Tallinna Ülikool

Informaatika Instituut

# Riskijuhtimine pilveteenuste kasutuselevõtul

Magistritöö

Autor: Karel Lember

Juhendaja: Andro Kull

Kaasjuhendaja: Riho Kurg

Autor: ..... „ ..... „2015

Juhendaja: ..... „ ..... „2015

Kaasjuhendaja: ..... „ ..... „2015

Instituudi direktor: ..... „ ..... „2015

Tallinn 2015

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

..... .....

(kuupäev) (autor)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina _____ (sünnikuupäev: _____)

(*autori nimi*)

1. annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
   _____
   _____
   _____

   (*lõputöö pealkiri*)

   mille juhendajad on _____,

   (*juhendajate nimed*)

   säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.
2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas _____

*allkiri ja kuupäev*

# Sisukord

# Lühendite seletused

NIST - *National Institute of Standards and Technology*

ISACA - *Information Systems Audit and Control Association*

CSA - *Cloud Security Alliance*

ENISA - *European Network and Information Security Agency*

ITSM - *IT Service Management*

ISMS - *Information Security Management System*

SME - *Small and Medium Enterprises* - väikese- ja keskmise suurusega ettevõtted

AKI - Andmekaitse Inspektsioon

IT - infotehnoloogia

AWS - *Amazon Web Services*

SaaS - *Software as a Service* - tarkvara teenusena

PaaS - *Platform as a Service* - platvorm teenusena

IaaS - *Infrastructure as a Service* - taristu teenusena

SLA - *Service Level Agrement* - teenustaseme leping

VPN - *Virtual Private Network* - virtuaalne privaatvõrk

# 1. Sissejuhatus

Euroopa komisjoni hinnangu kohaselt on pilveteenuste turg ja kasutusmaht Euroopa Liidus lähiaaastatel jätkuvas tõusutrendis ning selles nähakse suurt potensiaali. Samas leitakse, et suurim takistus kõigi võimaluste ärakasutamisel on teenuste usaldusväärsus ja sellega seotud riskid (Euroopa Komisjon, 2013). Järeldusele, et mittepiisavad teadmised pilveteenustest on suurim teenuste mittekasutamise põhjus, on jõudnud ka Eurostat oma 2014. a uuringus (Eurostat, 2014), kus leitakse, et oma teadmisi peab mittepiisavaks 42% Euroopa Liidu ettevõtetest. Olukorras, kus ühest küljest tuntakse pilveteenuste vastu suuremat huvi, teisest küljest ei peeta neid usaldusväärseks, kuid samaaegselt tunnistatakse teadmiste puudulikkust, on oluline tõsta üldist teadlikkust valdkonnast, selgitada probleeme ja pakkuda võimalikke lahendusi.

Seoses igapäevase kokkupuutega pilveteenustel põhinevate infotehnoloogiliste lahendustega, näeb autor vajadust kirjutada teemal, mis kaldub pilveteenuste käsitlemisel valdavalt varju jääma, kuid on oma olemuselt siiski tähtis. Väga tihti keskendutakse teenuste ning teenusepakkujate valikul funktsionaalsusele ja hinnale, mis on kahtlemata olulised, kuid teenustega seotud ohtude ja riskide maandamise osas jäädakse ebamääraseks. Peitutakse mugava ja üldsõnalise "pilveteenused on ebaturvalised" käibefraasi ja muude müütide (Gartner, 2014) taha . Tihti aga ei mõtestata seda ebaturvalisust kasutajate poolt lahti ja veel vähem mõistetakse, et tegelikkuses on pilveteenuste kasutamise turvalisus lisaks teenusepakkujate poolsele panusele tingitud ka kasutajate omapoolsetest oskustest, teadmistest, suhtumisest ja nõuetest teenusepakkujatele.

Magistritöö eesmärk on anda ülevaade pilveteenustest, nende teenustega seotud riskidest, teenusepakkujate poolsetest riskimaandusvõimalustest, oma teenuse kvaliteedi tõestamisest ning olulise info leitavusest teenuste kirjeldusest. Samuti uuritakse teenuste (võimalike) kasutajate nägemust pilveteenuste kasutamisest ja kasutamise riskantsuse hindamist. Eelnevast lähtudes antakse soovitusi, kuidas pilveteenustega seotud riske maandada.

## 1.1 Magistritöö uurimisprobleem ja eesmärgid

Kuigi pilveteenuseid[1] on võimalik kiirelt ja mugavalt kasutusse võtta, ei ole seda mõistlik teha kiirustades ning tarbija seisukohast lähtudes on mitmeid asjaolusid, mida tasub tähele panna. Lähtuvalt pilveteenuste kasutamise kasvust kasvab ka vajadus tunda sellega kaasnevaid ohte ning oskus neid ennetada või tekkinud probleeme lahendada. Magistritöö uurimisprobleem on: kuidas vähendada pilveteenuste kasutuselevõtul ja kasutamisel erinevaid riske, et kasutatavad teenused töötaksid võimalikult probleemidevabalt.

Magistritöö põhieesmärk on välja selgitada võimalikud pilveteenustega seotud riskid ning välja tuua viise nende maandamiseks. Tööna moodustub kompaktne ülevaade valdkonda puudutavast olulisemast teabest.

Põhieesmärgi saavutamiseks on mitmeid alameesmärke:

- anda ülevaade pilveteenustest ja nendega seotud mõistetest;
- anda ülevaade pilveteenustega seotud põhilistest riskidest;
- anda ülevaade teenusepakkujate poolsetest riskide maandusvõimalustest ja vastavasisulisest klientide teavitamisest;
- anda ülevaade teenuse (võimalike) kasutajate poolsest suhtumisest pilveteenustesse, riskinägemusest ja riskide maandamise võimalustest;

Eelnenud loetelu põhjal teha ettepanekuid ja anda soovitusi pilveteenustega kaasneda võivate riskide maandamiseks teenuste edukaks rakendamiseks.

## 1.2 Magistritöö struktuur ja kasutatavad meetodid

Magistritöö on koostatud ülevaateuuringuna, mille eesmärk on asjassepuutuva olulise ning ajakohase info kokkukogumine, süstematiseerimine ja tõlgendamine. Lisaks tööle allikatega nagu raamatud, artiklid, internet, on täiendavaid andmeid kogutud uuringute näol kvalitatiivsete ja kvantitatiivsete meetodite (Õunapuu, 2013) kaudu.

[1] Vt peatükk 2. Pilveteenused

Töö koosneb neljast põhilisest osast:

Esmalt pilveteenuseid ja sellega seotut puudutav ülevaateline osa, kus kirjeldatakse teenuste tüüpe, levinumaid probleeme, standardeid.

Teises osas kirjeldatakse ja teostatakse uuring, milles vaadeldakse internetist andmete kogumise põhjal teenusepakkujate teenuste tingimuste leitavust ja arusaadavust tavakasutaja vaatenurgast. Uuringu eesmärk on välja selgitada, kuivõrd panustavad teenusepakkujad ise oma teenuste kvaliteeti omades vastavaid kolmanda osapoole sertifikaate ja kvaliteeditunnistusi. Uuritakse, kuidas on vastav info võimalikele klientidele leitav ja kas seda on peetud oluliseks esile tuua. Magistritöös lähtub töö autor seisukohast, et sõltumatute kolmandate osapoolte hinnangud teenusele on sisuline tagatis teenusepakkujate üldistele turunduslubadustele.

Kolmandas osas on pilveteenuste (potentsiaalsete) kasutajate seas tehtud uuring, mille eesmärgiks on teabe ja arvamuste võrdlus. Uuritakse kasutajate suhtumist pilveteenustesse, mida peetakse teenusepakkuja valikul oluliseks, teadlikkust võimalike probleemide osas, olulisemaid riske, valmisolekut riskide avaldumiseks jne.

Neljas osa on kokkuvõte järelduste ja ettepanekutega riskide maandamiseks.

## 1.3 Kitsendused

Kuigi töös leiduvas pilveteenuste kirjelduses tuuakse välja mitmed võimalikud pilveteenuste võimalused, keskendub autor peamiselt avaliku pilve teenustele, neis sisalduvatele *IaaS*[2] ja *SaaS*[3] teenusmudelitele ning teenuste kasutajana lähtub kliendivaates vaid väikese ja keskmise suurusega ettevõtete, kui paindlike ja oma otsustes kõige vabamate ärikasutajate, vajadustest.

Piirang on vajalik, sest kõigi võimalike teenuste ning kõigi võimalike teenusetarbijate hulk ja võimalike teenuste kombinatsioon on liialt mahukas. Samas annab enamlevinud teenuste käsitlemine piisava ülevaate, mida saab vajadusel laiendada ka teistele teenustele, kui ka

[2] Vt peatükk 2.4 Pilve teenusmudelid
[3] Vt peatükk 2.4 Pilve teenusmudelid

nende tarbijatele. Töös ei vaadelda suurettevõtteid, sest nende IT on valdavalt hästi hallatud ning kompetents on ettevõttesiseselt olemas, riigiasutusi, sest neile kohalduvad piirangud teevad avaliku pilve teenuste kasutamise keeruliseks ega eraisikuid, sest eratarbimises pole vajadust ettevõtetele loodud lahenduste järele.

# 2. Pilveteenused

## 2.1 Mõiste

Pilveteenused on jätkuvalt arenev paradigma (AKI, 2012). Selle definitsioonid, kasutusjuhud, alustehnoloogiad, probleemid, riskid ja saadav kasu on alles välja kujunemas ja on aja jooksul muutumas. Pilvandmetöötluse sektor esindab suurt ökosüsteemi, milles on palju pilveteenuse vorme, teenusepakkujaid ja turunišše. Järgnev definitsioon on üks üritus hõlmata võimalikult palju lähenemisi: pilvandmetöötlus on teenusmudel, mis võimaldab mugava, kliendi vajadusest lähtuva võrguligipääsu ühisele seadistatavale arvutusressursile (nt võrgud, serverid, andmesalvestusruum, rakendused ja teenused), mis on kliendi poolt kiirelt rakendatav ja kasutussevõetav minimaalse haldusvajadusega ja/või minimaalse teenusepakkuja poolse sekkumisega. (Mell & Grance, 2010)

## 2.2 Põhilised tunnused

Mis puudutab pilveteenuste erinevust muudest IT teenustest, siis siinkohal kalduvad arvamused ühtima. Toon välja ISACA käsitluse (ISACA, 2011):

- Vajaduspõhine iseteenindus (*On-demand self-service*) - arvutiteenuseid nagu näiteks e-post, erinevad rakendusetarkvarad, võrk või serveri teenused saab kliendile kasutamiseks pakkuda ilma, et oleks vaja teenusepakkuja poolse inimese poolt sekkumist. Samuti saab klient ise määrata temale vajalikku arvutusvõimsust, kasutajate hulka või muid süsteemi parameetreid.

- Ressursside ühiskasutus (*Resource pooling*) - teenusepakkuja arvutiressursid on võimalik anda mitme samaaegse kasutaja käsutusse nii, et erinevaid füüsilisi ja virtuaalseid ressursse saab kasutaja oma nõudmisel dünaamiliselt määrata.

Sellised jagatavad ressursid on näiteks andmesalvestusruum, protsessorid, mälu, võrk, virtuaalmasinad, eposti teenused.

