálózati pontról a másik hálózati pontra átvihető bájtok számával mérjük.

Mindhárom mérőszám az elmúlt évtizedek alatt sokszorosára nőtt. A laptopunk részeként megvásárolt processzorok kapacitása akár csak 1970 óta több, mint tízmilliószorosára nőtt, jelenleg 1 GByte-nyi, azaz egymilliárd bájtnyi adatot néhány fillérért tárolhatunk, ez négy évtizede még sokmilló forintba került volna, ha egyáltalán erre lett volna lehetőség. Az interneten másodpercenként több tízmillió adatot tudunk az egyik számítógépről a másikra átvinni, erre korábban egyáltalán nem volt lehetőség.

1980-ban egy Gigabájt tárolásához szükséges lemezkapacitás ára félmillió dollár lett volna, ma ez 10 dollárcent. Amíg 1980-ban egy kereskedelmi forgalomban kapható processzor mintegy 700 ezer műveletet volt képes elvégezni másodpercenként, ma ez a szám meghaladja a 200 milliárdot. A 80-as évek elején az interneten elérhető sávszélesség fél kilobájt volt, ma ez a szám 100 megabájt nagyságrendű egy egyszerű felhasználó esetén is, azaz az előző érték 200 ezerszerese.

A fenti műszaki és gazdasági adatokból világosan látszik, hogy nincs elvi akadálya annak, hogy az informatikai feladataink elvégzéséhez a világ bármely, tőlünk távol eső pontján elhelyzett számítástechnikai kapacitást használjuk.

Ezt a lehetőséget ragadta meg számos, informatikai szolgáltatásra szakosodott vállalat és hozta létre saját felhő alapú számítástechnikai szolgáltatásait. Néhányuknál a motiváció az időszakosan fölös kapacitások értékesítése, másoknál saját termékeik népszerüsítése, míg megint másoknál egyszerűen az üzleti lehetőségek kihasználása volt.

A számítási felhő típusai

A számítási felhőben informatikai szolgáltatásokat vehetünk és veszünk igénybe. A szolgáltatások típusait az XaaS ("X as a Service") rövidítéssel szokás jelölni, ahol X sokféle szolgáltatástípust jelölhet. (IaaS - Infrastructure as a Service; PaaS – Platform as a Service, SaaS – Software as a Service, vagy IdaaS – Identity as a Service, BaaS- - Billing as a Service, stb.) A leggyakrabban használt osztályozás az IaaS, PaaS és SaaS csoportokat jelöli meg, a többi betűszó ezekbe az osztályokba sorolható be.

Itt nem célunk az egyes típusok részletes ismertetése, csak röviden mutatjuk be jellemzőiket.

Az IaaS lényege a számítási, tárolási és hálózati kapacitás szolgáltatás, ahol az erőforrásokat a szolgáltató saját eszközein biztosítja az interneten keresztül, a felhasználó pedig adott szerződéses feltételek alapján ezekért fizet. A díjakat túlnyomó részben az igénybevett kapacitások mennyisége alapján határozzák meg. Az infrastruktúra szolgáltatók szinte bármilyen processzálási és tárolási kapacitást tudnak nyújtani.

A szolgáltatásban használt hardver eszközök típusa a felhasználó számára érdektelen, a fizikai hardver az alkalmazott virtualizációs technika következtében a felhasználó számára nem látható, ő egy saját maga által kiválasztott operációs rendszerben (pl. Windows vagy Linux) saját maga által kiválasztott egyéb alapszoftverekkel (fordítók, adatbáziskezelők, rendszerintegrációs és egyéb szoftverek) dolgozik. A szolgáltatók az igénybe vehető infrastruktúrát többféle, a felhasználó igényeihez alkalmazkodó, jól skálázható csomagban kínálják. Sok más mellett IaaS szolgáltatást kinál például az Amazon, az Oracle, az IBM.

A PaaS szolgáltatás egy meghatározott gyártó termékcsaládjának alkalmazási platformként történő igénybevételét jelenti. Itt a felhasználó mind az infrastruktúráért, mind a platformért fizeti a díjat, általában a felhasználás arányában. PaaS-t kínál például a Microsoft Azure néven, amely a .net környezetet és az ehhez kapcsolható szoftver eszközök felhasználását biztosítja.

A SaaS kész alkalmazásokat nyújt a felhasználónak anélkül, hogy a hardver és szoftver infrastruktúrát feltárná. Ilyen például a Google levelezési és dokumentumkezelési szolgáltatása, vagy a Microsoft Office 365 alkalmazása.

Az 1. sz. táblázatban bemutatjuk, hogy a különböző szolgáltatások esetén a rendszer mely elemeit ill. tulajdonságait kontrollálja a felhasználó, és melyeket tartja kézben a szolgáltató.

Iaas	PaaS	SaaS
Alkalmazások	***Alkalmazások***	Alkalmazások
Programok	Programok	Programok
Biztonsági programok	Biztonsági programok	Biztonsági programok
Adatbázisok	Adatbázisok	Adatbázisok
Szerverek	Szerverek	Szerverek
Virtualizáció	Virtualizáció	Virtualizáció
Szerver hardver	Szerver hardver	Szerver hardver
Tároló	Tároló	Tároló
Hálózat	Hálózat	Hálózat

1. sz táblázat
A vastagon, dőlt betűvel szedett rendszerelemeket a felhasználó, míg a többit a szolgáltató működteti és felügyeli. Az összes többi rendszerelem feletti ellenőrzést a szolgáltató gyakorolja.

