

előadás az Óbudai Egyetemen

A Hírközlési és Informatikai Tudományos Egyesület Számítástechnikai Szakosztálya,
a European Organisation for Quality MNB Informatikai Szakbizottsága,
az (ISC)² Hungary Chapter, és
az ISACA Magyar Fejezete közös rendezvénye

Óbudai Egyetem, Neumann Informatikai Kar
III. ker., Óbuda, Bécsi út 96/b.

2016. február 22. hétfő

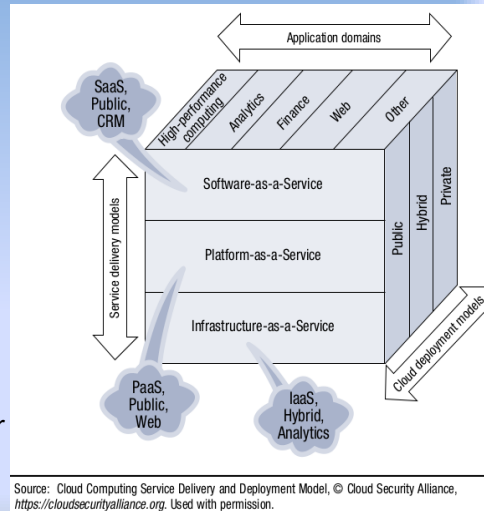
Miről lesz szó?

- Felhőszolgáltatások alapvető specifikumai
- Szabályozási környezet nagy vonalakban
- A felelősség kérdése, auditálhatóság
- Tipikus problémák
- Technikai aspektusok
- Mire figyeljünk a szerződésben?
- Hol szeretjük, hol nem – a felhőt
- *Néhány „kis színes”*
- Egy majdnem elképzelt eset, majdnem happy end-del

Cloud szolgáltatások specifikumai

- Egy definíció
- “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

/National Institute of Standards and Technology (NIST) 2011./



Cloud szolgáltatások néhány lényeges specifikuma

- Az adatok konkrét helye nem feltétlenül ismert
- Konfekció jellegű „SaaS” megoldás
- Interneten érhető el
- Magas rendelkezésre állás, skálázhatóság – dinamikus IP range
- A rendszer felügyelete végül másé

Szabályozási környezet

- EU 95/46/EK adatvédelmi irányelv
- 2011. CXII. Törvény (Infotv.)
- A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye az Európai Unió Bíróságának a Safe Harbor ügyben hozott ítéletéről (C-362/14.)
- 2013. évi CCXXXVII. Törvény a hitelintézetekről és a pénzügyi vállalkozásokról
- A Kormány 42/2015. (III. 12.) Korm. Rendelete a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről
- MNB - 4/2012. számú Vezetői körlevél - a pénzügyi szervezeteknél a közösségi és publikus felhőszolgáltatás igénybevételéből eredő kockázatokról

A felelősség kérdése

- **A felelősség nem szervezhető ki!**
- Szolgáltatási katalógus
 - SLA – érdemes alaposan átvizsgálni!
- Kockázati leltár
 - KRI – monitorozás
- Értesítések – incidensek, „KRI sértés”
- Jóváhagyások - módosítások esetén
- **Audithoz való jog – a Megrendelőé, az őt felügyelő Hatóságé**

Felhő-specifikus problémák

- *„Itt az adat, hol az adat?”*
 - EGT-n belül (?) – Meddig?
- *Titkosított adattárolás – dekódolás*
 - Titkosító kulcsok tárolása
 - Titkosító portálok
- *Hitelesítés*
 - kezdeti hitelesítés
 - erős hitelesítés...
- *Hibakezelés – üzleti döntések*
 - Pl. a szolgáltatási csatorna leállítása

Felhő-specifikus problémák

- *TelCo – kapcsolat*
 - Üzleti szolgáltatás
 - Management kontroll
- *DoS / DDoS támadások*
 - Szolgáltató
 - Megrendelő
- *Szolgáltatás lemondása*
 - Hitelt érdemlő adattörlés
 - Adatok átadása megfelelő struktúrában

Technikai aspektusok

- *Mentés - Archiválás*
- *Adatok bizalmassága, sértetlensége*
- *Kapcsolat kiesése -- kontrollvesztés*
- *Biztonsági vizsgálatok problémája*
- *Sérülékenységek kezelése, mellékhatások*
- *Változáskezelés – engedélyek*

Mire figyeljünk a szerződésben?