- Ligipääs üle arvutivõrgu (*Broad network access*) - teenuse võimalused on kättesaadavad üle võrgu ja ligipääsetavad läbi standardsete lahenduste, mida kasutavad erinevad võimalikud kliendiseadmed nagu näiteks mobiiltelefonid, sülearvutid ja tahvelarvutid.

- Teenuse elastsus (*Rapid elasticity*) - pilveteenuste ressursse saab igal ajal kiirelt ja elastselt ümber seadistada, vajadusel on võimalik seda teha lasta ka automaatselt ja seda mõlemas suunas - kas teenuse mahte ja kasutatavaid ressursse suurendades või vähendades.

- Teenuse mõõdetavus (*Measured service*) - pilveteenuse ressursikasutust saab mõõta ja kontrollida, mis annab võimaluse teenuse läbipaistvuseks nii teenuse pakkujale kui kliendile. See omakorda võimaldab mõlemapoolselt teenuse ressursikasutust optimeerida. Teenuse eest tasumine käib kasutamise arvestuse põhiselt.

- Ühiskasutamine *(Multi - tenancy*) - reeglistikupõhiselt, segmenteerimise, isoleerimise, halduse tulemusena ja teenustasemete ning erineva hinnastamise poolest saab sama keskkonda teineteisest sõltumatult kasutada hulk erinevaid kasutajaid.

## 2.3 Pilveteenuste paigaldusmudelid

Paigaldusmudel näitab ära pilveteenuse eesmärgi, kasutuse ja asukoha. NIST määratleb neli paigaldusmudelit (Sosinsky, 2011):

- Privaatpilv (*Private cloud*) - vajalik infrastruktuur (serverite riistvara) on täielikult seda omava ja kasutava ettevõtte hallatav, samas kui süsteemi haldajaks võib omava

organisatsiooni asemel olla ka kolmas osapool. Privaatpilved võivad paikneda nii omaniku oma valdustes või väljaspool (näiteks renditavates serveriruumides).

- Kogukonna pilv (*Community cloud*) - teenus on seatud täitma mingit üldist funktsiooni või eesmärki. Võib kuuluda nii ühele kui mitmele organisatsioonile, kellel on samad huvid kas missiooni, reeglite, turvanõuete, vastavusnõuete vms osas. Haldajaks üks või mitu osapooltest, või väline kolmas osapool.

- Avalik pilv (*Public cloud*) - on avalikuks kasutamiseks kõigile soovijatele ja kuulub pilveteenust pakkuvale ettevõttele.

- Hübriidpilv (*Hybrid cloud*) - kombineerib omavahel erinevaid pilveteenuste tüüpe (privaatne, avalik, kogukondlik), kus nimetatud teenustele jäävad nende unikaalsed intentiteedid, kuid need on omavahel koos tööle seatud. Hübriidpilv võib pakkuda standardiseeritud või eriligipääsu andmetele ja rakendustele.

## 2.4 Pilve teenusmudelid

Seoses pilveteenuste arenguga on tekkinud mitmeid lühendeid, mille ühine nimetaja inglise keeles on *XaaS - X as a Service* ehk "*anything as a service*". Nimetatud lühend viitab kasvavale arvule teenustele, mida on võimalik üle interneti klientideni tuua. Mõnede vähemlevinud näidetena nimetaks *Storage as a Service - Saas* ehk salvestusruum teenusena, *Network as a Service - NaaS* ehk võrk teenusena või *Communications as a Service - CaaS* ehk kommunikatsioonivahendid teenusena jne. Tuntumad on siiski praegu kõige enam levinud kolm teenusmudelit (Sosinsky, 2011):

- Tarkvara teenusena (*Software as a Service - SaaS*) - kasutusvalmis rakendustetarkvara töökeskkond koos vastavate haldusvahenditega. Klient kasutab rakendusi valdavalt läbi veebibrauseri ning tema vastutus algab ja lõpeb andmete sisestamise ja nende haldamisega. Kõik mis jääb rakenduse kihist allapoole (riistvara ja sellel töötavad haldussüsteemid) on teenusepakkuja vastutusalas.

- Platvorm teenusena (*Platform as a Service - PaaS*) - platvormina pakutakse virtuaalmasinaid, operatsioonisüsteeme, rakendusi, teenuseid, arenduskeskkondi ja nende haldusvahendeid. Klient saab paigaldada omapoolsed rakendused pakutavale taristule või kasutada rakendusi ja töövahendeid, mis on *PaaS* keskkonda teenusepakkuja poolt eelnevalt juba paigaldatud. Teenusepakkuja tagab teenuse taristu, operatsioonisüsteemid ja vajalikud töökeskkonnad. Klient on vastutav endale vajalike rakenduste paigaldamise ja nende haldamise eest.

- Taristu teenusena (*Infrastructure as a Service - IaaS*) - teenusena pakutakse virtuaalmasinaid (servereid), virtuaalset andmesalvestusruumi, virtuaalset võrku, virtuaalset riistvara ja muid elemente, mida klient peab vajalikuks hallata. Teenusepakkuja haldab füüsilist taristut samas kui kliendi vastutusel on kõik muud süsteemihalduse aspektid: täielikult hallatavad operatsioonisüsteemid, serveril kasutatavad teenused ja rakendused, detailsed pääsuhaldused jms.

## 2.5 Pilveteenustega seotud põhilised riskid

Käesolevas töös käsitletakse pilveteenuste kasutamisega kaasnevaid riske järgneva mõiste sõnastusena: risk on mingi sündmuse või juhtumi esinemine, mis on seotud pilveteenuste kasutuselevõtuga või kasutamisega, millel on ebasoovitavad tagajärjed või mõjud kasutajale (Dutta, Choudhary, & Peng, 2013).

Avaliku pilve teenustega kaasneb rida spetsiifilisi probleeme, mida ettevõttesiseselt majutatavate ja kasutatavate IT lahendustega ei esine. Teisest küljest annavad pilveteenused eeliseid (Newson, 2015), mida ettevõttesisesel IT'l ei ole, mistõttu on mõlemal IT kasutusviisil omad eelised ja loomupärased vead. Samas on osa probleeme ka sarnased ja eksisteerivad nii teenusepakkuja kui IT siselahenduse korral. Erinevate osapoolte, nagu uuringufirmad ja tehnoloogiaettevõtted, arutelu all on ka küsimus, kas pilveteenused võivad olla ehk isegi turvalisemad kui majasisesed lahendused (Gartner, 2014; Aberdeen Group, 2011).

Ühe probleemina nähakse ka, et mitte kõik pilveteenuste pakkujad ei ole turvalisuse küsimustes eksperdid, teisalt ei ole turvalisus, hoolduskindlus ega käideldavus alati garanteeritud ka majasiseste lahenduste puhul (European Commission Directorate-General for Justice and Consumers, 2012).

ENISA on oma uurimuses (ENISA, 2012) välja toonud pilveteenuste põhilised riskid. Riskide hindamisel on lähtutud ISO/IEC 27005:2008 standardist.

| | Likelihood of incident scenario | Very Low (Very Unlikely) | Low (Unlikely) | Medium (Possible) | High (Likely) | Very High (Frequent) |
|---|---|---|---|---|---|---|
| Business Impact | Very Low | 0 | 1 | 2 | 3 | 4 |
| | Low | 1 | 2 | 3 | 4 | 5 |
| | Medium | 2 | 3 | 4 | 5 | 6 |
| | High | 3 | 4 | 5 | 6 | 7 |
| | Very High | 4 | 5 | 6 | 7 | 8 |

**Joonis 1: riskide hindamisskaala**

Madal risk: 0 - 2
Keskmine risk: 3 - 5
Kõrge risk: 6 - 8

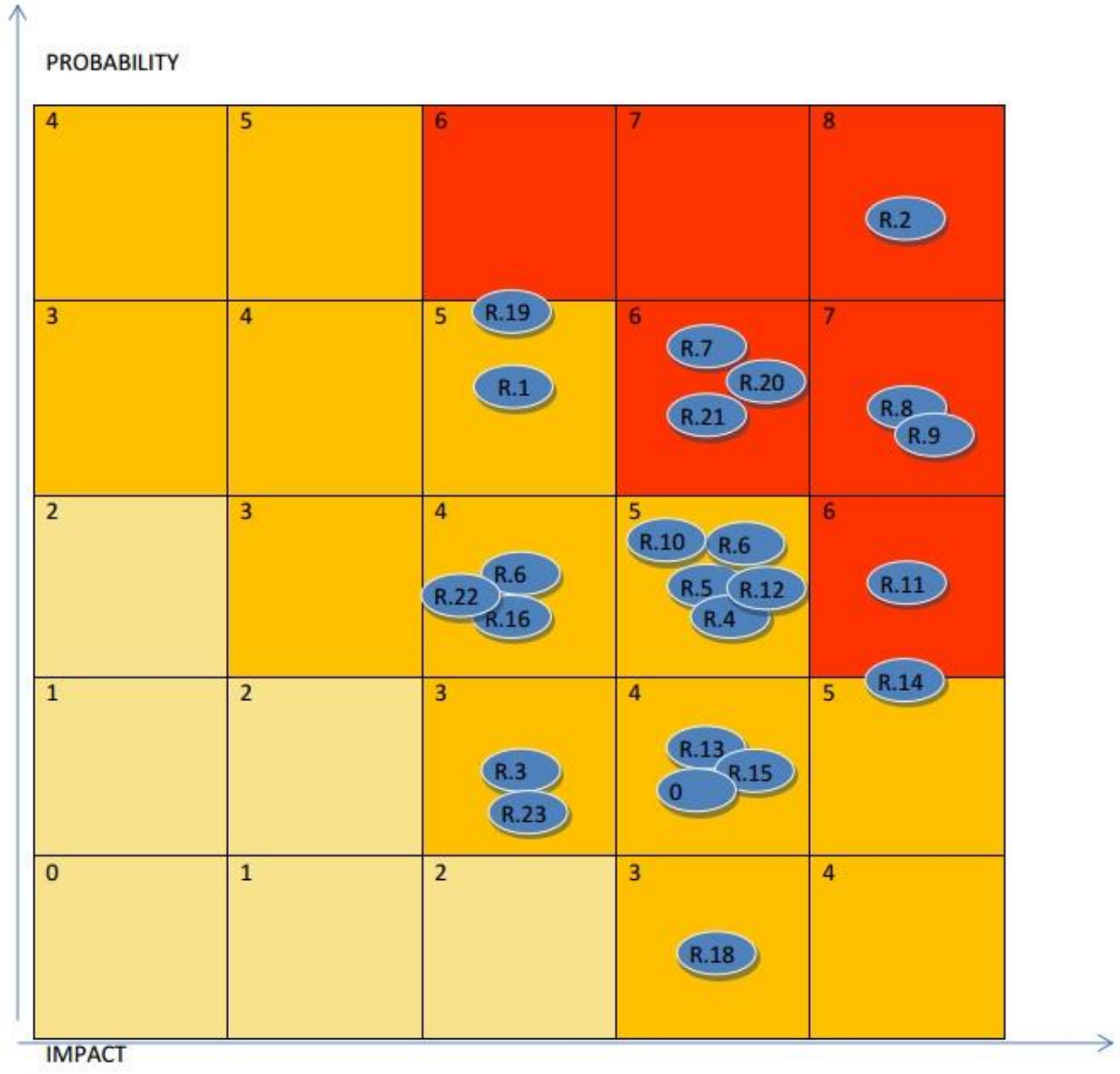
*Business Impact* - mõju ettevõttele

Mõju on kasvav suunal ülevalt alla (väga madal, madal, keskmine, kõrge, väga kõrge).

