PUBLIKUS CLOUD BIZTONSÁGI KÉRDÉSEK

GONDOLATOK AZ BIZTONSÁGI KOCKÁZATOKRÓL

ÖSSZEGZÉS

EGYFELŐL
A felhőszolgáltatók által implementált biztonsági megoldások magasan az ipari átlag fölött, vannak: teljeskörű mélységi védelem (IDS, IPS). Paranoid, szisztematikus biztonsági eljárások…

MÁSFELŐL – a nemzetközi helyzet …
Az országok háborúja már informatikai csatatéren is zajlik
A támadással járó nyereség növekszik, ezért ezek a cégek esetleg előbb válhatnak célponttá?

KOCKÁZATOK 1

Kockázat = Valószinűség x Következmény x Sérülékenység

- Adatvédelem : adatvesztés, adatszivárgás, nem törlés
- Hálózat biztonsága
- Alkalmazásbiztonság – eddig biztonságos zónában
- Multitenant környezetekből adódó sérülékenység
- Felhasználói azonosítók eltulajdonítása
- Menedzsmentfelületek sérülékenysége

KOCKÁZATOK 2

- Biztonsági incidensek kezelése
- Szolgáltatás elérhetetlensége, szolgáltató csődje, átalakulása
-Szolgáltató személyi állománya, belső támadás, üzemeltetési hibák
- Szolgáltatóváltás, megkötöttség
- Compliance – standardoknak, előírásoknak megfelelés – és jogi kockázatok
- Auditálhatóság, átláthatóság
- Elosztott környezet következményei - minden megosztott: a fenyegetettségek a technológiák a felelősség – kellő körültekintéssel járunk-e el? Marad e rés a szabályozáson? (governance)

KITŐL VÉDJÜK MEG AZ ADATAINKAT?

- **Játékoskedvű fiatalok?**
- **Zsarolós hackerek? – *önmegvalósítás egy formája***
- **Kém hackerek? – *egy célpont***
- **Államilag támogatott hackerek? - *mindenki célpont***
- **Hacktivisták? - *revans***
- **Cyber terroristák? – *zavarkeltés, károkozás***

- **Terroristahajlamú, aktívan kárt okozó belső munkatárs?**
- **Szabotőrhajlamú nem együttműködő belső munkatárs?**
- **...**

HOGYAN VÉDJÜK MEG AZ ADATAINKAT ?

Bizalmasság - *Confidentiality*
- Titkosítsuk a mozgó adatokat
- Titkosítsuk a tárolt adatokat
- Robosztus kulcsmenedzsment
- IdAM

Intergritás - *Integrity*
- Naplózás, naplóelemzés
- Kétoldalú auditálhatóság
- Vírusellenőrzés és rosszindulatú szoftverek szűrése

Rendelkezésreállás - *Availability*
- Failover zónák
- Adatreplikáció?
- Hybrid cloud?

HOGYAN VÉDJÜK MEG AZ ADATAINKAT ? HYBRID CLOUD

Zero Trust Model (Forrester Research)

- **Minden erőforrás elérésére nagy biztonságú követelmények vonatkoznak– nincs biztonságos zóna**

- **Legkisebb jogosultság a hozzáférésszabályozási startégia, alapértemezett a nulla jogosultság**

- Minden forgalom mitorozása és naplózása a hálózat típusától -LAN vagy WAN - függetlenül

ÖSSZEGZÉS 2

A publikus felhőszolgáltatás egyrészt új biztonsági kockázatokat generál, másrészt a régieket meg felszámolja …

MÁS SZEMPONTOK, VÉLEMÉNYEK?