Júní 2022

Algengar fullyrðingar og spurningar um rekstrar- og hýsingarumhverfi

Viðauki við

Öryggis- og þjónustustefnu fyrir hýsingarumhverfi

- Stefna um notkun skýjalausna

Stjórnarráð Íslands
Fjármála- og efnahagsráðuneytið

Útgefandi:
Fjármála- og efnahagsráðuneytið

Júní 2022

fjr@fjr.is

www.fjr.is

Umbrot og textavinnsla:
Fjármála- og efnahagsráðuneytið

Algengar fullyrðingar um notkun rekstrarumhverfa í umsjón þjónustuaðila

Öll kerfi ríkisaðila eiga að fara í skýið

- Öryggis- og þjónustustefna fyrir hýsingarumhverfi er hvorki ákvörðun um að öll kerfi skulu vistuð í skýjaþjónustu né hjá einum tilteknum þjónustuaðila.
- Stefnan felur ekki í sér að „allt skal fara í skýið“ (e. cloud-only) heldur að nýta skuli skýjalausnir á réttan hátt (e. cloud-smart).
- Stefnan gefur ríkisaðilum umgjörð til að meta vistunarstað, þ.m.t. skýjalausnir út frá áhættu og ávinningi.
- Stefnan er hluti af upplýsingatæknistefnu hins opinbera og styður við aðrar stefnur s.s. stafræna stefnu um þjónustu hins opinbera, öryggisflokkun gagna ríkisins, sem er í vinnslu, og gagnastefnu sem verður unnið að og birt.

Gögn í skýjaþjónustu eru ekki örugg

- Öryggi gagna í skýjaþjónustu er að jafnaði betur tryggt en í staðbundnum rekstri (e. on premise). Skýjaþjónustuaðilar hafa í krafti stærðar, reynslu og þekkingar betri og meiri möguleika til að tryggja öryggi og veita viðskiptavinum sínum öflugri öryggislausnir á hagkvæmari hátt en viðskiptavinir geta komið sér upp sjálfir. Öryggi gagna er betur tryggt með að nýta þjónustu sérhæfðra þjónustuaðila á öruggan hátt og staðfesta hæfni þeirra með vottunum og úttektum.
- Viðnámsþróttur skýjalausna og skýjaþjónustuaðila gagnvart álagsárásum og þjónusturofsárásum er meiri en hjá minni aðilum.
- Þótt þjónusta sé kölluð almennt ský (e. public cloud) er hægt að takmarka aðgengi að gögnum með sambærilegum eða betri hætti en ef um staðbundinn rekstur er að ræða.
- Skýjaþjónustur gefa stofnunum möguleika á að greina að gögn og vinnslur í aðskilin rekstrarumhverfi innan skýjaþjónustu og lágmarka þannig hugsanlegt tjón af öryggisbrestum og árásum. Þessi umhverfi geta verið algerlega lokuð frá almennum aðgangi og aðeins aðgengileg frá starfsstöð ríkisaðila ef þess er krafist.

Gögn verða óaðgengileg og tapast ef samband Íslands við umheiminn rofnar

- Skýjaþjónustur geta verið staðsettar innan sem utan íslenskrar lögsögu og reknar af íslenskum eða erlendum lögaðilum. Stofnanir geta því blandað saman virkni og staðsetningu eigin kerfa að eigin óskum t.d. út frá flokkun gagna, kröfum um varðveislu, lögsögu eða afköst.
- Skýjalausnir bjóða upp á að gögn og vinnslur séu spegluð/afrituð milli mismunandi landfræðilegra staðsetninga sama þjónustuaðila, milli þjónustuaðila eða í staðbundin rekstrarumhverfi, jafnt erlendis sem á Íslandi.
- Á grundvelli áhættumats er nauðsynlegt að tryggt sé að stjórnvöld hafi aðgengi að gögnum þó að eldgos eða aðrar hamfarir eigi sér stað á Íslandi. Því eru skýjaþjónustur erlendis góð viðbót við núverandi rekstrarumhverfi. Staðsetning og afritun gagna er hluti

af nauðsynlegri kröfugreiningu til grundvallar ákvörðunar um fyrirkomulag hýsingar jafnt innanlands sem utan.