Nyilvános, magán és hibrid felhő

A felhő alapú szolgáltatásokat szokás megkülönböztetni a szolgáltató szervezet szerint is. Amennyiben a szolgáltatásokat egy erre szakosodott üzleti vállalkozástól vesszük igénybe, akkor nyilvános felhőről beszélünk, hiszen bárki használhatja a szolgáltatást. (ld. Google Docs, MS Azure, Amazon EC2, salesforce.com, stb.) Amennyiben a számítási felhőt egy szervezet, például kormányzat kizárólag saját használatra hoz létre, azaz alkalmazza mindazon technológiai eszközöket, elsősorban virtualizációs technológiát, amelyek a számítási felhőt jellemzik, de a használatot a saját dolgozóira vagy szervezeteire korlátozza, akkor magán felhőről beszélünk. Amennyiben egy szervezet egyes rendszereit a nyilvános felhőben, más rendszereit a falakon belül üzemelteti, akkor hibrid felhőről szokás beszélni, bár itt nem a rendszer, hanem a használati mód kevert. Biztonsági szempontból a magán felhő sem a szabályozás, sem az üzemeltetés szempontjából nem különbözik lényegesen más, nem felhő alapú rendszerektől, így ebben az anyagban a magán felhő és a hybrid használat biztonsági kérdéseivel nem foglalkozunk, a nyilvános felhőre koncentrálunk.

A számítási felhő gazdasági és szervezeti előnyei

Az alábbaikban összefoglaljuk, hogy mely tényezők szólnak a számítási felhő alkalmazása mellett a versenyszférában és a közszférában.

Előnyök:

1. A számítási felhő használatának díja általában a felhasználással arányos, nincsenek előre fizetendő költségek, vagy beruházási igény. Így nem jelentkeznek a beruházás finanszírozásának költségei sem.
2. Jobb hatékonyság – a felhőben használt hardver nincs telerakva mindazokkal a szoftverekkel, amelyekkel egy átlagos felhasználó a saját gépére, - egyéb célból – telepít. Így a programok futása ugyanazon a hardveren is gyorsabb lehet.
3. Olcsóbb szoftver – a felhőben számos szoftver ingyenes, a legtöbb általánosan használt, licenszdíjas szoftver helyett használhatjuk ingyenes megfelelőjét.
4. Gyakorlatilag korlátlanul, igény szerint növelhető kapacitások - skálázhatóság - mind a tár, mind a feldolgozás terén.
5. Megbízható adattárolás. A szolgáltatók gondoskodnak az adatok megőrzéséről és visszaállításáról meghibásodás esetén.
6. A számítási felhő általában a korszerű technikát képviseli, az eszközök megújítása, karbantartása a szolgáltató feladata, így a felhasználónak nem kell mérlegelnie, hogy hogyan tartson lépést a fejlődéssel. Ugyanez vonatkozik a szoftver aktualizálásra is.

7. Helyfüggetlen hozzáférés – a felhőben lévő adataink és alkalmazásaink nincsenek egy adott géphez kötve, azokat bárhonnan elérhetjük, nem kell fájljainkat magunkkal vinni, ha megyünk valahova. A felhőben való tárolás megkönnyíti a verziókövetést is, nem kell a különböző eszközeinket szinkronban tartani.
8. A számítási felhő a legjobb csoportmunka támogató eszköz. Dokumentumainkat könnyen megoszthatjuk, egyszerű az együttműködés és a projektmunka.
9. Eszközfüggetlenség – nem kell azzal törődnünk, hogy hardver és szoftver eszközeink képesek-e együttműködni, a felhőben tárolt adatainkat a legtöbb mobil és fix eszközről gond nélkül használhatjuk.
10. A "belépési küszöb" alacsony. A felhasználónak viszonylag alacsony informatikai szaktudással is lehetősége van olyan bonyolult alkalmazások használatára, amelyeket saját eszközeivel - részben a szaktudás, részben a finanszírozás hiánya miatt - képtelen lenne felépíteni. (gondoljunk például egy többszázezres ügyfélkört kezelő alkalmazásra). Ez a szempont a KKV-k és kisebb szervezetek esetén különösen fontos. .

Hátrányok:

1. Internet kapcsolat nélkül nem működik. Ahol az Internet kapcsolat nem biztonságos, vagy lassú, ott a felhő alapú számítástechnika nem alkalmazható.
2. Minthogy az adatforgalom nagy, különösen a webes alkalmazásoknál, a válaszidők nagyobbak lehetnek, mint a saját eszközökön.
3. A funkcióknál és szolgáltatásoknál egy előre megadott menüből választhatunk, ami sokszor szegényesebb, mint a helyi alkalmazások. (Pl. a Google Docs nem tartalmaz annyi lehetőséget, mint az MS Office)
4. A biztonság és adatvédelem feladata és kockázata alapvetően a felhasználónál marad, a védelmi lehetőségek nagy része ugyanakkor a szolgáltató kezében összpontosul. Például. az adatvesztés következményei igen jelentősek lehetnek. Egy kompromittált szerver mind a felhasználót, mind a szolgáltatót veszélyezteti. A kockázatok csökkentése érdekében az USA-ban például adatvesztés esetén a szolgáltatónak kötelező a felhasználók azonnali tájékoztatására. Ekkor a felhasználók, különösen, ha személyes adataik tűntek el, azonnal meg kell, hogy kezdjék a kárelhárítást. A szolgáltató pedig jogi eljárásoknak néz elébe. Ezek az eljárások 2011-ben 1 milliárd USD-be kerültek az USA felhő szolgáltatóinak[3].
5. Nehéz a szolgáltató váltás. Minthogy jelenleg nem léteznek a szolgáltatók által alkalmazott "felhő alapú szabványok", minden szolgáltató a saját adattárolási, adatkezelési, esetleg titkosítási eljárásait használja, mert számukra ez a hatékony megoldás. Az adatátvitelre többen[4] használják a rugalmas, XML alapon működő, HTTP-n futó REST (Representational State Transfer) eljárást, de ez nem kötelező és nem általános. Adataink teljeskörű visszaszerzése egy esetleges szolgáltató váltásnál költséges, és nem kockázatmentes feladat. Azt, hogy egy szolgáltató elhagyása nem egyszerű feladat, mutatja például a Nirvanix felhő alapú tárolási szolgáltatást nyújtó cég példája, amely 2013. szeptemberében bejelentette, hogy felhagy a szolgáltatással és felszólította ügyfeleit, hogy két-három héten belül vigyék el adataikat. Ha meggondoljuk, hogy 10TB adat letöltéséhez egy 10Mbit/sec sávszélességű hálózaton hónapokra lenne szükség, és még nem is vettük figyelembe az esetleges dekódolás időigényét. Ahhoz, hogy egy felhasználó a különlegesen soknak nem nevezhető 10TB adatmennyiséget két-három hét alatt letöltse, legalábbis gigabites sávszélességgel kellene rendelkeznie a szolgáltató és saját telephelye között. (Még csak nem is említettük az azonnal kiépítendő saját tárkapacitást, amit éppen a felhő szolgáltató igénybevételével szerettek volna elkerülni.) Nyilván ennyi idő kevés egy másik szolgáltató megbízására. A történet valószínű folytatása az, hogy a szolgáltatónál tárol adatok gazdái kénytelenek felvásárolni a céget, ami természetesen koránt sem jó üzlet.
6. A virtuális környezetben más felhasználók ugyanazt a hardvert használják, mint mi. Ez – a virtualizációs szoftver esetleges gyengesége esetén – hozzáférést engedhet a mi rendszereinkhez. Az sem kizárt, hogy a mi általunk is használt hardveren valaki törvényellenes tevékenységet folytat, és a bűnüldöző szervek lefoglalják a hardvert.
7. Nincs fizikai és vezetői ellenőrzésünk a rendszerek felett.
8. A számítási felhő a személyes adatok védelme szempontjából különösen érdekes, ui. az EU adtvédelmi szabályozása lényegesen különbözik számos más ország, akár az USA adatvédelmi előírásaitól, attól mind szemléletben, mind a felelősség kérdésében eltér. Ugyanakkor az EU jogi szabályozása - jelentősen leegyszerüsítve - azt írja elő, hogy az állampolgárok személyes adatai csak olyan környezetbe vihetők át, ahol az EU-nak

3 Bowen, Janine Anthony. (2011). Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations. Computer and Internet Lawyer Trade Journal. 28 (8),

4 pl. Amazon S3

megfelelő adatvédelmi szabályozás érvényes. Ugyanankkor a felhasználó többnyire azt sem tudja, hogy a szolgáltató szerverei mely országban működnek.

Biztonság és megfelelőség a felhőben

A számítási felhő közigazgatási alkalmazásának biztonsági kérdéseit az alábbi két fő megközelítésben lehet vizsgálni:

- A biztonság, mint a kockázatmenedzsment tárgya
- A biztonság, mint a megfelelőség vizsgálatának tárgya

A két nézőpont közötti eltérés a prioritásokban rejlik. A biztonságtechnikai szakemberek a kockázatmenedzsmenter koncentrálnak (az üzleti, folyamati és technológiai jellegű kockázatokat elfogadható szinten szeretnék tartani) míg a megfelelőségi szakemberek azt szeretné elérni, hogy a kockázatmenedzsment eszközrendszere megfeleljen az adott szabályoknak - a közigazgatás esetén ez elsősorban jogszabályokat jelent. A vonatkozó jogszabályok természetüknél fogva nem operacionálisak, azaz nem a hogyan kérdésre adnak választ, hanem a célt jelölik meg, míg a kockázatmenedzsment inkább az egyes kockázatok menedzselésére kialakított akciókat tartalmazza.

Az ENISA (Európai Hálózat- és Információbiztonsági Ügynökség), melyet az Európai Unió 2004-ben hozott létre abból a célból, hogy segítséget nyújtson a Biztottságnak az informatikai biztonsággal kapcsolatos jogaszabály előkészítő munkájában, 2009-ben részletes kockázatelemzést készített a számítási felhő alkalmazásáról. A tanulmány megállapításainak legnagyobb része a mai napig is érvényes, amint azt a későbbiekben majd be is mutatjuk.

A számítási felhő általános kockázatai

Az anyagban nem foglalkozunk az információs rendszerek általános adatbiztonsági kérdéseivel, mint pl. a vírusok, trójaiak, DDoS támadások, az emberi hanyagság szerepe, a “social engineering”, stb, kizárólag a felhő alapú számítástechnika speciális biztonsági és adatvédelmi kérdéseit tárgyaljuk.

Az 1. sz. táblázat jól szemlélteti, hogy melyek azok a területek, ahol saját magunknak kell gondoskodnunk a biztonságról, ugyanúgy, mintha az eszközök a mi irányításunk alatt lennének, és melyek azok, amelyek a szolgáltató hatáskörébe esnek. Könnyen belátható, hogy míg az IaaS esetén a biztonságot többé-kevésbé kézben tudjuk tartani, PaaS és SaaS alkalmazásakor a biztonsággal kapcsolatos majd minden feladat a szolgáltatóra hárul. Egy üzleti vállalkozásnál mindhárom esetben a kockázatok jellemzői (esemény bekövetkezésének valószínűsége és gazdasági hatása) szakértői becslésekkel jól jellemezhetők, a közigazgatási körben ez sokal nehezebb feladat, ugyanis például egy esetleges működésképtelenség, adatvesztés vagy adatlopás jelentős politikai, így nehezen kvantifikálható és kezelhető kockázatokat jelent. A későbbiekben meglátjuk, hogy egyes országok hogyan csökkentik ezt a kockázatot, amikor közigazgatási informatikai feladataikat a felhőbe helyezik.