*Likelihood of incident scenario* - riski realiseerumise tõenäosus

Tõenäosus on kasvav suunal vasakult paremale (väga madal, madal, keskmine, kõrge, väga kõrge).

Riskide hindamiskaala põhjal moodustati tabel, kus on ära näidatud riskide tõenäosuse ja mõju jagunemine:




**Joonis 2: riskide jagunemine**

X- telg, *impact* - mõju

Y- telg, *probability* - tõenäosus

Tabelisse kantud riskid on omakorda jagatud kolme kategooriasse:

Regulatoorsed ja organisatoorsed (*Policy and organizational*)

Tehnilised (*Technical*)

Õiguslikud (*Legal*)

### 2.5.1 Regulatoorsed ja organisatoorsed

R.1 - tootjalõks (*lock-in*):
tõenäosus: kõrge; mõju: mõõdukas; risk: kõrge

Pilveteenused põhinevad tihti mittestandardsetel andmeformaatidel ning rakenduste loogikal, mis võib andmete ülekandmise ühe teenusepakkuja juurest teise juurde teha keeruliseks või isegi võimatuks. Samas ei ole analoogne probleem välistatud ka klassikaliste - ettevõttesiseste IT lahenduste puhul.

Võimalik lahendus: väljumisstrateegia enne teenusega sidumist.

R.2 - halduskontrolli kadumine (*loss of governance*):
tõenäosus: väga kõrge; mõju: väga kõrge; risk: väga kõrge

Pilveteenuseid kasutades loovutab klient teenusepakkuja kätte kontrolli mitmete asjaolude üle, mis võivad mõjutada turvalisust. Näiteks teenusepakkuja kasutustingimustes võib olla keeld teha teenusele portide skaneerimist, teenuse haavatavuse hindamist ja sissetungiteste, mis võib omakorda tekitada olukorra, kus klient ei saa oma andmete turvalisust hinnata. Samas on analoogne probleem võimalik ka majasisese lahenduse puhul, kus nt andmesideteenuse pakkuja seab oma teenuse kasutamisele piiranguid.

Võimalik lahendus: teenusepakkuja turbe- ja vastavussertifikaatide kontroll ja olemasolu.

R.3 - varustusprobleemid (*suppy chain failure*):
tõenäosus: madal; mõju: keskmine; risk: keskmine

Teenusepakkuja ei ole piisava põhjalikkusega valmistunud riistvarariketeks või olulise kasutatava teenuse (nt *single-sign-on*) rikkeks, mis võib omakorda mõjutada kas üht või järjestikust hulka pakutavaid teenuseid. Sarnane olukord võib siiski tekkida majasisese IT lahenduse puhul.

Võimalik lahendus: teenuse läbipaistvus ja kasutustingimused: nõuda teenusepakkujalt ülevaadet, millistest välistest teenustest sõltutakse.

R.4 - klient ei täida teenusepakkuja poolseid turvanõudeid (*conflicts between customer hardening procedures and cloud environment*):
tõenäosus: keskmine; mõju: keskmine; risk: keskmine

Kui teenusepakkuja ei kirjelda, mida klient minimaalselt enda poolt kasutatava teenuse kaitsmiseks tegema peab, või klient ei tee nõutud tegevusi, võib tagajärjeks olla teenuse haavatavus. Eriti juhtudel, kui teenusepakkuja ei ole piisavalt põhjalikult klientide keskkondi isoleerinud. Analoogne risk tava IT puhul puudub.

Võimalik lahendus: klient peab mõistma endale pandud kohustusi oma kasutatavat teenust ja selles sisalduvaid andmeid kaitsta, teenusepakkuja peab omalt poolt põhjalikult selgitama teenusega kaasnevaid võimalikke nõudeid ja pakutavat tehnilist võimekust.

R.5 - andmete *õngitsemine* (*social engineering*):
tõenäosus: keskmine; mõju: kõrge; risk: keskmine

Eesmärk on info kogumine, inimeste manipuleerimine konfidentsiaalsete andmete avaldamiseks või mingite tegevuste sooritamiseks arvutisüsteemidele ligipääsuks ilma ohvri teadmata. Oht eksisteerib ka majasiseste IT lahenduste puhul.

Võimalik lahendus: kliendi töötajate teadlikuse tõstmine.

### 2.5.2 Tehnilised

R.6 - ressursside ammendumine (*resource exhaustion*):
tõenäosus: madal; mõju: kõrge; risk: keskmine

Et pilveteenused on nõudmisepõhised, siis on võimalus, et teenusepakkuja ei ole võimeline pakkuma kliendi poolt soovitud suuremat hulka mingit ühist ressurssi või ei suuda määratud taset hoida, mis võib põhjustada teenuse kättesaadamatust. Ressursi ammendumine on võimalik ka tava IT puhul, kuid pilveteenustel on korraliku ressursihalduse korral risk väiksem.

Võimalik lahendus: põhjalik teenusepakkuja valik.

R.7 - isolatsiooni katkemine (*isolation failure*):
tõenäosus: kõrge; mõju: kõrge; risk: kõrge

Ühiskasutatavate keskkondade puhul pole võimatu, et süsteemivigade või sihilike rünnakute tõttu pääseb üks teenusekasutaja (või ründaja) ligi teise kasutaja ressurssidele või andmetele. Sarnaseid lekkeid võib esineda ka tava IT's, kuid jagatud avaliku ühisressursi puhul on risk tõsisteks tagajärgedeks suurem.

Võimalik lahendus: põhjalik teenusepakkuja valik.

R.8 - teenusepakkuja poolne pahatahtlik tegevus (*cloud provider malicious insider*):
tõenäosus: keskmine; mõju: väga kõrge; risk: kõrge

Teenusepakkuja poolse töötaja pahatahtlik priviligeeritud õigustega ligipääs kliendi ressurssidele ja andmetele. Sarnane stsenaarium on võimalik ka tava IT puhul, kuid teenusepakkujate puhul on võimalike isikute ring ning nende huvid teadmata, samuti on teenusepakkujal rohkem võimalusi ning hallatava huvipakkuva info hulk suurem.

Võimalik lahendus: oma kasutatava teenuse põhjalik jälgimine ning teenusepakkuja tausta kontroll.

R.9 - haldusvahendite kompromiteerimine (*management interface compromise*):
tõenäosus: keskmine; mõju: väga kõrge; risk: kõrge

Avaliku pilveteenuse puhul on haldusvahendid interneti kaudu ligipääsetavad, mis tähendavad riski soovimatute ligipääsukatsete näol. Täiendav oht on kaugligipääsu vahendite (*remote access*) ja veebilehitsejate vigade ärakasutamine. Taoline oht on väiksem majasiseste lahenduste puhul.

Võimalik lahendus: hoolikas ligipääsuandmete ja -meetmete haldus.

R.10 - andmevahetuse pealtkuulamine (*intercepting data in transit*):
tõenäosus: keskmine; mõju: kõrge; risk: keskmine

Avaliku pilveteenuse ja kliendi vahelise andmevahetuse puhul on tõenäosus andmeside pealtkuulamiseks suurem kui majasiseste lahenduste puhul, kuid ka tava IT puhul pole see välistatud. Mõju on mõlemal juhul sama.

Võimalik lahendus: turvalised andmesidelahendused, teenusepakkuja poolsete turvalahendustega tutvumine ja nende rakendamine.

R.11 - ebaturvaline või ebapiisav andmete kustutamine (*insecure or ineffective deletion of data*):
tõenäosus: keskmine; mõju väga kõrge; risk: kõrge

Krüpteerimata andmete puhul on oht, et näiteks salvestusruumi mahu muutmisel suuremast väiksemaks või teenusepakkuja vahetamise korral, avalduvad kustutamata andmed kas teistele teenuse kasutajatele või teenusepakkujale. Ohu ilmnemise võimalus on suurem kui tava IT puhul.

Võimalik lahendus: andmete krüpteerimine, andmete hoolikas haldus ja töötlemine.

R.12 - DDos rünne (*distributed denial of service*):
tõenäosus: keskmine; mõju: kõrge; risk: keskmine

Ründe eesmärgiks on teenusepakkuja ülekoormamine, nii et klientidel on oma teenuseni jõudmine raskendatud. Tõenäosus, et taolist rünnet tehakse teenusepakkuja ühe kliendi vastu on väiksem, kui üksiku kliendi ettevõttesisese IT lahenduse vastu. Enamasti on pilveteenuste pakkujatel rohkem võimalusi ja ressursse taolise ründega toime tulla kui üksikettevõttel.

Võimalik lahendus: teenusepakkujaga suhtlemine varasemate juhtumite ja vastumeetmete osas.

R.13 - EDoS rünne (*economic denial of service*):
tõenäosus: madal; mõju: kõrge; risk: keskmine

Lähtuvalt asjaolust, et pilveteenuste puhul mõõdetakse erinevat ressursikasutust sh näiteks andmesidet ning süsteemi parameetreid ja neid saab koormuse tõustes lasta automaatselt suurendada, on halva teenuse halduse või rahaliste vahendite piiramise võimatuse tõttu võimalik põhjustada kliendi suurenenud rahalisi väljaminekuid, mis võib omakorda kliendi jaoks finantsressursside lõppedes teenuse peatada.

Võimalik lahendus: teenuse korrektne haldus, teenuse kulude jälgimine.

R.14 - teenuse mootori kompromiteerimine (*compromise of service engine*):
tõenäosus: madal; mõju: väga kõrge; risk: kõrge

Teenuse mootori (nt hüperviisori) edukas rünne võib ründajatele anda ligipääsu kõigi klientide andmetele, mis omakorda võib tähendada andmete kadu ja klientide ligipääsu takistamist. Tava IT puhul sellist riski ei eksisteeri.

Võimalik lahendus: teenusepakkuja peab klientidele andma selged miinimumnõuded, kuidas oma teenust kaitsta ning kliendi kohustus on neid täita.

R.15 - krüpteerimisvõtmete kaotus (*loss of cryptographic keys*):
tõenäosus: madal; mõju: kõrge; risk: keskmine

Näiteks krüpteerimise või autentimise krüptovõtmete kaotamine võib põhjustada vastavalt kas andmete kaotust või teenusele mitte ligipääsemist. Risk eksisteerib ka tava IT's, kuid et pilveteenustes kasutatakse krüpteerimist rohkem, on ka oht intsidentideks suurem.

Võimalik lahendus: korrektne süsteemihaldus.

R.16 - pilveteenusest olenematud võrguprobleemid (*Non Cloud-Specific Network-Related Technical Failures or Attacks*):
tõenäosus: keskmine; mõju: keskmine; risk: keskmine

Võrguprobleemid, mis võivad ilmneda ka majasiseste IT lahenduste puhul, ründed andmesidevõrgule, võrguoperaatori ühenduse probleemid, pilveteenuse pakkuja võrguoperaatori võrguprobleemid.

Võimalik lahendus: võimalikult probleemivaba võrguühendus, varuühendused.