- *Üzleti igények pontos, teljes körű leírása*
- *SLA pontok leírása minden lényeges jellemzővel*
- *Titoktartási megállapodás*
- *Mentés – archiválási rend pontos leírása*
- *Auditálhatóság biztosítása, illetve audit riportok hozzáférhetővé tétele*
- *Értesítések, riportok pontos leírása*
- *Monitorozás lehetővé tétele*
- *Incidens- és kríziskezelési megállapodás*
- *Kártérítési egyezség*

Hol szeretjük, hol nem - a felhőt példák

- 😊
 - DNS szolgáltatás – „kényelmes”, és ha nem elég gyors, kockázatos is!
 - Hírportál; média streamer portál
- ☹️
 - Banki core rendszer
 - Egészségügyi szolgáltató központi rendszere
- ??
 - Email
 - Dokumentum tár

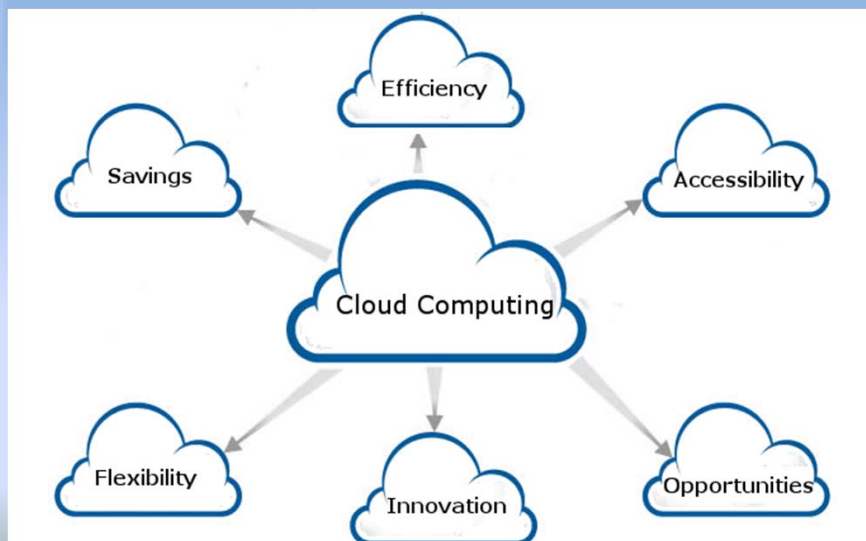
Hol szeretjük, hol nem - a felhőt Szempontok a döntéshez

- **Kockázatok felmérése – C, I, A tekintetben**
 - szolgáltatások,
 - adatkörök,
 - folyamatok
- **Felhő kontrollok elemzése**
 - Technikai kontrollok
 - Szerződéses lehetőségek – SLA, kárviselés stb.
- **Maradvány kockázatok**
- **Megfelelési kötelezettségek**
- **Érdemes SWOT-ot készíteni!**

***Kis színesek, avagy
Meglepő és mulatságos mondások***

- „Biztonságos, mert cloud!”
– *Rendelkezésre állás tekintetében talán...*
- „A Megrendelőnek nincs gondja a karbantartással”
– *Legalábbis nem olyan, mintha neki kellene végeznie...*
- „Multinacionális cégek használják, nyilván megfelel...”
– *Erre nincs mit mondani...*

***Egy majdnem elképzelt eset,
majdnem happy end-del***



Egy majdnem elképzelt eset, majdnem happy end-del

- **Megjelenik a Csábító Szolgáltatás,**
- **Az Üzlet meglátja a lehetőséget**
- **Specialisták (elit alakulat) segítik a „Csábító Szolgáltatás” használatba vételét – profi módon**
- **...a kockázatok, szabályozók figyelmen kívül maradnak...**
- **A kick-off meetingen kiderül, hogy vannak adatvédelemre, hitelesítésre vonatkozó „kötelezők”.**
- **Az elit alakulat meglepődik...**
- **Az Üzlet a megfelelő hatékonyság, az elit alakulat saját presztízse miatt erőlteti a gyors továbbhaladást.**

Egy majdnem elképzelt eset, majdnem happy end-del

- **A fő problémák**
 - *Adatok EGT-n kívül, bár Safe Harbour listán van*
 - *Adatok bizalmassága*
– *deperszonalizáció, titkosítás, házon belül tárolás*
 - *Hitelesítés – nem valódi dupla faktorú, a kezdeti hitelesítés miatt*
- **A megoldás**
 - *Titkosított tárolás + bizalom a Safe Harbour-ban...*
 - *Az adott subdomainre belépése csak dedikált csatornán lehet belépni – IP, CERT*
- **HAPPY END!!!**
- **...AZTÁN JÖTT SNOWDEN, ÉS LEROMBOLTA A BIZALMAT.**

Zárszóul

**A Felhő nem cél, hanem eszköz – használjuk
a megfelelő helyen, megfelelő célra,
megfelelő módon!**

KÖSZÖNÖM A FIGYELMET!

PÁV LICZ GYÖRGY

Hivatkozások

- <https://atos.net/content/dam/global/we-do/atos-cloud-risk-analysis-white-paper.pdf>
- <http://naih.hu/files/2015-10-06-Kozlemeny--Safe-harbor.pdf>
- <https://cloudsecurityalliance.org/group/cloud-controls-matrix/>
- <https://cloudsecurityalliance.org/csaguide.pdf>
- <http://mnb.hu>