A felhőben történő tárolás kockázatai és a kockázatok ill. felelősség kérdése

Az alábbiakban felsoroljuk a már említett ENISA tanulmányának alapján a felsőspecifikus kockázatokat[5].
Az ENISA tanulmány az alábbi, felhő specifikus kockázatokat elemzi:

- A rendszereket nem a felhasználó irányítja,
- A szolgáltatóváltás nehéz és költséges,
- A virtuális technológia gyengesége a felhasználók elkülönítését veszélyeztetheti,
- Megfelelőségi kockázat - az audit dokumentumok és naplók, ill. egyéb megfelelőségi dokumentumok hozzáférhetősége bizonytalan
- A felhasználói interfészek kikerülnek az internetre, így nehezebben védhetők, mint egy zárt rendszerben,
- Az adatok törlése nem mindíg biztonságos, vagy teljes, ui. a tényleges adatmegsemmisítés igen költséges művelet,
- Egy rosszindulatú rendszergazda a felhő esetében különösen nagy károkat tud okozni.

5 Cloud Computing - Benefits, risks and recommendations for information security, Nov 2009 ed. Daniele Catteddu and Giles Hogben

Az egyes kockázatokkal - különös tekintettel a közigazgatási alkalmazásokra - a tananyagban részletesen foglalkozunk. Ugyanakkor nem győzzük eléggé hangsúlyozni az ENISA végső megállapítását, mely szerint a kockázatokat részben ki tudjuk helyezni egy szolgáltatóhoz, de a felelősséget nem.

Adatok titkosítása és a titkosított adatok tárolása a felhőben

A biztonságos adattárolás legegyszerűbben az adatok titkosításával valósítható meg a számítási felhőben. A titkos adattárolás alkalmazására többféle megoldás is lehetséges. Az egyik az, hogy a szervezet a felhőben tárolandó adatokat saját eszközein kódolja, és a felhőbe történő adatátvitel, a tárolás és a visszatöltés is ebben a kódolt formában történik meg. Nyilvánvaló, hogy, amennyiben a felhőben nem csak tárolás, hanem feldolgozás is történik, ez a folyamat így nem működik, erre az esetre később visszatérünk.

Sok felhő szolgáltató titkosítási szolgáltatást is kínál, ez esetben a felhasználó adatainak tikosításáról és ebben a formában történő megőrzéséről ő gondoskodik, ilyenkor az adatátvitel titkosítása még megoldandó kérdés. Mindkét esetben alapkövetelmény, hogy az adatok a forrástól a visszaérkezésig végig titkosítottak legyenek.

Akár a felhasználó, akár a szolgáltató végzi a titkosítást, a titkosító kulcsok kezelése (encryption key management) központi szerepet játszik a folyamatban. A kulcs elvesztésével ui. kódolt adatainknak is örökre búcsút mondhatunk, a kulcs kompromittálódása viszont adataink illetéktelen kezekbe kerülésével járhat.

A megfelelő kulcsmenedzsment lényege a kulcsok biztonságos tárolása, és elérhetőségének biztosítása a - jogosultsággal rendelkező - személyek, folyamatok, rendszerek számára.

Ha adataink tárolását egy felhő szolgáltatóra bízzuk, alaposan meg kell ismernünk az általa alkalmazott titkosítási folyamatokat, kulcsmenedzsment szabályzatot és, hogy milyen audit és egyéb eszközökkel biztosítja saját munkatársai körében a szabályzatok betartását. A szabályzatnak, az alkalmazott titkosító algoritmusoknak, tárolási módoknak és kulcsmenedzsmentnek összhangban kell lennie az általunk elvárt biztonsággal. A kódolási algoritmusok terén jó támpontot nyújtanak a NIST kiadványai. A NIST jelenleg az alábbi három titkosító algoritmust tartja elfogadhatónak:

- AES,
- Triple DES
- Skipjack

(ld. http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html)

Ugyanakkor meg kell jegyezni, hogy 2014. februárjában maga a NIST kezdeményezte a titkosítási algoritmusok fejlesztési folyamatainak teljes átvizsgálását, ui. a Snowden ügy kapcsán felmerült a gyanú, hogy az NSA egy, a titkosításnál használt és a NIST által jóváhagyott, Dual_EC_DRBG nevű véletlen bitgenerátorba hátsó ajtót helyezett el, lényegesen gyengítve ezzel minden olyan titkosító algortimust, amely a bitgenerátort használja. [6]

Mindezek ellenére feltételezhetjük, hogy a fenti szabványos kriptográfiai eljárások - különösen most, miután a NIST ezek teljes átvizsgálását végzi - a szokásos közigazgatási eljárásokban kellően biztonságosak.

A kulcsmenedzsment “kulcs”-kérdései

A kriptográfiai kulcsok menedzselése a megfelelő erősségű titkosító kulcsok létrehozását, tárolását, cseréjét, a jogosultsággal rendelkezők számára történő elosztását, védelmét, szükség esetén megsemmisítését és a folyamatok auditálhatóságának biztosítását jelenti. Minden kriptográfiai eljárás biztonságának alapja a kulcsmenedzsment megfelelősége.