R.17 - varundatud andmete kaotus (*loss of backups*):
tõenäosus: madal; mõju: kõrge; risk: keskmine

Teenusepakkuja tehtud andmevarundus kliendi andmetest läheb kaduma, kaotab terviklikkuse või füüsilise andmekandja puhul varastatakse. Mõju on samane kui tava IT lahendusega, selle vahega, et teenusepakkujatest oodatakse paremaid tehnilisi lahendusi ja võimalusi kui klientidel on.

Võimalik lahendus: täiendav andmevarundussüsteemi loomine.

R.18 - loodusõnnetused (*natural disasters*):
tõenäosus: väga madal; mõju: kõrge; risk: keskmine

Loodusõnnetuste (uputused, maavärinad jne) mõju teenusepakkuja tegevusele, mis võib mõju avaldada ka õnnetuskohast kaugel asuvale kliendile. Enamasti on teenusepakkujate taristulahendused piisava liiasusega, et teenus saaks jätkuda, olles seega töökindlam kui paljude klientide tavalahendused. Samas, mõju esilepääsu korral, võib teenuste taastamiseks aega kauem minna, kui kliendil enda üksiklahenduse puhul.

Võimalik lahendus: tutvumine teenusepakkuja geograafilise asukohaga.

### 2.5.3 Õiguslikud

R.19 - kohtuasjad ja juurdlused (*subpoena and e-discovery*):
tõenäosus: kõrge; mõju: keskmine; risk: kõrge

Õiguskaitseorganite tegevuse tõttu (kriminaaluurimised, tsiviilkohtuasjad) on võimalik, et teenusepakkuja andmesalvestusseadmed või muu riistvara arestitakse või konfiskeeritakse kui asitõend. See tähendab samas ka teiste samu ressursse kasutanud klientide töö peatamist, mis teeb riski realiseerumise tõenäolisemaks kui ettevõttesiseste IT lahenduste puhul, kuigi mõju on sama. Samas on tõenäosus, et üksiku riigi õiguskaitseorganid konfiskeerivad pilveteenuse, üsnagi küsitav.

Võimalik lahendus: andmete varundamine, teenuste taasteplaanid.

R.20 - õigusalluvuse risk (*risk from changes of jurisdiction*):
tõenäosus: kõrge; mõju: kõrge; risk: kõrge

Kui kliendi andmeid hoitakse või töödeldakse mõnes muus riigis, mitte kliendi asukohamaal, võib esineda olukordi kus: andmed arestitakse või teenused katkestatakse põhjustel, milliseid kliendi asukohariigis ei eksisteeri; andmete arestimist põhjendatakse teenuse asukohamaa rahvuslikule julgeolekule viidates; teenusepakkuja vastu suunatud rahvusliku julgeoleku või muude õiguslike põhjendustega ja tegevustega võib mõju ulatuda kaugemale kui ettevõtte peakontori asukohamaa, hõlmates ka muudes riikides asuvad andmekeskusi.

Risk on kõrge põhjusel, et teenusepakkujaid on palju, erinevates riikides ning kõigile kohalduvad erinevad õigused ja seadused.

Võimalik lahendus: teenusepakkuja tingimustega põhjalik tutvumine, andmekeskuste paiknemise kontroll.

R.21 - andmekaitse riskid (*data protection risks*):
tõenäosus: kõrge; mõju: kõrge; risk: kõrge

Andmete kaitse õiguslikud asjaolud võivad muutuda kui teenusepakkuja muudab kliendi teadmata tema andmete asukohta mõne teise, erineva õigusliku korraga riigi andmekeskusesse. Pilveteenuste puhul on selline risk kõrgem kui tava IT's, sest teenusepakkujal on täielik kontroll andmete paiknemise üle.

Võimalik lahendus: teenusepakkuja tausta kontroll, andmekeskuste asukohtade väljaselgitamine, andmekaitsesertifikaatide olemasolu.

R.22 - litsenseerimisprobleemid (*licensing issue*):
tõenäosus: keskmine; mõju: keskmine; risk: keskmine

Kasutatava tarkvara kasutamine, ilma et see vastaks tarkvaralitsentsi tingimustele. Paljude tarkvaralahenduste puhul ei ole veel nende pilveteenustes kasutamist tingimustes sätestatud, mistõttu võib klient riskida trahvidega või maksta rohkem, kui tegelikult põhjust oleks. Sarnane oht on ka tava IT's ning ka mõju on sama.

Võimalik lahendus: kasutatava tarkvara litsentsitingimustes veendumine.

R.23 - intellektuaalomandi probleemid (*intellectual property issues*):
tõenäosus: madal; mõju: keskmine; risk: keskmine

Kasutades teenusepakkuja spetsiifilist tarkvara või teenuse keskkonda, on võimalus, et luuakse originaalloomingut (nt uued tarkvaralahendused), mis on seotud teenusepakkuja konkreetse keskkonnaga. Juhul kui taoline intellektuaalomand ei ole teenusepakkuja ja -kasutaja vahelises lepingus või kokkulepetes kaetud, kätkeb loodav originaallooming omandiriski. Selline olukord võib juhtuda ka tava IT lahenduste puhul, kuid pilveteenuste puhul on riski avaldumise oht suurem.

Võimalik lahendus: klient viib end teenusepakkuja tingimustega kurssi ning vajadusel ja võimalusel lepib teenusepakkujaga võimalikes lisatingimustes kokku.

## 2.6 Teenusepakkujate poolsed teenuse tagamise meetmed

Nagu nähtus enamlevinud riskide loetelust, on pilveteenustel nõrku kohti, millele tähelepanu pöörata, piisavalt. Siiski võib tõdeda, et kuigi osad riskid on teenusele omaselt unikaalsed, siis on mitmeid riske, mis võivad analoogselt avalduda ka majasiseste IT lahenduste puhul. Autori hinnangul on üle poolte loetletud riskide puhul võimalik probleeme ennetada põhjaliku teenusepakkuja tingimuste, tausta, maine, lahenduste jms eelneva kontrolliga ja enda vajaduste ning võimaluste parema hindamisega. Sellest lähtuvalt on teenusepakkuja valikul lisaks funktsionaalsusele ja hinnafaktoritele oluline teenuse tunnustatud kvaliteet ja läbipaistvus. Nimetatud riskide lahendusi on esmasel tutvumisel teenusepakkujate võrdluses keeruline vaadelda, seda enam, et teenusepakkujad ei soostu oma sisulisi probleeme avalikkusele ja seeläbi klientidele vabatahtlikult tunnistama. Samuti on keeruline saada ammendavaid selgitusi juba juhtunud intsidentide kohta, sest positiivse mainekujunduse ja klientide hoidmise huvides on mõistlikum juhtumeid ilustada või võimalusel varjata. Samuti ei ole mõistlik konkurentidele oma ettevõttega seotud detailide avaldamine. Veel üks põhjus, miks teenusepakkuja tausta, tehnoloogilise ning organisatoorse võimekuse väljaselgitamine on oluline, on asjaolu, et eksisteerib pakkujaid, kellel ainus seos pilveteenusega on vaid lubav tekst teenuse kirjelduses või nimetus "pilveteenus" teenusele viitaval veebiaadressil. Puudub sisuline pilveteenus. Raske on pilveteenuseks nimetada teenuseid, millel puuduvad vastavad tunnused alates täielikust iseteenindusest ning teenuse käivitamine vajab kliendihalduri poole pöördumist, oluliste kasutustingimuste leidmine nende lugemiseks on vaevaline või teenuse reaalse maksumuse väljaselgitamiseks tuleb end kasutajaks registreerida.

Et leida väga paljude teenusepakkujate seast kvaliteetsemaid ja riskide maandamisega tegelevaid teenuseid, on üheks võimaluseks võrrelda teenusepakkujatele sõltumatute osapoolte poolt omistatud vastavustunnistusi (*compliance standard*) ja sertifikaate. Ühest küljest ei garanteeri nende olemasolu küll teenuse katkemist, kuid võrdluses teenusepakkujatega, kellel pole ette näidata sisulisi tagatisi peale veebilehel turunduslikul

eesmärgil välja toodud 100% töökindlusega, annab tunnustuse omamine suurema kindluse, et teenusepakkuja on ka sisuliselt tegelenud oma teenuse turvalisusega, nende protsessid on läbi mõeldud, käideldavus on tagatud ja seda ka sõltumatu hindaja arvamuse kohaselt. Muidugi eksisteerib võimalus, et teenusepakkujad on olulised tunnistused küll omandanud, ent need on kodulehel välja toomata jäänud. Lähtudes asjaolust, et pilveteenuse pakkujaid on palju ning tunnistuste olemasolu annab konkurentsieelise, siis ei näe autor põhjust, miks peaks sellist väga olulist infot võimalike klientide eest varjama.

Alljärgnevalt on välja toodud loetelu enamlevinud regulatsioonidest, sertifikaatidest ja kompetentsidest, mille olemasolu USA ja Euroopa Liidu pilveteenuse pakkuja valikul tähele tasub panna.

COBIT[4]

ISACA (*IT Governance Institute and the Information Systems Audit and Control Association*) poolt välja töötatud COBIT (*Control Objectives for Information and Related Technology*) on raamistik arendamaks, rakendamaks, monitoorimaks ja parendamaks IT haldust ja halduspraktikaid. Kuigi algne versioon keskendus auditeerimisele, siis uuem versioon sisaldab ka ettevõtete riskihaldust.

ITIL[5] (Information Technology Infrastructure Library)

ITIL on IT teenuste halduse (*IT Service Management* - ITSM) praktikate kogum, mis keskendub IT teenuste vastavusseviimisele vastavalt ärivajadustele. ITIL kirjeldab protsesse, protsetuure ja tegevusi, mida teenusepakkuja saab kasutada, et luua IT integratsiooni ettevõtte strateegiaga. Võimaldab ettevõttel defineerida alustingimused, millelt edasisi tegevusi planeerida, rakendada ja mõõta. ITIL'it saab kasutada, et demonstreerida IT vastavust nõuetele, mõõta arengut.

[4] http://www.isaca.org/cobit
[5] https://www.axelos.com

ISO 2700x[6]

ISO/IEC 27000-seeria (samuti tuntud kui 'ISMS standardite kogu' või lühendina 'ISO27k') hõlmab endas infoturbe standardeid, mis on ühiselt välja antud ISO (*International Organization for Standardization*) ja IEC (*International Electrotechnical Commission*) poolt.

Nimetatud seeria pakub parimate praktikate soovitusi infoturbe ja riskide halduseks lähtudes üldisest ISMS (*Information Security Management System*) kontekstist. Olles oma skoobilt üsna lai, on kaetud rohkem kui vaid privaatsuse, konfidentsiaalsuse ja IT või tehnilise turbe küsimused ja on kohalduv erinevate suuruste ja eesmärkidega ettevõtetele. Tegevus näeb ette infoturbe riskide hindamist ja seejärel vastavalt vajadusele vastavate infoturbemeetmete rakendamist. Infoturbe loomusest lähtuvalt toimub pidev tagasiside ja parandustegevus lähtudes planeeri-teosta-kontrolli-tegutse (*Plan-Do-Check-Act* ehk PDCA) mudeli põhimõttest.

