SZÁMÍTÁSI FELHŐ ALAPÚ KRITIKUS INFRASTRUKTÚRÁK VÉDELME

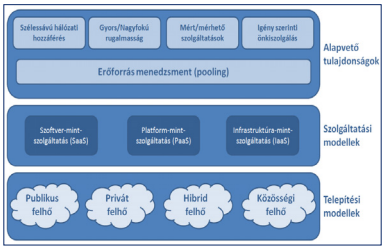
Kozlovszky Miklós [1] , Schubert Tamás [1], Ács Sándor [2], Prém Dániel [1], Póser Valéria [1]
1: Óbudai Egyetem, Neumann János Informatikai Kar, 2: MTA SZTAKI
{kozlovszky.miklos, schubert.tamas, prem.daniel, poserne.valeria}@nik.uni-obuda.hu, acs@sztaki.hu

Bevezetés

•A nyilvános felhő infrastruktúrák
- elosztott működést támogatnak
- nyilvános számítási infrastruktúrák

kedvelt célpontjai és rosszabb esetben könnyen eszközei is lehetnek kibertámadásoknak.
•A privát felhő infrastruktúrák
- elosztott működést támogatnak
- zárt (vállalat léptékű) számítási infrastruktúrák

alkalmasak kritikus infrastruktúrák működtetésére.
A megfelelően kialakított cloud infrastruktúrák sokféle „hagyományos" kibertámadás ellen hatékony védelmet biztosít(hat)nak, mindazonáltal a technológia sajátosságaiból adódóan új támadásokat is lehetővé tesznek.



Az általános felhőszámítási modell

•Informatika mint szolgáltatás (IT as a Service)
•Erőforrások adatközpontokba koncentrálása és konszolidálása
•Virtualizáció
•Infrastruktúra automatizálás (on-demand) igények alapján tetszőleges helyen és időben
•Rugalmasság (Elasticity) tetszőleges mennyiségben
•Erőforrás igénybevétele díjfizetés ellenében
•Monitorozás, szolgáltatás mérése
•Magas rendelkezésre állás

Felhő szolgáltatási modellek

A legelterjedtebb szolgáltatási modellek többnyire egymásra épülnek:
•Infrastructure as a service (IaaS)
•Platform as a service (PaaS)
•Software as a service (SaaS)
•…
•Security as a service (SecaaS)

Infrastruktúra szolgáltatás - IaaS

•Virtuális gépek (Pl.: Amazon EC2, GoGrid)
•Tárolókapacitás bérbeadása (Pl.: Amazon S3)
•Teljes virtuális adatközpont bérbeadása (virtual data center) (pl.: Amazon VPC, Vmware vCloud, Cisco Virtual Multi-tenant Data Center)
•A hálózat és a virtuális gépek tűzfallal védettek lehetnek, terhelésmegosztás lehetséges, redundáns eszközök alkalmazhatók
•Hozzáférés interneten keresztül

Cloud előnyök vs. problémák

•Költséghatékonyság >>korábbi megoldások
•Rugalmasság
•Biztonsági problémák (Gartner 2008)
- Privilegizált, több szintű felhasználói hozzáférés
- Adatkezeléssel kapcsolatos jogszabályi megfelelőség
  - A felhasználóra akkor is kötelezőek, ha cloud-ot használ.
- Adatkezelés földrajzi határok alapján
- Adat elkülönítés (titkosítás)
- Adatvisszaállítás
- Felhasználói ellenőrzési eljárások támogatása
- Hosszútávú szolgáltatásmegbízhatóság
  - Lock-in probléma, stabil vállalati szolgáltatások, stabil szolgáltató.

Felhő infrastruktúrák biztonsági problémái

•A felhő szolgáltatóknak meg kell védeni az ügyfelet (néha önmagától is).
•Az elosztott nagyméretű infrastruktúrák (cloud, grid, stb.) potenciális eszközök bizonyos típusú támadásokhoz
•Túlterheléses támadások (elosztott és nagyméretű infrastruktúra)
•Authentikációs, titkosítási feladatok költséghatékony, anonim numerikus megoldása
•A cloud sajátosságaiból adódóan az infrastruktúra szolgáltatót nehezebb megtörni, de ha sikerül: a homogenizált rendszer méretviszonyai, illetve a felhasználói bázis (több ezer vállalat) értéke hatalmas (v.ö.: bankrablás).
•A kereskedelmi felhők használatánál: 1 bankkártya ellopása egyszerűbb mint több ezres zombi gépfarmhoz vírus készítése.

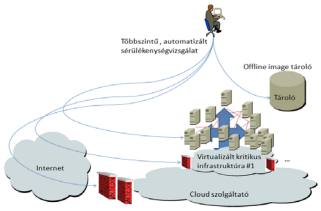
Eddigi „hangosabb" *felhő biztonsági* incidensek

•Magánszemélyek (Mat Honan /2012 augusztus/)
- Hatás: Apple iCloud (Social Eng.)--->GMAIL (Google)-->Twitter+…-> távolról reset-elt iPhone, iPad és MacBookAir
- Dropbox (incidens: többször) /utolsó bejelentett incidens 2012 július/
  - Hatás: Felhasználói email címek eltulajdonítása/értékesítése →kéreletlen levelek

•Vállalati ügyfelek
- Salesforce/force.com (incidens: 2007)
- SunTrust és ADP cégek: ~40.000 saját dolgozók + ~900.000 ügyfél rekord
- Amazon EC2/S3 (2008) BitTorrent site üzemeltetése
- Amazon EC2 (2011 április)
  - Sikeres támadás a SONY ellen EC2-ről
  - 70-100 millió PlayStation Network felhasználó adatai.

Felhő infrastruktúrák sérülékenysége

- Távoli menedzsment megoldások (VPN, Távoli asztal, Remote Shell, Web konzolok)
- Virtualizációs kiszolgáló (Hypervisor sérülékenységek)
- Hálózati sérülékenységek (lehallgatás, man in the middle, packet repeat, packet injection)
- Patch menedzsment
- Configuráció managemet
- Tárolók sérülékenysége (adatvesztés, adatmódosítás, illetéktelen hozzáférés)



Automatizált, felhő alapú sérülékenység vizsgálat

•A vizsgáló eszköz és a vizsgálandó infrastruktúra is virtualizált/felhő alapú
•Masszívan párhuzamosított eljárások
•Sebezhetőség vizsgálat
- Hálózati szinten
  - Felhőn kívüli és felhőn belüli vizsgálatok
- Szoftver stack szintű belső ellenőrzés (virtuális gépben)
- Online/offline image ellenőrzés támogatás

Virtuális környezetek monitorozása

•Online image figyelés
•Image szintű logolás és log elemzés
•Központi incidens monitorozó felügyelet

Összefoglalás

A felhő infrastruktúrák védelem szempontjából egyaránt tudnak pajzsként (privát , zárt felhők) és kardként (publikus, IaaS felhők) is működni.
Az általunk fejlesztett automatikus sérülékenység vizsgáló szoftvermegoldás több szinten, hatékonyan képes biztonsági szempontok alapján vizsgálni a felhő alapú infrastruktúrákat.

Köszönetnyilvánítás

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

ÚJ SZÉCHENYI TERV
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.