- Hluti af skipulagningu á notkun hýsingarumhverfa og skýjalausna er að huga að útleiðingu og flutningi gagna. Eignarhald gagna, flutningur þeirra og útleiðingaráætlanir eru hluti af kröfum sem gerðar eru til seljenda í innkaupaferli Ríkiskaupa.
- Miðað við núverandi fjölda gagnatenginga Íslands við umheiminn og fyrirhugaða viðbót (ÍRIS) er rekstraröryggi þeirra tenginga talsvert meira en núverandi öryggi flestra ríkisaðila og smærri þjónustuaðila á íslenskum markaði. Miðað við núverandi stöðu er talið að uppitími gagnasambands Íslands sé um það bil 99,997% til 99,9997% og muni aukast með tilkomu ÍRIS sæstrengsins. Auk þess er fyrir tilstilli nýrra möguleika í fjarskiptatækni sífellt verið að bjóða upp á fleiri gerðir tenginga en sæstrengi, t.d. gervihnattasambönd sem nota má til neyðarsamskipta og á hamfara- og stríðssvæðum.

Erlend stjórnvöld og eftirlitsstofnanir hafa aðgang að upplýsingum

- Hluti af hönnun öruggra lausna er að beita bestu mögulegu dulritun á gögn sem sett eru í skýjaþjónustur. Stofnunum mun verða veitt leiðsögn og aðstoð við að meta hversu mikið og þá hvernig skuli verja gögn með dulritun eða öðrum hætti byggt á áhættumati og hvar gögnin eru vistuð.
- Í gegnum innkaupaferli Ríkiskaupa verður tryggt að allir þjónustuaðilar sem vista og vinna upplýsingar uppfylli kröfur persónuverndarlaga og að starfsemi sé innan Evrópska efnahagssvæðisins (EES)[1].
- Stórir, alþjóðlegir þjónustuaðilar hafa í auknum mæli lýst yfir að þeir muni lágmarka og takmarka eins og mögulegt er afhendingar til yfirvalda á grundvelli rannsóknarheimilda hvort heldur bandarískra aðila (þar sem móðurfélag er) eða af hálfu þess ríkis sem gagnaver er staðsett í.

Notkun stórra þjónustuaðila (Microsoft, Amazon, Google o.fl.) hamlar samkeppni og dregur úr nýsköpun

- Öruggar og staðlaðar skýjaþjónustur gera ríkisaðilum mögulegt að koma nýsköpun og prufum fyrr í þróun, samanber Stafrænt Ísland, sem flýtti fyrir stafrænni umbyltingu með að hagnýta sér skýjaþjónustur sem undirliggjandi rekstrarumhverfi.
- Stöðlun og vönduð innkaup tryggja að umhverfi ríkisaðila séu færanleg milli þjónustuaðila byggt á opnum stöðlum svo mögulegt sé að halda virkri samkeppni á markaði.
- Öruggar skýjaþjónustur gera smærri aðilum á markaði, s.s. nýsköpunarfyrirtækjum, mögulegt að bjóða þjónustu til ríkisaðila hraðar en uppfylla á sama tíma kröfur um öryggi og rekstur.
- Innkaupaferli er hannað með tillit til að þessir eiginleikar þjónustunnar verði nýttir af ríkisaðilum.

[1] Evrópska efnahagssvæðið telur þjóðríki innan Evrópusambandsins auk landanna þriggja innan EFTA, Íslands, Noregs og Liechtenstein..

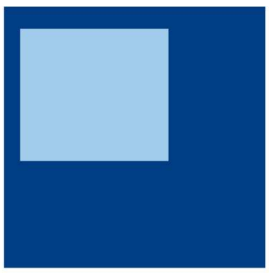
Algengar spurningar um rekstrar- og hýsingarumhverfi í umsjón þjónustuaðila

Mun ríkið geyma gögn sín í erlendum skýjaþjónustum og er það öruggt?