CSA CCM[7]

CSA CCM (*Cloud Security Alliance Cloud Controls Matrix*) on spetsiaalselt välja töötatud pakkumaks pilveteenuste pakkujatele põhilisi andmeturbe põhimõtteid ja aidata võimalikel klientidel hinnata üldist teenusepakkuja riskitaset. CSA CCM põhineb teistel valdkonnas tunnustatud turvastandarditel, regulatsioonidel ja raamistikel nagu näiteks ISO 270001/27002, ISACA COBIT, PCI jt. CSA CCM tugevdab olemasolevat andmeturbekeskkonda rõhutades ettevõtete andmeturbekontrolli nõudeid, vähendab ja identifitseerib sagedasemad turbeohud ja haavatavused, pakub standardiseeritud turbe- ja tegutsemisriskide haldust.

Raamistik pakub kolme erinevat taset, kus iga järgev tase tähendab turbe lisakihti. Teenusepakkujatel on võimalik enda olukorda raamistikule kohaselt nii ise hinnata, kui lasta end hinnata kolmandate osapoolte poolt.

[6] http://www.iso.org
[7] https://cloudsecurityalliance.org

ECSA (EuroCloud Star Audit)[8]

*EuroCloud Europe* (ECE) eesärk on kergendada Euroopa teenuste usaldusväärsust rahvusvahelisel turul. ECE teeb pidevat koostööd oma partnerite võrgustikuga ning ka valitsusasutustega. Pakutakse ECSA (*EuroCloud Star Audit*) nimelist sertifitseerimisskeemi, mille eesmärgiks on teenusepakkujate ja klientide vahelise usalduse loomine. Sertifikaat on välja töötatud konkreetselt pilveteenuste hindamiseks.

EuroPriSe[9]

EuroPriSe (*European Privacy Seal*) on Euroopa IT toodete ja IT-põhiste teenuste privaatsussertifikaat, mis vastab Euroopa Liidu andmekaitseregulatsioonidele. Sertifikaat on omakorda jagatud nelja ossa: üldvastavus; andmete käitlemise õigusjärgsus; tehnilised - organisatoorsed vastavused; andmeomanike õigused.

AICPA SOC[10]

SOC (*Service Organization Control Reports*) on välja töötatud AICPA (*American Institute of Certified Public Accountants*) poolt olles raamistikuks, mille järgi teenusepakkujad saavad tõestada oma vastavust ette nähtud infoturbe, andmete töötlemiskindluse, konfidentsiaalsuse, kättesaadavuse ja privaatsuse nõuetele.

Eristatakse tasemeid SOC1, SOC2, SOC3. Kui SOC 1 on mõeldud peamiselt finantskontrolliks, siis SOC 2 & 3 keskenduvad eeldefineeritud ja standardiseeritud mõõdikutele, mis kontrollivad andmekeskuste ja seal olevate andmete turvalisust, andmete terviklikkust ja konfidentsiaalsust.

[8] https://eurocloud-staraudit.eu
[9] https://www.european-privacy-seal.eu
[10] http://www.aicpa.org

SSAE 16[11] / ISAE 3402[12]

Varasema rakendusnimega SAS70, mida veel kohata võib, on SSAE 16 (*Standards for Attestation Engagement No. 16* ) ja ISAE 3402 (*International Standard on Assurance Engagements No. 3402*) teenusestandardid, mis on üsna sarnased ning vaadeldakse seetõttu tavaliselt koos. Kui SSAE on lähtuv Ameerika Ühendriikide nõuetest, siis ISAE on rahvusvaheline. Standard lähtub nõuetest hoida finantsandmeid käsitlevad andmekeskused teataval füüsilise turbe ja käitluskeskkonna tasemel.

Tier Certification [13]

Tier 1 kuni 4 on standardiseeritud meetod defineerimaks andmekeskuste talitluspidevust ja kättesaadavust, mis katab nii tehnoloogilisi kui organisatoorseid hindamiskriteeriume.

Tier 1 = liiasuseta komponendid (*non-redundant*), näiteks üks andmesidekanal ning serverid.

Tier 2 = Tier 1 + liiasusega komponendid.

Tier 3 = Tier 1 + Tier 2 + topelttoitega seadmed ja mitmed andmesideühendused.

Tier 4 = Tier 1 + Tier 2 + Tier 3 + kõik komponendid on täielikult veakindlad, sh sideühendused, andmesalvestid, jahutussüsteemid, serverid jne. Kõik on varutoitega.

Tier 1: tagab 99.671% teenuste saadavaloleku.

Tier 2: tagab 99.741% teenuste saadavaloleku.

Tier 3: tagab 99.982% teenuste saadavaloleku.

Tier 4: tagab 99.995% teenuste saadavaloleku.

[11] http://www.ssae16.org
[12] http://isae3402.com
[13] https://uptimeinstitute.com

PCI DSS[14]

PCI DSS (*PCI Data Security Standards*) on tehniliste ja opereerimisnõuete kogu, mille eesmärgiks on kaitsta maksekaartide ja kaardiomanike andmeid. Seda andmete hoiustamise, käitlemise, ülekannete osas.

Safe Harbor / EU Directive 95/46/EC[15]

Safe Harbor on sertifitseerimisprogramm, mille eesmärk on tagada andmekaitse vastavalt Euroopa Liidu andmekaitsenõuetele. Levinud peamiselt Ameerika Ühendriikide teenusepakkujate seas, kes soovivad osa saada Euroopa Liidu kasutajateturust.

HIPAA[16]

HIPAA (*Health Insurance Portability and Accountability Act*), määrab standardid kaitsmaks terviseasutustes patsientide kohta käivat tundlikku infot. Kontrollib, et IT taristu, võrgu ja protseduuride kontroll on rakendatud ja hiljem ka järgitud. Tegemist on Ameerika Ühendriikide standardiga, ent sellise sertifikaadi olemasolu on kasulik teada, kui valida teenusepakkujaid ka USAst.

FedRAMP[17]

Sarnaselt eelmisele USA põhine, kuid taaskord hea teada. USA riiklik riski ja isikutuvastuse halduspprogramm.

FedRAMP (*Federal Risk and Authorization Management Program*), standardlahendus turbe hindamiseks, volituste haldamiseks ning pilveteenuste ja - toodete monitooring.

[14] https://www.pcisecuritystandards.org
[15] http://www.export.gov/safeharbor/
[16] http://www.hhs.gov/ocr/privacy/
[17] http://www.fedramp.gov

Nimekiri pole kaugeltki täielik, sest pilveteenuste standardiseerimisel ei ole universaalse lahenduseni veel jõutud. On veel muude riikide ühisregulatsioone (nt Aasia riikides), siseriiklikke (enamus Euroopa riike loovad oma reeglistikke, Eesti puhul ISKE). Väiksema levikuga, tootjapõhiseid (nt IBM, HP), kindla suunitlusega (nt riigiasutustele) ja muud tüüpi (nt TRUSTe, mis väljastab erinevatele koondnõuetele vastavaid "turvakleebiseid") sertifikaate, mis on olulised teatud konkreetsetes tingimustes ja turuolukorras jne.

# 3. Teenusepakkujate riskimaandusmeetmete ja kasutatavate standardite uuring

Uuringu eesmärk on vaadelda hulga pilveteenuste pakkujate (asukohaga Eestis, Euroopa Liidus ja USA's) (King & Raja, 2013) teenuste kirjeldusi nende kodulehtedel kui esmasel infoallikal, hindamaks nende poolt rakendatud ja/või neile omistatud vastavussertifikaate ja tunnistusi ehk püütakse mõista teenusepakkuja tunnustatud kvaliteeditaset. Lähtutakse tavakasutaja võimalustest tutvuda vabalt ligipääsetava infoga, täiendavaid küsimusi teenusepakkujatele ei esitata, infole ligipääsemiseks kasutajaks ei registreeruta. Uuring on kvalitatiivne, ehk vaadeldakse teenusepakkujate kodulehti kui objekte hindamaks neil teatud tunnuste esinemist, esitatava info leitavust ja arusaadavust. Vaatluse käigus ei võrrelda pakutavate teenuste funktionaalsust ega hindu, küll aga jälgitakse, kas teenusepakkuja on oma teenuseid tutvustades eksitav ehk pakutav sisuline teenus ei lähe kokku pilveteenuse tunnustega.

Uuring viidi läbi perioodil 01.04 - 01.05.2015, iga teenusepakkuja puhul kulutatati info otsimiseks aega maksimaalselt 20 minutit, mis on piisav, et tavakasutaja leiaks vajamineva informatsiooni, saaks veenduda selle raskelt leitavuses, mitteolemasolus või kaotada huvi teenusepakkuja vastu. Töövahendiks on tavaline internetilehitseja Mozilla Firefox 37.0.1

Teenusepakkujate tutvustustest otsiti järgmisi tunnuseid:

ISO/IEC 2700x

SSAE 16 / ISAE 3402

PCI DSS

Safe Harbor / EU Directive 95/46/EC

EuroCloud Star Audit (ECSA) või EuroPriSe

SLA (*Service Level Agreement*) ehk teenustase

Pilveteenuste üldtunnused (vajaduspõhine iseteenindus, ressursside ühiskasutus, teenuse elastsus, teenuse mõõdetavus).

Kuigi võib väita, et nt Eesti teenusepakkujate puhul polegi mõistlik või puudub vajadus nt USA põhiste standardite ja sertifikaatide järele, on töö ja uuringu autor seisukohal, et lähtuvalt pilveteenuse piiride ülesusest ja universaalsusest ollakse siiski osa globaalsest turust ning väljastpoolt Eestit tulevad võimalikud kliendid hindavad siiski üldtunnustatud ja -tuntud standardeid.

Vaadeldavateks teenusepakkujateks on lihtsustamise kaalutlusel valitud taristulahenduste pakkujad.

Uuringu tulemused:

| | | ISO/IEC 27001 | SSAE 16 / ISAE 3402 | PCI DSS | Safe Harbor / EU Directive 95/46/EC | ECSA või EURO-PRISE | SLA | Pilve-teenuse tunnused |
|---|---|---|---|---|---|---|---|---|
| 1 | Amazon Web Services[18] | jah | jah | jah | jah | ei | 99,9% | jah |
| 2 | CloudSigma[19] | jah | jah | jah | jah | ei | 100% | jah |
| 3 | Microsoft Azure[20] | jah | jah | jah | jah | ei | 99,9% | jah |

[18] http://aws.amazon.com
[19] https://www.cloudsigma.com
[20] http://azure.microsoft.com/en-us/

| | | ISO/IEC 27001 | SSAE 16 / ISAE 3402 | PCI DSS | Safe Harbor / EU Directive 95/46/EC | ECSA või EURO-PRISE | SLA | Pilve-teenuse tunnused |
|---|---|---|---|---|---|---|---|---|
| 4 | Rackspace[21] | jah | jah | ei | jah | ei | 99,9% | jah |
| 5 | GoGrid[22] | ei | jah | jah | jah | ei | 100% | jah |
| 6 | Mochahost[23] | ei | jah | ei | jah | ei | 100% | jah |
| 7 | City Cloud[24] | ei | ei | ei | ei | ei | 100% | jah |
| 8 | DataCenter[25] | ei | ei | ei | ei | ei | 100% | ei |
| 9 | UpCloud[26] | ei | ei | ei | ei | ei | 100% | jah |
| 10 | Elion[27] | ei | ei | ei | ei | ei | - | ei |
| 11 | Termnet[28] | ei | ei | ei | ei | ei | 99,98% | ei |
| 12 | Virtuaal.com[29] | ei | ei | ei | ei | ei | 99,98% | jah |
| 13 | Wavecom.ee[30] | ei | ei | ei | ei | ei | 100% | jah |