Néhány általánosan elvet minden kulcsmenedzsment rendszerben kötelezően be kell tartani: [7]

- a kulcsokat a kriptográfiai egységeken kívül titkosítva kell tárolni. Minthogy a titkosító algoritmusok többnyire nyilvánosak, a kulcs titkossága biztosítja a védelmet az adatokhoz való illetéktelen hozzáféréssel szemben

6 http://www.fiercegovernmentit.com/story/nist-proposes-encryption-standard-development-process-internal-guidance/2014-02-20#ixzz2u2Bg9cRB (letöltve: 2014 február 21

7 Shon Harris: CISSP Exam Guide, 2010, McGraw Hill

- a kulcsok kezelése automatikusan, a felhasználó elől rejtve, az alkalmazói rendszerben vagy az operációs rendszerben kell, hogy történjék. A manuális kulcskezelés (régebben ez volt az általános) kockázat forrása lehet, az ember hibázhat vagy szándékosan is visszaélhet a kulccsal
- a kulcsok elveszhetnek vagy megsemmisülhetnek, ezért szükséges másolati példányok tárolása is, természetesen megfelelően biztonságos módon.
- a kulcs használatát sokszor egy természetes személynek kell kezdeményeznie, például egy alkalmazás elindításával, amely például adatokat visz át a felhő alapú tárba. Amennyiben az a személy nem elérhető (pl. beteg) vagy elveszíti a hozzáférési tokent, akkor meg kell oldani a helyettesítését. Rendkívül fontos, hogy a helyettesítést előre szabályozott módon hajtsák végre, és a folyamatot több, mint egy főből álló csoport felügyelje és jegyzőkönyvezze. Elfogadott szabály, hogy a csoportban valaki képviseli a szervezet vezetését, és a csoport nem minden tagja informatikus.

Fentiek figyelembevételével, az államigazgatási adatok tárolásánál - különös tekintettel személyes adatok védelmére - a kulcsmenedzsment átadása egy külső szolgáltató partner számára nem kezelhető kockázatot jelent.

Megjegyezzük, hogy a versenyszférában sem szeretik a szervezetek a kulcsmenedzsmentet a szolgáltatóra bízni, hiszen számos olyan eset ismert, amikor egyes kormányok arra kényszerítették a szolgáltatót, hogy a felhasználókról adatokat szolgáltasson.

Az adatátvitel titkosítása a felhőben

Az átvitt adatok titkosítására - aszerint, hogy a titkosítás melyik OSI rétegben történik - két koncepciót szokás megkülönböztetni, a kapcsolati szintű (link encryption, online encryption) és a végponttól végpontig (end-to-end) történő titkosítást.

A kapcsolati szintű titkosítás az OSI fizikai és adatkapcsolati szintjén történik, ekkor az adatcsomagok szinte teljes egészben tikosítottak, kizárólag az adatkapcsolat szinkronizációjához szükséges adatok haladnak a routerek között kódolatlan állapotban. Így az adatcsomagok fej és lábrészei, a címek és útvonalválasztáshoz szükséges információk is kódoltak. Ez gyakorlatilag kizárja a hálózaton áthaladó adatcsomagok megfigyelését (packet sniffing), viszont a módszer hátránya, hogy minden routeren vissza kell fejteni a továbbításhoz szükséges adatokat és a továbbküldés előtt újra kell azokat kódolni. A kapcsolati szintű kódolást a hálózati szolgáltatónak kell biztosítania, ez nem a felhasználó, és nem a felhő szolgáltató dolga.

A végponttól végpontig történő titkosítás során az adatcsomagnak kizárólag a felhasználó számára hasznos része kerül titkosításra, az adatcsomag fej és lábrésze, a címek, útvonal információk nem. A packet sniffing támadások a nem kódolt adatokhoz hozzáférhetnek, de a hasznos tartalomhoz nem. A végponttól végpontig történő titkosítást vagy a felhasználó végzi (amikor az adatokat a felhő szolgáltató tárolójába feltölti) és/vagy a felhő szolgáltató (amikor az adatokat letölti a felhasználó számára,) vagy a felhasználó által tikosított adatokat a felhő szolgáltató tikosítva tárolja és így is küldi vissza.

A felhőben történő tárolásnál alighanem a legcélszerűbb a végponttól-végpontig történő titkosítás alkalmazása, amit különösen érzékeny adatok esetén kapcsolati szintű titkosítással is ki lehet egészíteni. Ez esetben a kulcsmenedzsment a felhasználónál marad, a felhő alapú szolgáltató, vagy az őt támadó hacker viszont semmilyen módon nem fér hozzá az adatainkhoz. Az adatátviteli titkosításról viszont a hálózat szolgáltatója gondoskodik.

A tikosítás erőforrásigénye vs. könnyítések

A szabványos kriptográfiai aljárások alkalmazása processzorigényes feladat. Számos felhő szolgáltató kevésbé költséges megoldásokat javasol, pl. azt, hogy csak egyes adatokat (pl. jelszavakat) tároljanak tikosított formában. Egy ilyen javaslatnál mérlegelni kell a kockázatokat, de például személyes adatok tárolása esetén a harmadik félnél (felhő szolgáltatónál) történő kódolatlan tárolás nem kezelhető kockázatokat eredményez.

