RIIGI INFOSÜSTEEMI AMET

Riik ja pilved

Kaur Virunurm

Riigi infosüsteemi amet
Küberturvalisuse teenistus

Kevad 2017

Minust

- Riigi infosüsteemi amet, küberturbe R&D
- Enne seda 9 aastat Skypes / Microsoftis
- MS tõstis / surus kõik teenuseid Azure suunas
  - Olen näinud Azure *compliance* ehitamist ja vastavaid protsesse „seestpoolt“
- Riigiametis 1a4k

Mis on üldse pilv?

- Pilv on:
  - Kellegi teise arvuti
  - Kellegi kolmandaga koos kasutuses
  - Hallatud üle avaliku neti ja ühise (veebi-) liidese
- Piir tavalise IT-haldusteenusega on hajus
  - Azure / Amazoni / Zone.. ühis-infra
  - O365 / Google / Dropboxi.. rakendus-teenused
  - Google Analytics? Akamai?
  - Ènamik moodsaid IT asju on pilved ☹

Ja mis on meil mureks?

- Riik ütleb:
  Asutus (andmekogu omanik) ja järelevalve tegija peavad süsteemile vajadusel alati juurde saama
- Aga pilved:
  - On (tihti) Eestist väljas
  - On nii suured, et nendega ei saa kaubelda
  - Ei haaku hästi ühegi EU riigi IT normidega
  - On tont-teab-kelle kontrolli all
- Andmeturbel (RIA) ja -kaitsel (AKI) samad mured

Seadused

- Avaliku teabe seadus
  Kas AvTS lubab või ei luba pilves andmekogu?
  Justiitsministeerium: jah, lubab!!!
- Isikuandmete kaitse seadus,
  uus Euroopa andmekaitse-seadus (GDPR)
  Nõuab EU majandusruumi.
- ISKE määrused ja rakendusjuhendid
  (rakendamine ja auditeerimine)

Pilv võtab ja annab

Pilv muudab turvalisust – mõlemas suunas.

Annab	Võtab
Infra parem turve	Haldusliidesed on avalikud
Skaleeruvus	Andmekanalid on avalikud
DDoS jt rünnete kaitse (kui klient oskab seda osta)	Kontode kaotus on fataalne
Asutuse tähelepanu on rakendusel	Piiriülesed sõltuvused
Parem seire	Hüperviisori eba-turve
	Välismaa jõuorganid
DevOps töökorraldus	DevOps töökorraldus

Kokkulepped

- Kuhugi tuleb tõmmata piir paranoia ja ükskõiksuse vahel
- Hetkel selleks RIA juhend
- Sisuliselt AKI, RIA, MKM juristide ja tehnika-inimeste kokkulepe
- ISKE ökosüsteemi lisa
- IaaS, PaaS, SaaS jaoks samad reeglid

RIA juhendi sisu - 1

- Tundke enda andmeid ja teenuseid Riskianalüüs, ISKE klassid
- Teadke, mida pilve pakkuja garanteerib ja teeb, ja mida ta EI garanteeri ega tee
- Teadke pilveteenuste spetsiifilisi riske ja muud pilve kasutamisega kaasnevat
- ISKE S3 andmed pilve panna ei tohi
- ISKE K3 / T3 andmeid vaid pika mõtlemisega

RIA juhendi sisu - 2

- Euroopa andmeruumi nõue
- Kontode haldus tugevaks
  - Inventuur admin-kontodest
  - Kahefaktoriline autent
- Salvestatud andmete krüpto
- Liikluse krüpto
- Töökorralduse läbimõtlemine
  - Muudatuste ja intsidentide haldus, seire, ddos kaitse, varundus, taaste

ISKE rakendus-juhised 2017

- ISKE rakendamise uus juhend
  Arvestab pilvega.
  Lubab osad meetmed asendada paberiga.
  Lisaks soovitame infovarad grupeerida – et oleks lihtsam.
- ISKE auditeerimise uus juhend
  Arvestab pilvega.
  „Kui kohapealne kontroll ei ole võimalik, võib audiitor piirduda lepingute, teenuste tingimuste jne kontrolliga.“
  Praktikas testimata.
- Proovige ja andke meile teada, kuidas läks!

ISKE moodulid

- On avaliku pilve kasutamise moodul (B 1.17)
  - Hetkel skoobis vaid avalik pilv
  - Keskendub riskianalüüsile
- On väljasttellimise (B 1.11) ja virtualiseerimise (B 3.304) moodulid
  - Täitmiseks on need üsna keerulised
- Tehnilist „pilve-rakenduste-turbe“ osa pole
- Kas oleks vaja? Mis osas? Andke nõu!