[21] http://www.rackspace.com
[22] http://www.gogrid.com
[23] http://www.mochahost.com
[24] https://www.citycloud.com
[25] http://www.datacenter.fi/en
[26] https://www.upcloud.com
[27] https://www.elion.ee/ariklient/it-teenused/pilveteenused/pilveserver
[28] http://www.termnet.ee
[29] https://www.virtuaal.com
[30] https://www.wavecom.ee/pilveserver/

| | | ISO/IEC 27001 | SSAE 16 / ISAE 3402 | PCI DSS | Safe Harbor / EU Directive 95/46/EC | ECSA või EURO-PRISE | SLA | Pilve-teenuse tunnused |
|---|---|---|---|---|---|---|---|---|
| 14 | Leviracloud.ee[31] | ei | ei | ei | ei | ei | 100% | jah |
| 15 | Zone.ee[32] | ei | ei | ei | ei | ei | - | jah |
| 16 | Infobit.ee[33] | ei | ei | ei | ei | ei | - | ei |
| 17 | Procloud.ee[34] | ei | ei | ei | ei | ei | - | jah |
| 18 | Elisa[35] | ei | ei | ei | ei | ei | - | ei |
| 19 | Max[36] | ei | ei | ei | ei | ei | 99,98% | ei |
| 20 | Veebimajutus.ee[37] | ei | ei | ei | ei | ei | - | jah |

**Tabel 1: teenusepakkujate uuringu tulemused**

Uuringust järeldub, et erinevate vastavussertifikaatide olemasolule ja nende presenteerimisele on väga tugevat rõhku pannud väga suured ja nimekad teenusettevõtted. Näiteks Microsoft Azure on oma tutvustuses välja toonud 18 ja Amazon Web Services (AWS) 21 erineva sertifikaadi olemasolu, mille seas on nii USA kui muude regioonide ja

[31] http://www.leviracloud.eu/public/
[32] https://www.zone.ee/et/teenus/pilveserver/
[33] https://www.infobit.ee
[34] http://www.procloud.ee
[35] https://www.elisa.ee/et/ariklient/arilahendused/pilveteenused/serverimajutus
[36] http://www.max.ee/frontpage/teenused/pilveteenused/
[37] https://www.veebimajutus.ee/vps-pilveserver/

sertifitseerijate tunnistusi. Muuhulgas on AWS'l olemas IT-Grundschutz, millel põhineb ka Eesti kolmeastmeline etalonturbesüsteem ISKE, vastavuskinnitus.

Põhjusena näeb autor tugevamalt arenenud teenuse keskkonda, pikemat tegevuskogemust, konkurentsiolukorda ning muidugi ka suuremat turgu, käivet ja seeläbi rohkemaid vahendeid vastavuste saavutamiseks (seda ülemaailmselt, mis tähendab omakorda, et suurettevõtete jaoks on turg globaalne). Hea on tõdeda, et ka Euroopa Liidus on tugevaid teenusepakkujaid (CloudSigma), kes suudavad globaalselt tegutseda, kuid kelle peakontor ja päritolumaa on Euroopas. Samas, mida lähemal Eestile, seda sarnasemaks meie omadele muutuvad ka lähinaabrite (Soome, Rootsi) teenusepakkujate probleemid.

Mis puudutab Eesti pilveteenuseid, siis osad teenusepakkujad ei ole näiliselt hästi mõistnud, millega tegeletakse, sest pilveteenuste mõistet kasutatakse oma toodete kirjelduses peaaegu suvaliselt (Elisa, Max). Autor ei sea kahtluse alla asjaolu, et nimetatud teenusepakkujate pakutav ei võiks olla kvaliteetne ja üle võrgu kättesaadav, kuid kirjeldatud teenused vastavad pigem teenuse tavalise sisseostmise (*outsourcing*) kirjeldusele (Millard, 2013).

Uuringu põhiliseks vaatlusaluseks olnud sertifikaadid puuduvad teenusepakkujate tutvustusest pea täielikult (autor ei täheldanud tihti ka muude sertifikaatide ja tunnistuste, mida tabel ei kajastanud, olemasolu), või ei peeta nende esitlemist oluliseks, mis omakorda muudab kahtlusväärseks lubatava teenuse taseme ja kättesaadavuse. Tõsi, andmekeskuste puhul vihjati Tier tingimuste vastavusele (Virtuaal.com, Leviracloud), kuid kinnitust peale teenusepakkuja sõnadele siiski polnud.

Teenustele ligipääsemine on tülikas. Elion, Infobit, Max ja Termnet eeldavad teenuse avamist läbi kliendihalduri, mis ei vasta pilveteenuste üldisele tunnusele olla vajaduspõhiselt kättesaadav. Halva näitena võib siinkohal eriti välja tuua Elioni, kelle meelest võib pilveteenuse kliendile avada 3 tööpäeva jooksul teenuse avamise soovi avaldamise ajast alates[38]. Elioni nö pilveteenuse tingimustes on veel üks kummaline nõue kliendile: raporteerimiskohustus. See seisneb kliendi kohustuses raporteerida, milline on eeldatav kliendi poolt kasutatavate teenuste maht järgneval, poolte vahel kokku lepitud perioodil.

[38] https://www.elion.ee/files/documents/et/tootetingimused/it-teenused/TT_Pilveserver_est.pdf

Väga palju kirjeldatakse küll erinevaid tehnilisi lahendusi (serveriruumi ülesehitus, ruumi varustatus elektritoite ja kliimaseadmega, valvevahendid) kui ka serverite füüsilisi ja virtuaalseid parameetreid ning võimalusi (nt Max, WaveCom, Termnet). Kirjeldatu võib sisuliselt kõik õige olla, kuid kui kolmanda sõltumatu osapoole kinnitus puudub, siis muutub kogu kirjeldus kasutuks. Siin ei ole kasu ka kliendipoolsest andmekeskuse külastamisest, sest klient ei tea mida vaadata ega hinnata. Muuhulgas muutub kasutuks väga sageli välja toodud SLA tase, sest sellel lihtsalt ei ole tagatist. Viimast paraku kinnitab näiteks jaanuaris 2015 toimunud Wavecom'i teenuse katkestus (Delfi Forte, 2015), millest taastumiseks ettevõte valmis ei olnud. Isegi teenusega tutvumise eesmärgil ei olnud Wavecom'i teenuse koduleht külastamiseks uuringuperioodil kohati kättesaadav. SLA on veel seetõttu huvitav vaadelda, et väga suured teenusepakkujad (nt AWS, Azure), kelle tehnoloogiline ja lahenduste loomise võimekus tõenäoliselt suurem kui väiksematel teenusepakkujatel, ei lähe kaasa SLA 100% lubadustega, vaid jäävad 99,9% peale. Samas kui osade 100% teenustaset lubavate teenusepakkujate puhul on välja töötanud lausa kompensatsioonipaketid puhkudeks, kui teenus peaks katkema.

Kuigi uuringu eesmärgiks ei olnud võrrelda hindu ega funktsionaalst, jäi paratamatult silma, et kliendisõbralikke teenuse kalkulaatoreid ei pidanud kõik teenusepakkujad vajalikuks välja tuua, infot jagavad hoopis kliendihaldurid või müügijuhid, mis ei ole märk teenuste läbipaistvusest.

Eestist väljas asuvate andmekeskuste olemasolu tõid välja Procloud ja Zone.

Samuti jäi konkreetse uuringu skoobist välja asjaolu, et kuigi teenused on sertifikaatide mitteolemasolu või mitteesitlemise tõttu suunatud pigem pimesi Eesti siseturule, ei pea teenusepakkujad (Leviracloud) oluliseks oma teenuse tingimusi ja kehtestatud teenuslepinguid avaldada eesti keeles[39]. Leviral kodulehel oli kasutajana probleeme kindla keele raames püsida, sest osa infot polnud valitud keeles kättesaadav. Võttes Levira puhul veel arvesse, et 51%[40] sellest kuulub Eesti Vabariigile, on raske mõista, miks riik püüab pakkuda ebaõiget konkurentsi kohaliku avaliku pilveteenuse turul, kus suur enamus osalisi

[39] http://www.leviracloud.eu/et/avalik-pilv/juriidika/
[40] http://www.levira.ee/firmast/

peavad toime tulema erakapitalil. Ja seejuures ei suudeta oma teenuseid usaldusväärsel ja läbinähtaval tasemel pakkuda.

Autor mõistab, et korraliku teenuse tagamine võtab aega ja ressursse ning kohalikud teenusepakkujad on oma evolutsioonilises arengus veebiserverite rendist sammu edasi astunud, kuid sellisel juhul ei tasu siiski pilveteenust pakkuda ainult teenuse nime pärast ajades kas kogemata või meelega segamini erinevad IT teenused. Korralikult ette valmistamata teenuse katkemine on probleemiks nii klientidele kui teenusepakkujale endale, kuid taastamatute (või pika taastusajaga) riskide ilmnedes on just klientidele tekkiv kahju väga suur kas tööseisakute või andmekadude näol.

Lähtudes käesoleva töö alapeatükist 2.5, kus on loetud võimalikud pilveteenuste riskid, ei näe autor nende riskide vältimismehhanisme, mis tähendab, et Eestis pakutavates serverites julgeks hoida vaid testkeskkondi või väiksema tähtsusega IT lahendusi. Riskistsenaariumite avaldumisega kaasnev mainekahjustus tabab aga pilveteenuste sektorit üldiselt, tabades ka süütuid ja korralikke teenusepakkujaid.

# 4. Klientide pilveteenuste kasutamise ja riskiteadlikkuse uuring

Selgitamaks välja, kuivõrd kasutavad Eesti ettevõtted pilveteenuseid, mida teenusepakkujatelt oodatakse ning mida nähakse põhiliste riskide ja probleemidena, teostas töö autor kvantitatiivse meetodiga uuringu. See koosnes veebiuuringust Google Forms vahenditega[41], mis toimus ajavahemikul 01.04 - 10.04.2015 ning saadud andmete põhjal tehtavatest järeldustest. Küsitluse sihtrgrupiks oli valitud väikese - ja keskmise suurusega Eesti ettevõtted, kellele edastati palve uuringus vabatahtlikult ja anonüümselt osaleda. Vastuseid laekus 96, mida on piisavalt, et saadud vastuste põhjal hinnata uurimise all olevaid küsimusi.

Osade küsimuste puhul, kus on rohkem kui 4 valikvastust, on parema ülevaate andmiseks saadud vastused sorteeritud populaarsuse alusel. Rohkem kui 4 vastusega küsimuste puhul olid vastusevariandid esitatud suvalises järjekorras, see tähendab, et küsimustiku koostaja ei

[41] http://www.google.com/forms/about/

järjestanud vastuse valikuid eeldatava populaarsuse alusel, vaid küsitlejad pidid valikust endale sobivad ise leidma.

Küsitluses osalejad ei näinud teiste vastajate poolt antud vastuseid ega vastuste koondülevaadet.

Küsimused ja neile antud vastused on alljärgnevad.

1) Vastaja roll ettevõttes

| | | |
|---|---|---|
| Omanik / juht | 72 | 75% |
| Muu | 13 | 13.5% |
| Ettevõtte IT'ga tegelev isik | 10 | 10.4% |
| Ei soovi avaldada | 1 | 1% |

Kommentaar: lähtudes asjaolust, et vastajana määratles end ettevõtte juhiks, omanikuks või IT'ga seotud inimeseks kokku 82 inimest 96'st, siis võib eeldada, et vastaja on väga hästi kursis ettevõtte IT lahendustega, nende arengutega ja probleemidega, mis muudab vastused järgnevatele küsimustele usaldusväärsemaks.