Másik alternatív megoldás a szolgáltató saját - nem szabványos, de kevesebb erőforrást igénylő - kriptográfiai eljárásainak alkalmazása. Kis jóindulattal feltételezhetjük, hogy a szolgáltató szakértői megfelelően biztonságos eljárásokat alkalmaznak, így adatainkat egy harmadik féltől meg tudják óvni. Ugyanakkor a megbízó kiszolgáltatott helyzetbe kerül, hiszen ilyenkor sem a kulcsmenedzsment nincs a kezében, de még sokszor a titkosítási algoritmus sem ismert.

A közigazgatásban célszerű az ilyen helyzeteket elkerülni, mert túl nagy kockázatot jelentenek. Képzeljük el, hogy a szolgáltató bezárja vállakozását, szakemberei kilépnek, nem lesz, aki vissza tudja szerezni adatainkat. A titkosítás

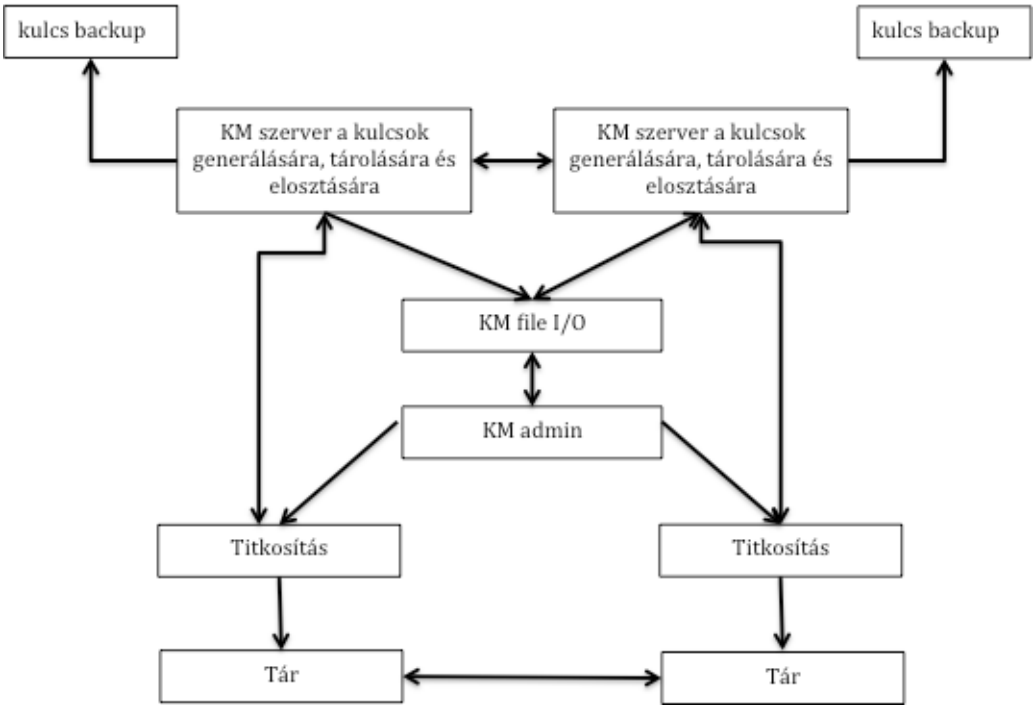
a számítási felhő alkalmazása esetén elsősorban a kulcsmenedzsment kérdésében speciális (ki és hogyan generálja és tárolja a kulcsokat) így itt erre térünk ki részletesebben.

A kulcsmenedzsment szabványosítása

Az elmúlt évek vállalkozásokra vonatkozó megfelelőségi szabályozásai (SOX, IEEE, HIPPA, stb.) valamint az adatlopások számának növekedésének hatására kulcsmenedzsment szabványosítási hullám indult el a világban.

Egyrészt az IEEE fogott bele egy P1619-3 jelű, adattároláshoz szükséges kulcsmenedzsment rendszer architektúra szabvány kidolgozásába8, másrészt több nagy cég (Cisco, IBM, HP, Thales, EMC, stb.) dolgozott ki egy termékfüggetlen kulcsmenedzsment szabvány javaslatot (Key Management Interoperability Protocol (KMIP)) és nyújtották be az Organization for the Advancement of Structured Information Standards (OASIS) konzorciumhoz, melynek feladata a termékfüggetlen szabványok, ajánlások elterjesztése. Az OASIS 2011-ben megjelentette a Symmetric Key Services Markup Language (SKSML) Version 1.0 specifikációt, amely egy XML alapú kulcsmenedzsment szolgáltató rendszer használatához szükséges protokol leírása.

Az IEEE kulcsmenedzsment architektúra ábrája:



A szabvány nem fedi le a teljes architektúrát, csak a KM szervereket, a KM file input/output műveleteket, a kriptográfiai modult, valamint a KM szerver és a kriptográfiai modulok közötti kapcsolatot. A többi modul és adatkapcsolat opcionális lehetőség.

A felhőben történő adattárolás esetén tehát az IEEE kulcsmenedzsment architektúra szabvány alkalmazása és az SKSML használata előírható a szolgáltatónak. Minden egyéb egyedi megoldás növeli a kockázatot.

Adatfeldolgozás a felhőben

A felhőben történő adatfeldolgozás biztonsági szempontból lényegesen különbözik az adattárolástól, akár SaaS, akár PaaS jellegű szolgáltatásról beszélünk.