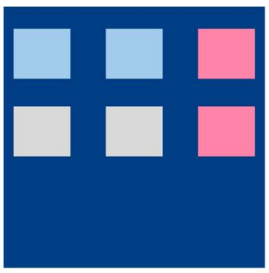
- Öryggi gagna í skýjaþjónustu sem ríkið kaupir er alla jafna meira en í staðbundnum rekstri (e. on premise) innan veggja einstaka ríkisaðila.
  - Einungis hæfir aðilar innan EES munu geta boðið ríkisaðilum þjónustu. Gera þarf birgjarýni á öllum aðilum hvort heldur þeir eru innlendir eða erlendir. Opinber innkaupaferli (Ríkiskaup) styðja þessa vinnu með að tryggja að aðeins hæfir þjónustuaðilar m.t.t. öryggis, persónuverndar og gæða þjónustunnar, séu aðilar að innkaupakerfi Ríkiskaupa.
  - Mörg nýleg dæmi eru til um hvernig skýjaþjónustur hafa ekki orðið fyrir minni áhrifum netárása á meðan staðbundinn rekstur verður fyrir miklum áhrifum:
    - Árás haustið 2021 á HR og fleiri stofnanir og fyrirtæki sem sérstaklega var beint að rekstri póstþjóna sem ekki voru í skýinu. Varð Háskólinn í Reykjavík til dæmis fyrir minni áhrifum þar sem hluti af rekstri var kominn yfir í skýjaþjónustu Microsoft.
    - Nýlegur „log4j“ veikleiki. Þrátt fyrir að endanleg áhrif veikleikans séu enn ekki ljós er vitað að skýjaþjónustuaðilar gátu í krafti stærðar sinnar, sérþekkingar og tæknilegra úrræða brugðist hraðar við og lagfært gallann meðan hægar gekk að finna og lagfæra veikleikann í minni umhverfum. Aðgengi að hæfum aðilum til að sinna viðhaldi og rekstri á staðbundnum tölvukerfum getur verið takmarkandi þáttur í að hugbúnaður sé uppfærður tímanlega, t.d. vegna öryggisveikleika.
    - Stærri þjónustuaðilar hafa meiri getu til að bregðast við ógn á skilvirkari hátt en einstaka stofnanir, sem þýðir hærra öryggisstig og lægri kostnað vegna öryggisúrræða.
    - Varnir gegn álagsárásum (DDOS) eru hluti af þjónustuframboði allra skýjaþjónustuaðila og í samræmdum tæknigrunnum fyrir upplýsingar sem gefnir verða út verður stofnunum leiðbeint um val og uppsetningar á slíkum vörnum. Möguleikar til að auka við afkastagetu skýjaþjónustu hratt eru líka meiri, auk þess sem skýjalausnir eru að jafnaði hraðari og hagkvæmari en staðbundinn rekstur.
    - Bandarísk yfirvöld hafa gefið út leiðbeiningar um öryggi upplýsingakerfa til stofnana sinna óháð hvort þau eru í skýjaþjónustu eða ekki sem byggir á „Zero Trust“ sem er grundvöllur að öryggisnálgun skýjalausna.
    - Skýjaþjónustur geta boðið upp á aðgengi að mikilli afkastagetu eða geymslu annað hvort í mjög skamman tíma eða með hagstæðum langtímakjörum. Því verður það fjárhagslega mögulegt fyrir stofnanir að varðveita gögn á nokkrum stöðum frekar en að þurfa að geyma gögn (t.d. mikið magn eins og kvikmyndasöfn) á einum stað. Aðskilin afrit tryggja að þó annað eintakið, hvort sem það er staðbundið eða í skýi, tapist þá séu gögnin tiltæk.