2) Ettevõtte suurus (töötajate arv)

| | | |
|---|---|---|
| 1 - 5 | 65 | 67.7% |
| 6 - 15 | 14 | 14.6% |
| 16 - 25 | 8 | 8.3% |
| 26 - 100 | 1 | 1% |
| 100 + | 4 | 4.2% |
| Ei soovi avaldada | 4 | 4.2% |

Kommentaar: küsimuse eesmärk oli välja selgitada vastava ettevõtte profiil töötajate arvu poolest. Suuruste vahemikud ei vasta küll Statistikaameti määratlusele (Statistikaamet,

2015), kuid vahemike määratlemisel huvitus autor just väiksemaarvuliste kollektiivide eraldamisest, et mõista paremini seal kasutatavaid IT lahendusi.

3) Kas Teie ettevõttes kasutatakse avaliku pilve teenuseid?

| | | |
|---|---|---|
| Jah, oleme olukorraga rahul | 37 | 38.5% |
| Jah, kuid näeme vajadust/soovi kasutatavaid teenuseid/mahte suurendada | 17 | 17.7% |
| Jah, kuid kavatseme kasutatavaid teenuseid/mahte vähendada | 2 | 2.1% |
| Ei, kuid pilveteenuste vastu tuntakse huvi | 26 | 27.1% |
| Ei ning ei kavatseta kasutusele võtta | 14 | 14.6% |
| Ei tea | 0 | 0% |

Kommentaar: küsimuse eesmärk oli välja selgitada pilveteenuste kasutamise määra või määrata nende kasutamise tendentsi (tõusev, langev). Huvipakkuv on asjaolu, et lähtudes võrreldes pilveteenuseid kasutatavate ettevõtete arvu Eurostati hiljutiste tulemustega (Eurostat, 2014), on kasutajate arv protsentuaalselt oluliselt suurem. Kui Eurostati andmetel on kasutajate hulk napilt alla 20%, siis käesoleva uuringu tulemus on tervelt 58,3% (koondsumma "Jah" vastustest). Nii suur erinevus võib olla põhjustatud erinevatest uuringumetoodikatest. Kas vastajad ei olnud oma vastustes siiski päris teadlikud, põhjus on Eurostati küsitletavate erinevas valimis (ettevõtted 10+ töötajaga) või küsitleti eelneva küsitluse osas IT'd mitte eriti laialt kasutatavate ettevõtteid. Igatahes on kõrge teenuste kasutamisprotsent märk innovatiivsusest ja huvist uute lahenduste vastu.

4) Kas pilveteenuste kasutamine/kasutuselevõtt on/oleks Teie hinnangul Teie ettevõttele kasulik ja mõttekas?

| | | |
|---|---|---|
| Jah | 59 | 61.5% |
| Ei | 9 | 9.4% |
| Lähiaastate jooksul on huvi mõned teenused juurutada | 14 | 14.6% |
| Ei oska öelda | 14 | 14.6% |

Kommentaar: küsimusega sooviti saada vastust, kuivõrd vajalikuks ja perspektiivikaks küsitletavad pilveteenuseid peavad. Vastust hinnates on märgata sarnast entusiasmi (kõrge 'jah' vastuse protsent) kui eelnenud küsimuse puhul. Tõenäoliselt on vastuse taga põhjus, et väikeettevõtetele on väga mugav teenuspõhist IT'd kasutada.

5) Milliseid teenusetüüpe kasutate/kasutaksite?

| | | |
|---|---|---|
| Tarkvara teenusena (*SaaS* - nt raamatupidamistarkvara, kliendihaldus, e-post jt) | 65 | 67.7% |
| Platvorm teenusena (*PaaS* - nt arenduskeskkonnad, andmebaasid jt) | 22 | 22.9% |
| Taristu teenusena (*IaaS* - nt taristukomponendid: serverikeskkonnad, andmete salvestusruum jt) | 47 | 49% |
| Ei soovi pilveteenuseid kindlasti kasutada | 7 | 7.3% |

Kommentaar: küsimuse eesmärk oli tuvastada erinevate teenusetüüpide kasutatavust. Ootuspäraselt kõrge oli tarkvara teenusena eelistamine, ka järgnev pingerida oli suhteliselt oodatav, sest platvormi kui teenust nii väga väikeettevõtetes ei kasutata. Samas, ilmselt on vastajad siinkohal jätnud tähelepanuta asjaolu, et ka veebikeskkonnad võivad olla näide platvormteenusest.

6) Kas kasutaksite pigem:

| | | |
|---|---|---|
| Vaid oma ettevõttesiseseid IT lahendusi (oma serverid, serveriruumid, tarkvara, haldus jne) | 21 | 21.9% |
| Vaid pilveteenustel põhinevaid lahendusi (serverid, tarkvara teenusena jne) | 18 | 18.8% |
| Kahe eelmise kombinatsiooni | 57 | 59.4% |

Kommentaar: küsimuse eesmärk oli välja selgitada kuivõrd kasutatakse nö äärmuslikke variante (vaid pilveteenus, vaid ettevõttesisene IT) või nende kombinatsioone. Kombineeritud variandi suur edumaa võib olla märk usaldamatusest pilveteenuste vastu, ent vajadusest ja soovist oma IT lahendused kiired ja kaasaegsed hoida. Konservatiivsete kasutajate hulk, kes vaid ettevõttesisest IT'd kasutaks, on tegelikult üsna väike. Mitmes mõttes väga huvipakkuv on grupp, kes on valmis kogu vajamineva IT pilveteenustena sisse ostma.

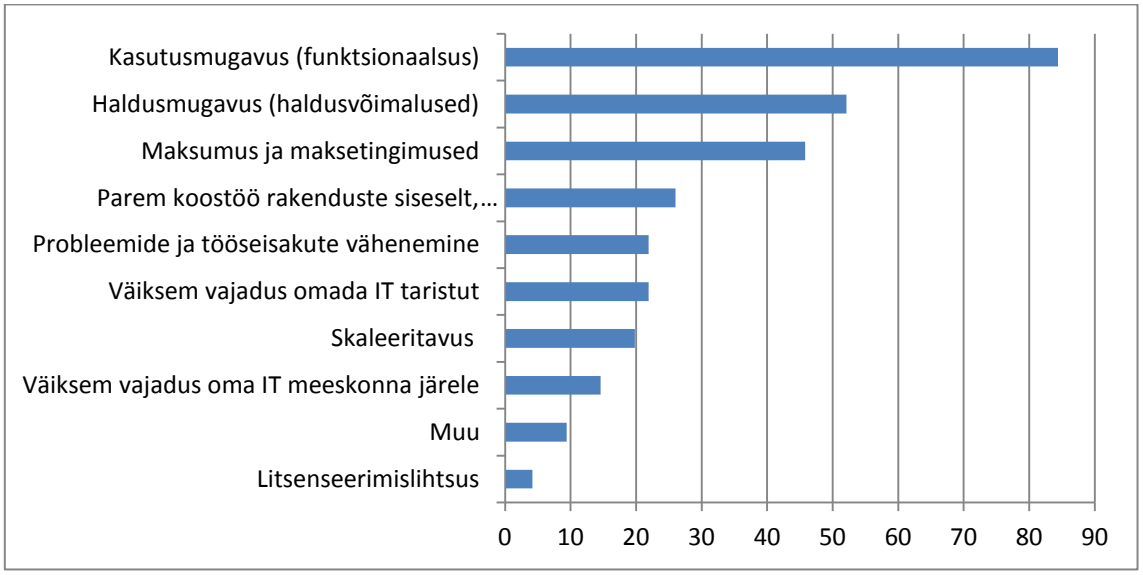
7) Kas Teie jaoks on oluline teenusepakkuja asukohamaa?

| | | |
|---|---|---|
| Eelistatud on Eesti teenusepakkujad | 31 | 32.3% |
| Eelistatud on Euroopa Liidu teenusepakkujad | 9 | 9.4% |
| Vajatakse funktsionaalsust ja teenuse omadusi, asukohamaa pole oluline | 30 | 31.3% |
| Eelistataks Eesti teenusepakkujaid, kui vajalikud teenused ja funktsioonaalsus oleks saadaval | 26 | 27.1% |

Kommentaar: küsimusele kujunenud vastus peaks rõõmustama Eesti teenusepakkujaid, sest ilmneb, et kliendid (59% vastajatest) on huvitatud omamaisest teenusest, paraku ei ole vajalikku funktsionaalsust täielikult saadaval. Euroopa Liidu teenusepakkujaid alternatiivina ei nähta, küll aga on konkreetsete vajadustega kliendid nõus oma andmeid hoidma ükskõik millises muus riigis.

8) Mis oleks/on pilveteenuste kasutamise puhul Teile kõige olulisemad argumendid (valida olulisemad 3)?

| | | |
|---|---|---|
| Kasutusmugavus (funktsionaalsus) | 81 | 84.4% |
| Haldusmugavus (haldusvõimalused, halduse kiirus) | 50 | 52.1% |
| Maksumus ja maksetingimused | 44 | 45.8% |
| Parem koostöö rakenduste siseselt, rakenduste ja töötajate vahel | 25 | 26% |
| Probleemide ja tööseisakute vähenemine | 21 | 21.9% |
| Väiksem vajadus omada täiemahulist IT taristut ( nt serveriruume) | 21 | 21.9% |
| Skaleeritavus (võimalus teenuse mahtu vastavalt vajadusele muuta) | 19 | 19.8% |
| Väiksem vajadus oma IT meeskonna järele | 14 | 14.6% |
| Muu | 9 | 9.4% |
| Litsenseerimislihtsus | 4 | 4.2% |




**Joonis 3: kasutajate küsitluse 8. küsimuse vastuste graafik**

Kommentaar: selle küsimusele vastamiseks anti küsitletavatele kolm valikuvõimalust saamaks kliendiootustest paremat ülevaadet. Vaid ühe valikvastuse valimise korral oleks vastused ebainformatiivsemalt jagunenud, sest inimesed oleks valinud vaid kõige olulisema ning muud olulised aspektid poleks küsitlejale avaldunud. Tulemused räägivad selgelt, et pilveteenustest otsitakse ja leitakse valdavalt sobivat funktsionaalsust. Samuti on oluline teenuste haldamise lihtsus ja kiirus (uute süsteemide loomine, kasutajate

tekitamine/kaotamine jne). Hinnaargument on klientidele samuti oluline. Litsenseerimisega kliendid end eriti ei vaeva ning valikvastuse "Muu" valinud vastajad ei pidanud kahjuks täpsustuste lisamist oluliseks. Järjestuses keskmiste vastuste blokk näitab samuti pilveteenuste positiivsete külgede märkamist.