Nemrégen az ENISA megvizsgálta és átdolgozta az 1999/93/EC számú, az elektronikus aláírásról szóló EU Direktívát, és új elektronikus azonosítási és bizalmi szolgáltatási elveket dolgozott ki az elektronikus tranzakciók belső

8 IEEE P1619.3/D6, February 2009

piacon történő alkalmazására. Megvizsgálta az alkalmazott biztosnági eljárásokat és interoperabilitási kérdéseket. Megjelentette a "TSP Services, standards and risk analysis report" c. tanulmányt, amely az e-government szolgáltatók számára fogalmaz meg olyan javaslatokat, hogy a szolgáltatásokat használó állampolgárok bizalmának erősítése érdekében a bizalmi szolgáltatások bevezetésénél és használatánál vegyék igyénybe olyan megbízható harmadik fél szolgáltatásait, amelyek erősítik az állampolgároknak a szolgáltatások megbízhatóságába vetett bizalmát. A tanulmány néhány nagyobb EU-s projekt (epSOS, e-CODEX and PEPPOL) tapasztalataira épül.

Kockázatkezelési elvek a felhőben

Az informatikai feladatok felhőbe költöztetése esetén pontosan kell ismerni a kockázatokat, ki kell alakítani azt a kockázatmenedzsment rendszert, amellyel a biztonsági kockázatok kézben tarthatók.

A számítási felhő alkalmazásánál a közigazgatásban nem elfogadható a "80/20" szabály, azaz a nyilvánvaló kockázatokat (80%) menedzseljük, a maradékot meg akkor, ha a biztonsági esemény bekövetkezik. Itt zéró eseményre kell törekedni, mert semmilyen adatvesztés nem megengedett. Képletesen szólva, a technológia kihelyezhető, de a kockázat nem.

A számítási felhő biztonságának menedzselésében természetesen célszerű alkalmazni a meglévő kockázatmenedzsment rendszereket, a COBIT az ITIL és az ISO 27000-es szabványok biztonsági útmutatóit. A COBIT elsősorban a kihelyezés üzleti folyamataiban rejlő és a szervezeti/szervezési kockázatok menedzselésére alkalmas, az ITIL a szolgáltatási szempontokat, rendelkezésre állást, mérést, minőségbiztosítást helyezi a középpontba. Az ISO 27000-es szabványcsalád rendszerszemléletben együtt kezeli a biztonságot, a rendszerek és adatok integritását és a szolgáltatások rendelkezésre állását, priorizálja a biztonsági kockázatokat és gyakorlati útmutatást is ad az adatok menedzselésére. A közigazgatásban természetes elvárás, hogy a választott számítási felhő teljes mértékben megfeleljen az ISO 27000-es szabványoknak.

Az internetes "szakirodalomban" számos helyen fogalmaznak meg igen hasznos ellenőrző kérdéseket arra vonatkozóan, hogy a kiszemelt számítási felhő szolgáltatás mennyiben felel meg kockázatmenedzsment elvárásainknak. [9]

Az alábbiakban felsoroljuk a legfontosabb, a biztonságra és adatvédelemre vonatkozó ellenőrző kérdéseket, amelyeket a szolgáltatónak meg kell válaszolnia, mielőtt rendszereinket áthelyezzük a kezébe.
Az ENISA 2013-as jelentése szerint[10] a megbízható közszolgáltatásoknál mindíg meg kell győződni:

- az autentikációs eljárás erősségéről
- a végponttól végpontig történő titkosításról
- az elektronikus bizonyítékok naplózásáról az audit naplóban

Felsoroljuk az ezekből következő, általános, a biztonságra vonatkozó ráészletes ellenőrző kérdéseket:

- Milyen rendszerben irányítja a felhő szolgáltatást nyújtó szervezet az informatikai infrastruktúrát?
- Milyen rendszerarchitektúrát alkalmaznak?
- Hol tárolják - fizikailag és logikailag - az adatokat?
- Kinek lesz hozzáférése az adatokhoz?
- Hogyan, mikor és hol titkosítják az adatokat tároláskor és a kommunikáció során?
- Megengedett-e nyílt szövegű protokollok használata a hálózatban és léteznek-e ilyenek a gyakorlatban?
- Hogyan kezelik a biztonsági eseményeket?
- Milyen hibatűrő technológiát és folyamatokat alkalmaz a szolgáltató?
- Mi a szolgáltató üzleti modellje? (egyéni ügyfél/társaság; KKV/nagyvállalat)?
- Milyen alkalmazásokat helyezünk ki? Milyen adatokat kezelnek a kihelyezett rendszerek?
- Mely belső műszaki szabványokat kell alkalmaznia a szolgáltatónak?
- Mely szabályozói követelményeknek kell eleget tennie a szolgáltatónak?
- Hogyan menedzselik a kriptográfiai kulcsokat? Ki fér hozzá a kulcsokhoz?
- Van-e szerver és munkaállomás szintű védelem a vírusok és más rosszindulatú szoftverek ellen?
- Hajtottak-e végre teszt támadásokat a belső és külső hálózatban? Milyen eredménnyel?

9 (pl. http://www.informationweek.com/security/risk-management/security-questions-to-ask-your-cloud-provider/d/d-id/1092040? letöltve2014. február 10-én, http://searchcompliance.techtarget.com/ehandbook/Risk-management-for-cloud-computing, letöltve 2014. február 11-én, ENISA: Cloud Computing: Benefits, risks and recommendations for information security Nov. 2009)

10 (Trusted e-ID Infrastructures and services in EU - Recommendations for Trusted Provision of e-Government services Report, December 2013)

- Mi a szolgáltató jelszó szabályzata? Létezik-e elfogadott és bevezetett felhasználói hozzáférési szabályzat és dokumentáció?
- Milyen tűzfalakat, IPS/IDS (behatolás figyelő és megelőző szoftvereket) és Web szűrő rendszereket használnak?
- Van-e működő adatszivárgás-megelőző kontroll a hálózatban, elektronius levelezésben és a végfelhasználói rétegben?
- Vannak-e dokumentált, elfogadott, a szoftverfejlesztésben, alkalmazás implementációban, adatbáziskezelésben, rendszer és hálózati infrastruktúrák esetén, valamint az információfeldolgozásban használt biztonsági követelmények?
- A használt vezeték nélküli hálózatok WPAv2-t használnak-e és el vannak-e különítve a belső hálózatoktól?
- A hálózati és infrastrukturális eszközök külső adminisztrációjánál kétfaktoros autentikációt alkalmaznak-e?