- Margar stofnanir eru nú þegar kaupendur að mismunandi skýjaþjónustu sem hafa verið keyptar til að leysa ákveðin verkefni.
    - Mikilvægt er að samhæfa og tryggja kröfur ríkisaðila til öryggis og kostnaðareftirlits í skýjainnleiðingu. Innkaupaferli Ríkiskaupa á hýsingar- og rekstrarumhverfi ríkisaðila styðji við þær kröfur.
- Öll gögn í einu hugbúnaðarkerfi eru ekki endilega á sama öryggis- eða viðkvæmnisstigi.
    - Viðkvæmustu gögn ríkisins ber að vernda út frá virði og eðli þeirra og afleiðingar uppljóstrunar, s.s. með aðskilnaði rekstrar- og hugbúnaðarkerfa frá öðrum umhverfum.
    - Önnur gögn en þau sem falla í hæsta öryggisstig er heimilt að vista í skýjaþjónustum innan EES.
    - Vinna við öryggisflokkun gagna ríkisins er í gangi í samráði ráðuneyta og fer í opið samráðsferli í kjölfarið.
    - Með því að blanda saman staðbundnum rekstri, hýsingu hjá þjónustuaðila og skýjaþjónustum er hægt að aðgreina varðveislu, viðhald og miðlun mikilvægra upplýsinga, þ.m.t. grunnskráa samfélagsins. Þá er t.d. tryggt að þó miðlun verði óvirk sé varðveisla mikilvægra upplýsinga ósköðduð.
- Mikilvægt er að aðgreina gögn á hæsta öryggisstigi og setja í aðskilin „eldvarnarhólf“. Skýjaþjónustur veita þann möguleika að hægt er að aðgreina ólík verkefni sama aðila til að tryggja að öryggisbrestur í einu verkefni hafi ekki áhrif á gögn í öðrum verkefnum á hagkvæman hátt þar sem ekki þarf að fjárfesta í vélbúnaði eða uppsetningu hans.

Ef öll gögn eru í sama rekstrarumhverfi og varin með sama hætti er líklegt að einhver gögn séu ofvarin en önnur ekki varin nægjanlega vel



Með því að aðgreina ákveðin gögn eða vinnslur er hægt að hækka öryggisstig innan sama rekstrarumhverfis



Með því að aðgreina gögn og vinnslur eftir mikilvægi og öryggisstigi og sækja þjónustur frá mismunandi rekstrarumhverfum (staðbundið, hýst hjá þjónustuaðila eða skýjaþjónustu) er hægt að hámarka öryggisstig út frá eðli gagnanna

Bandarísk yfirvöld geta skv. lögum óskað eftir að fá gögn annarra þjóðríkja frá þjónustuaðilum svo fremi sem móðurfélag skýjaþjónustu sé bandarískt.

Bandarísk stjórnvöld og eftirlitsstofnanir geta, skv. lögunum, óskað eftir gögnum sem hýst eru af bandarískum lögaðilum eftir tveimur leiðum.

- Hleranir rafrænna samskipta á grundvelli FISA section 702 sem fara um fjarskiptainnviði bandarískra lögaðila eða eru í vörslu bandarískra aðila safnað saman af fjarskiptaaðila út frá t.d. netfangi eða símanúmeri þess aðila sem á að afla gagna um.
    - Mikilvægt er að notkun upplýsingakerfa óháð staðsetningu og rekstrarformi uppfylli viðeigandi öryggi m.t.t. dulritunar samskipta til að verja samskipti og gögn í flutningi. Samskipti við skýjaþjónustur sem og aðrar hýstar lausnir getur geta farið yfir ýmsa

óvarða samskiptainnviði sem stjórnvöld eða aðrir aðilar eru að hlera. Því er dulritun samskipta mikilvægi frá enda til enda (e. End-to-End Encryption). Skýjastefna og öryggisflokkun gagna leggur nauðsynlegan grunn að slíku varnarkerfi.

- Í Evrópu hefur FISA valdið nokkrum óróa, þar sem löggjöfin uppfyllir ekki kröfu Sáttmála ESB / Mannréttindasáttmála Evrópu um grundvallarréttindi um að kveða skuli á um skerðingar á friðhelgi einkalífs með skýrum hætti í lögum, s.s. skilyrði fyrir skerðingunni og réttindi einstaklinga vegna hennar.