Avalikud suured pilved

- Amazon AWS, Azure, Microsoft O365, Google ja sarnased
  - Enamasti väljaspool Eestit
- Euroopa majandusruumi nõue
  - Mõnikord on teenusest seadistatav
  - Mõnikord (O365) ei ole
- Andmete krüptimise nõue
  - Transpordil – üldiselt kerge seadistada
  - Salvestamisel – keerulisem

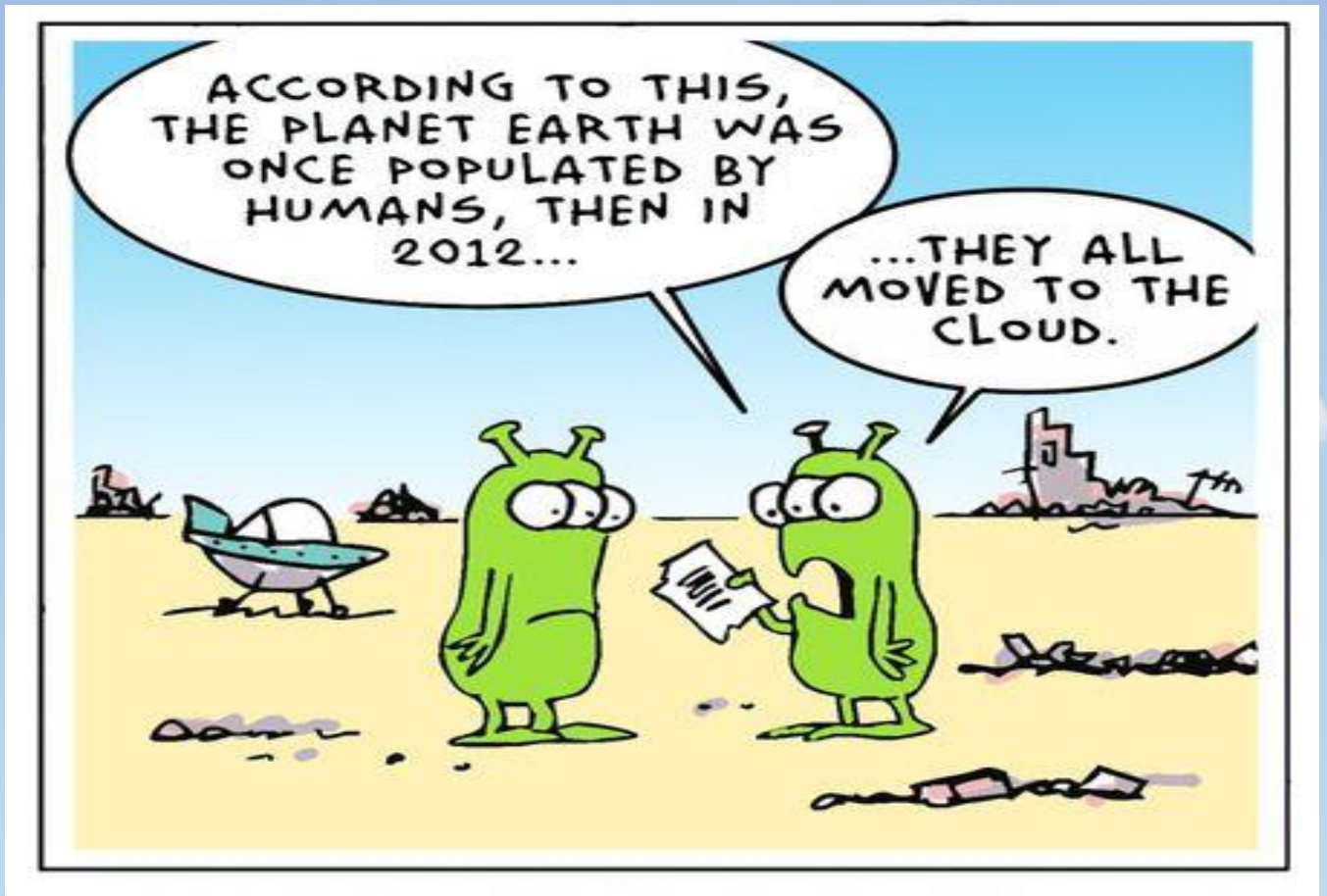
Avalikud Eesti pilved

- Zone, virtuaal.com, Levira jne on sisuliselt pilved
- Nende kasutamine riigis on hetkel hall ala. Neil pole riigi jaoks sobivat garantiid. Läbirääkimised käivad.
- „Eestist ostetud“ hosting teenus võib kasutada keda tahes, ka mitte-EU andmeruumi
- ISKE ei oska jagatud vastutusega arvestada.

Tulevik

- Pilv on teatud juhtudel okei
- Praktikat vähe (või on ebaseaduslik)
- Proovige!
- Vajadusel küsige MKM või RIA käest nõu
  - MKM – Mikk Lellsaar
  - RIA – Tarmo Hanga, Andres Kütt
  - arhitektuurinõukogu / baastaristu nõukogu
- Jagage oma kogemust!

Küsimused?



Kaur Virunurm
kaur.virunurm@ria.ee