Ehhez hasonlóan j**ól** használható ellenőrző listát hozott létre a Cloud Security Alliance (CSA) nevű non-profit szervezet is. [11] Felállítottak egy "felhő-ellenőrzési mátrixot", és leírták ennek leképezését más, szabványos ellenőrzési eljárásokra (ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP, stb).

A felhő szolgáltató átvilágítása

Fenti ellenőrző kérdéseinkre a szolgáltató átvilágítása (due diligence) során kaphatunk választ. Az átvilágítás alatt egyrészt kielégítő válaszokat kell kapni a fenti tartalmi kérdésekre, ugyanakkor szükséges néhány formális dokumentum meglétéről és minőségéről is megbizonyosodni, mint például:

- Harmadik féltől származó értékelések, beleértve a szervezet és a munkatársak releváns bizonyítványait (SSAE 16, PCI, CISA, CISSP, stb.)
- A szolgáltató információbiztonsági és üzletmenetfolytonossági dokumentumai
- Pénzügyi és biztosítási adatok
- Referenciák, független vizsgálatok jegyzőkönyvei
- Szolgáltatás története (szolgáltatási hibák, a szolgáltatás szünetelése, törvényi vagy szabályozói elmarasztalások, stb.)

Néhány külföldi példa

A felhő alapú számítástechnika számos - a biztonsággal és adatvédelemmel összefüggő és nem teljesen megoldott problémája elllenére számos ország közigazgatásában a nyilvánvaló gazdasági és társadalmi mozgatórugók hatására egyre jelentősebb szerepet kap. Az EU Digitális Menetrendjének is stratégiai eleme a felhő alapú szolgáltatások kialakítása és elterjesztése Európában. Az alábbiakban néhány érdekes külföldi példát mutatunk be semmiképpen nem törekedve átfogó elemzésre.

Egyesült Királyság

2014, február 25-én nyitotta meg az Egyesült Királyság kormánya a G-Cloud 5 rendszert, amely az ország közigazgatása számára kialakított elektronikus keretrendszer ötödik verziója. A keretrendszert a Kormány üzemelteti, az egyes közigazgatási alkalmazásokat viszont a versenyszféra szereplői szállítják, miután előzetes kormányzati minősítésen estek át.

Tipikus szolgáltatások a web hosztolás, dokumentum menedzsment, kollaboratív eszközök, elemző programok, de minden féle IaaS, PaaS és SaaS szolgáltatások, konfigurációmenedzsment és monitoring is elérhetők. A felkínált programok száma 1700. Az alkalmazás szállítók programjaikat a kormányzati CloudStoreba töltik fel, ahonnan az alkalmazó szervezetek megvásárolják a használati jogot. A CloudStore tartalmát időről időre felülvizsgálják, és az irreleváns és nem használt programokat kiselejtezik. A G-Cloud 2011-ben indult, és az Egyesült Királyság Kormányának informatikai stratégiája szerint 2015-ig az összes új IT beszerzés 50%-a felhőbe fog irányulni. A 2014 eleji adatok szerint azonban az előminősített szállítók 80%-ától még egyáltalán nem vásároltak semmit, és a helyi önkormányzatoknak mintegy 10%-a van csak tisztában a G-Cloud funkciójával.

11 https://cloudsecurityalliance.org/research/ccm/

USA

*Az USA Kormányának szolgáltató hivatala (*General Services Administration) 2012-ben bejelentette a "Szövetségi Kockázat és Autorizáció Menedzsment Program" elindítását, amely felhatalmaz egyes felhő szolgáltatókat, hogy meghatározott felhő alapú szolgáltatásokat nyújtsanak a szövetségi hivataloknak és kormányzati szerveknek. A GSE szervezet ezeket a szolgáltatásokat biztonsági szempontból állandó megfigyelés alatt tartja.

Megemlíthetjük, hogy egyes nagy cégek, saját kezdeményezésben létrehoztak saját, a közigazgatásnak felkínált felhő alapú szolgáltatást. Az IBM például létrehozta saját Szövetségi Felhőjét (Federal Community Cloud) amely IaaS és SaaS szolgáltatásokat, analitikai eszközöket, webhosztingot, stb. nyújt. Ehhez meg kellett szerezniük az un. Fed Ramp (Federal Risk and Authorization Management Program) megfelelőségi tanúsítványokat. A tanúsítványoknak az USA-ban 2002-ben elfogadott Federal Information Security Management Act megfelelőséget kell bizonyítaniuk. A szolgáltatások megvásárlása közbeszerzés útján történik.

A cég hasonló központokat nyitott Írországban, Németországban, Braziliában, Japánban, Délafrikában, Kínában, és más országokban.

Egyéb országok

Jelentős felhő alapú e-government fejlesztések folynak a világ számos más országában is, például Szingapúrban, Ausztráliában, ezekben az országokban külön G-Cloud fejlesztési stratégiát fogadtak el és jelentős összegekkel, milliárd dollárokkal támogatják a szolgáltatás elterjedését.[12]

12 ICT Strategy 2012-20154. Australian Government Cloud Computing Policy Maximising the Value of Cloud July 2013. v 2.1.