- Afhending gagna frá þjónustuaðila til að uppfylla réttarúrskurð á grundvelli CLOUD Act (Clarifying Lawful Overseas Use of Data Act) frá eftirlitsstofnunum.
  - Þjónustuaðilar (Microsoft, Amazon Web Services, o.fl.) hafa verið að bregðast við þessu, bæði út frá lagalegum forsendum og samningum og að tryggja að gögn viðskiptavina séu aðeins innan þess landfræðilega svæðis sem þeir kjósa, bæði gögnin sjálf og upplýsingar um notkun, fjarmælingar- og greiningagögn (Service Generated Data).
  - Þjónustuaðilar og kaupendur þjónustu þurfa að nýta viðeigandi öryggisúrræði, s.s. dulritun gagna í vörslu ytri aðila óháð staðsetningu og rekstrarformi í samræmi við öryggisstig gagnanna. Dulritunarlykla skal vera hægt að varðveita utan þjónustunnar og gera þannig þjónustuaðila ómögulegt að afhenda gögnin til ytri aðila í ódulrituðu formi.
    - Hafi þjónustuaðili ekki dulritunarlykil (Private Key) til að afkóða gögnin getur hann ekki afhent gögnin til yfirvalds á læsilegu formi. Margir þjónustuaðila bjóða upp á lausnir til að viðskiptavinir varðveiti dulritunarlykla utan kerfanna (Bring Your Own Key).
  - Stærstu þjónustuaðilar á þessu sviði (Microsoft og Amazon Web Services / AWS) hafa á undanförnum mánuðum brugðist við kröfum evrópskra aðila og sett af stað verkefni í að gera þjónustur sínar í Evrópu aðgreindari og sjálfstæðar frá allri vinnslu innan Bandaríkjanna, þ.m.t. notkunarupplýsinga, bilanagreining, tölfræði og reikningagerð, þ.m.t. „Storing and Processing EU Data in the EU“ (Microsoft) og EU Data Protection (amazon.com).
  - Afhendingar á grundvelli þessara laga eru tiltölulega fátíðar og stærri þjónustuaðilar birta yfirlit yfir þær með reglubundnum hætti:
    - AWS: Law Enforcement Information Requests - Amazon Customer Service
    - Microsoft: Law Enforcement Request Report | Microsoft CSR
    - Google: Global Request for user information (Transparency Report)

Ef Ísland verður sambandslaust við umheiminn er ótækt að gögnin liggi á erlendum netþjónum / Er gögnum íslenska ríkisins ekki best komið fyrir í innlendum gagnaverum?

- Staðan í dag er þannig að nær einungis íslenskir þjónustuaðilar bjóða upp á þjónustur í íslenskum gagnaverum. Stórir þjónustuveitendur (e. hyperscalers) á borð við Microsoft, Amazon og Google gera það ekki enn sem komið er.
- Ríkisaðilum er frjálst að velja þjónustuaðila m.t.t. kostnaðar, áhættumats og fleiri þátta, s.s. að undangengnu innkaupaferli Ríkiskaupa um skýjaþjónustur, sem kláraðist vorið 2022.
- Algert sambandsleysi við útlönd er möguleiki en ólíklegt er að það gerist. Þennan þátt og fjölda annarra skal hafa í huga í áhættumati á skýjaþjónustu innan ramma opinberra innkaupa. Viðbrögð við áhættu á sambandleysi geta m.a. falist í afritunarkröfum.

- Með nýjum sæstreng (IRIS) verður enn ólíklegra að sambandsrof hafi áhrif á þjónustur. Auk þess mun samskiptahraði aukast til muna.

Er löglegt að geyma gögn íslenska ríkisins utan Íslands?

- Það fer eftir því um hvaða gögn ræðir – tryggja þarf öryggi (leynd, réttleika og aðgengi) gagna óháð staðsetningu með viðeigandi aðferðum (aðgangsstýringar, dulritun, afritun, speglun, o.s.frv.).
- Almenna svarið við spurningunni er já, en sum gögn sem varða tiltekin afmörkuð viðfangsefni stjórnvalda er skylt að varðveita innanlands. Hér er mikilvægt að aðgreina vinnslu/miðlun annars vegar og varðveislu til að afmarka gögn með skilvirkum hætti til að hámarka öryggi og notagildi.
- Leyfilegt er að vista gögn, að fráskildum gögnum í hæsta öryggisstigi, í skýjaþjónustum innan EES, þar með taldar persónugreinanlegar upplýsingar að undangengnu áhættumati/mati á áhrifum á persónuvernd.

Dæmi um þjóðríki sem leyfa notkun á skýjaþjónustum innan EES

- Evrópusambandið (EU) samþykkir Amazon Web Services sem skýjaþjónustu („Rammasamningur" – Cloud II)
- Danmörk, sameiginlegar mannauðslausnir
- AWS vinnur með GAIA-X, evrópsku skýjasamvinnuverkefni
- Bresk yfirvöld hafa gert stofnunum aðgengileg innkaup og auðveldað uppsetningar á Google Cloud þjónustum

Tilskipun ESB 2018/1807 um frjálst flæði ópersónugreinanlegra upplýsinga (e. framework for the free flow on non-personal data) tekur af allan vafa um að aðildarlöndum ESB sé leyfilegt að vista gögn í gagnaverum eða skýjaþjónustum hvar sem er innan evrópska efnahagssvæðisins. Lög um persónuvernd og vinnslu persónuupplýsinga (GDPR) leyfa að sama skapi frjálst flæði persónuupplýsinga innan innri markaðarins. Tilskipunin tryggir þannig frjálst flæði allra gagna innan hans. Stefnt er að því að tilskipunin verði innleidd í íslensk lög eftir að tilskipunin verður tekin upp í EES samninginn.

Nánar um vistunarstaði ópersónugreinanlegra gagna.

Tegundir skýjaþjónustu

Skýjaþjónustur skiptast í nokkrar tegundir sem er mikilvægt að greina á milli þegar rætt er um þær:

IaaS – Infrastructure as a Service – Innviðaþjónustuveita. Auðlindir, s.s. reiknigeta eða geymslupláss, í innviðum innan eða utan Íslands.

> *Dæmi um þjónustu: „Azure high-performance computing" og „Amazon Web Services S3 storage" þar sem viðskiptavinur fær aðgang að auðlindum til að keyra vinnslur og geyma gögn. Notendur setja svo upp eigin hugbúnað eða smíða kerfi sem nota þessar auðlindir og bera ábyrgð á rekstri og öryggi þess hugbúnaðar.*

PaaS – Platform as a Service – Kerfisþjónustuveita. Staðlaðar uppsetningar sem sinna ákveðnum tilgangi, t.d. gagnagrunnar sem eru aðgengilegir án þess að þurfi að setja sérstaklega upp undirliggjandi auðlindir. Hver viðskiptavinur er aðskilinn frá öðrum.

> *Dæmi um þjónustu: Gagnagrunnar þar sem þjónustuaðili ber ábyrgð á rekstri grunnsins og allra undirliggjandi auðlinda. Eldveggir sem keyra á samnýttum auðlindum.*

SaaS - Software as a Service – Hugbúnaðarþjónustuveita. Þegar þjónustuaðili ber fulla ábyrgð á rekstri lausnarinnar og veitir aðgang að tilbúnum hugbúnaði/virkni t.d. tölvupósti.

> *Dæmi um þjónustu: Microsoft 365 skýjaþjónustan þar sem veittur er aðgangur að hugbúnaði og þjónustum (tölvupóstur, dagbækur) á staðlaðan hátt til margra aðila. Fjárhagskerfið ORRI er notað af mörgum aðilum en sameiginlegir innviðir eru notaðir undir kerfið. Verkstjórnarkerfi sem aðgengileg eru í gegnum vafra (t.d. Asana og Monday) eru önnur dæmi á markaði.*

Skýjaþjónustur eru veittar með nokkrum nýtingarmódelum eftir því hvernig þjónustan er veitt:

Almenn skýjaþjónusta (Public Cloud) er rekin af þjónustuaðila og notuð af mörgum lögaðilum en gögn og vinnsla eru aðgreind innan umhverfisins. Uppsett þjónusta í almennu skýi getur þó haft aðgangstakmörk fyrir tiltekinn hóp notenda og/eða verið tengd við einkaský.

Blönduð skýjaþjónusta (Hybrid Cloud) eiga við þar sem einn tiltekinn lögaðili er búinn að samtengja umhverfi í eigin eigu við almenna skýjaþjónustu.

Samfélagsský (Community Cloud) eru tölvuský sem ætluð eru tilteknum (einsleitum) hópi lögaðila. Samfélagsský geta verið rekin af og í eigu eins notanda eða þjónustuaðila.

Einkaský (Private Cloud) er í eigu þess lögaðila sem notar það og býður upp á marga af eiginleikum skýjalausna og er ekki í notkun annars lögaðila.

Alþjóðleg skilgreining á skýjaþjónustu

Heimild: National Institute of Standards and Technology (NIST).