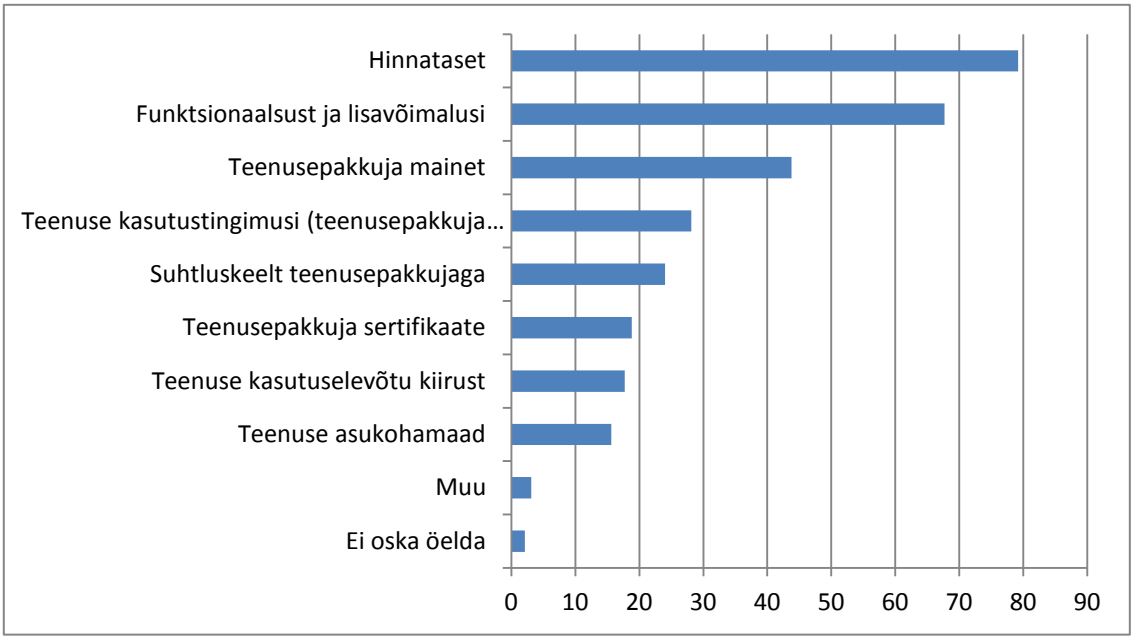
9) Kas peate pilveteenuste kasutamist riskantseks?

| | | |
|---|---|---|
| Jah | 29 | 30.2% |
| Ei | 38 | 39.6% |
| Ei oska öelda | 29 | 30.2% |

Kommentaar: töö autor ootas sellele küsimusele vastajate poolt kahtlevamat seisukohavõttu. Nähtavates tulemustes nähtub hoopis positiivsem vastus. Riskantsust mitte täheldatavate vastuste hulk oli üllatavalt suur, kahtleva seisukoha puhul oleks huvitav analüüsida vastanute vanuselist profiili, kahjuks sellist võimalust ei ole. Ohte märkab siiski kolmandik vastanutest, mis on iseenesest hea näitaja, eriti kui arvestada Eesti teenusepakkujate eelistamist ning viimaste teatud hoolimatust, mis avaldus eelmises töö peatükis kus vaadeldi sertifitseerimisprobleeme ja vastavuskontrolle.

10) Mida peate oluliseks teenusepakkuja valikul (valida 3)?

| | | |
|---|---|---|
| Hinnataset | 76 | 79.2% |
| Funktsionaalsust ja lisavõimalusi | 65 | 67.7% |
| Teenusepakkuja mainet | 42 | 43.8% |
| Teenuse kasutustingimusi (õigused, kohustused jne) | 27 | 28.1% |
| Suhtluskeelt teenusepakkujaga | 23 | 24% |
| Teenusepakkujale omistatud sertifikaate, rakendatud standardeid | 18 | 18.8% |
| Teenuse kasutuselevõtu kiirust | 17 | 17.7% |
| Teenuse asukohamaad | 15 | 15.6% |
| Muu | 3 | 3.1% |
| Ei oska öelda | 2 | 2.1% |



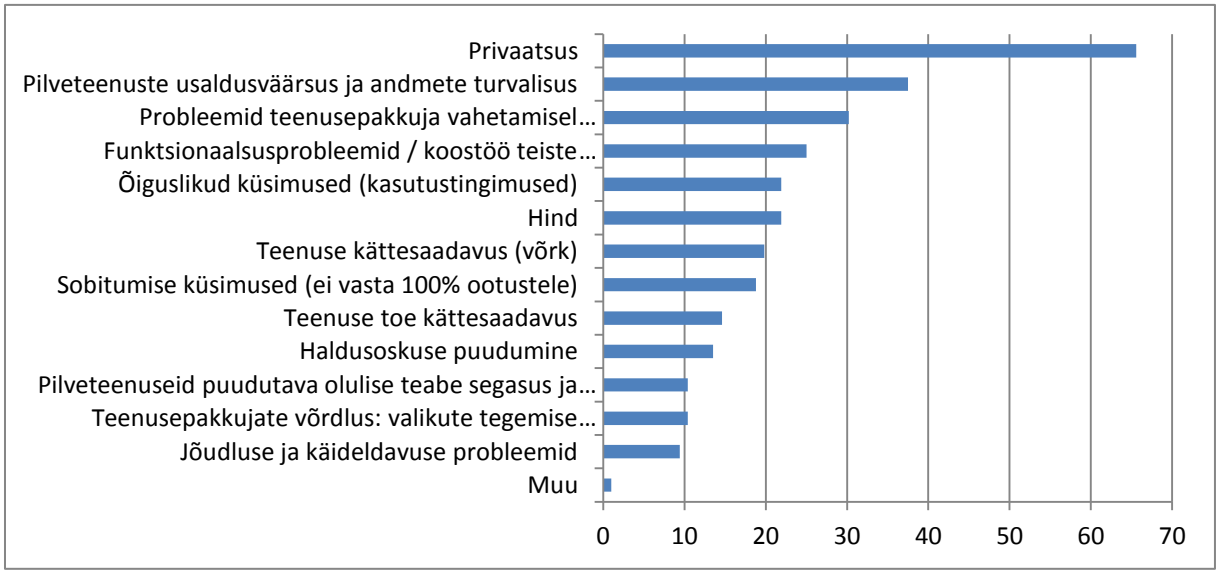

**Joonis 4: kasutajate küsitluse 10. küsimuse vastuste graafik**

Kommentaar: kui üks eelnenud küsimus ( 8) Mis oleks/on pilveteenuste kasutamise puhul Teile kõige olulisemad argumendid?) puudutas pilveteenuseid üldiselt, siis see küsimus tundis huvi, mida jälgitakse teenusepakkuja valikul. Ilmselgelt märgatakse esmajärjekorras teenuse hinda, seejärel funktsionaalsust. Seejärel kaheldakse veidi teenusepakkuja headuses ning see probleem lahendatakse maine uskumisega. Kvaliteeti otsides märgatakse küll ka sertifikaate ja standardeid, kuid ometi usaldatakse halvastimõõdetavat mainet mõnevõrra

rohkem. Suhtluskeel teenusepakkujaga kui ka teenuse asukohamaa sai siin ootamatult vähe tähelepanu, sest 7. küsimuses saadud järeldus enam ei toimi, funktsionaalsus võidab.

11) Mida näete põhiliste probleemidena/riskidena pilveteenuste puhul (valida 3)?

| | | |
|---|---|---|
| Privaatsus | 63 | 65.6% |
| Pilveteenuste usaldusväärsus ja andmete turvalisus | 36 | 37.5% |
| Probleemid teenusepakkuja vahetamisel (tootjalõks) | 29 | 30.2% |
| Funktsionaalsusprobleemid | 24 | 25% |
| Õiguslikud küsimused (kasutustingimused) | 21 | 21.9% |
| Hind | 21 | 21.9% |
| Teenuse kättesaadavus (võrk) | 19 | 19.8% |
| Sobitumise küsimused (ei vasta 100% ootustele) | 18 | 18.8% |
| Teenuse toe kättesaadavus | 14 | 14.6% |
| Haldusoskuse puudumine | 13 | 13.5% |
| Pilveteenuseid puudutava olulise teabe segasus ja leitavus | 10 | 10.4% |
| Teenusepakkujate võrdlus raskendatud ja aegavõttev | 10 | 10.4% |
| Jõudluse ja käideldavuse probleemid | 9 | 9.4% |
| Muu | 1 | 1% |




**Joonis 5: kasutajate küsitluse 11. küsimuse vastuste graafik**

Kommentaar: vastustest nähtub, et eelkõige muretsetakse privaatsuse pärast, see on ka üldiselt üks põhilisi pilveteenuste murekohti. Siinkohal saab paraku jälle tõdeda, et kliendi käes on valiku tegemise otsus, millise teenusepakkuja kätte oma andmed usaldatakse ning siin muutub oluliseks tehtav kodutöö nii teenusepakkuja tausta, asukohamaa, suutlikkuse, rakenduvate seaduste ja regulatsioonide koosmõju. Taas muutub määravaks kliendi enda hinnang oma andmete väärtusele, arusaam teenuse tingimustest, teenusepakkuja pakutavate riskide ja teenuse headuse tasakaal jne. Muud riskid on suhteliselt võrdselt jagunenud, kuid teabe segasus ja leitavus oleks võinud kõrgemal positsioonil asuda, eriti arvestades pilveteenuste osas skeptiliste vastajate osakaalu (9. küsimus, teenuseid pidasid riskantseks 30% vastanutest). Samuti oleks olnud hea näha kõrgemal teenusepakkujate võrdlemise probleemi, sest vastusest järeldub, et kliendid muretsevad rohkem teenuse usaldusväärsuse ja turvalisuse pärast, kuid ei nähta probleemi, mille magistritöö autor on tuvastanud - olulise info puudumine teenuste tutvustusest. Riskide avaldumisel näeb autor seega ka klientide süüd liigse pealiskaudsuse näol.

12) Kas olete mõelnud enda jaoks oluliste riskide maandamisele või olete seda valmis tegema?

| | | |
|---|---|---|
| Jah | 29 | 30.2% |
| Ei | 7 | 7.3% |
| Mingil määral | 43 | 44.8% |
| Puudub vajadus | 8 | 8.3% |
| Ei oska midagi ette võtta | 9 | 9.4% |

Kommentaar: küsimuse eesmärk oli välja selgitada, kuivõrd mõeldakse riskide maandamise peale. Positiivne on, et neid, kes ei oska või ei kavatse riskidega tegeleda, on üsna vähe. Seevastu neid, kes näevad oma osalust riskide maandamisel ning ei jäta kõike teenusepakkuja mureks on tervelt 75% vastanutest. See protsent võiks muidugi veel kõrgem olla, kuid kui ka need vastajad, kes ei osanud riske maandada, oma muredele lahenduse leiavad, läheneb vastutustundlike klientide osakaal 85%le ja selle tulemusega võiks juba rohkem rahule jääda.

13) Kas olete pidanud tegelema realiseerunud riskide tagajärgede kõrvaldamisega?

| | | |
|---|---|---|
| Ei, sest ei kasuta pilveteenuseid | 26 | 27.1% |
| Ei, intsidente pole õnneks esinenud | 54 | 56.3% |
| Tõsiseid intsidente pole esinenud tänu ennetustegevusele ja riskide maandamisele | 12 | 12.5% |
| Jah | 4 | 4.2% |

Kommentaar: nende vastajate osakaal, kes on seni riskide mitteavaldumise osas lihtsalt õnnelikud olnud, on kahjuks päris kõrge. Vastus annab mõista, et liialt oma andmete ja rakenduste turvalisusele ei mõelda, või kui mõeldakse, siis ei tegutseta vastavalt. Kahjuks on ka suhteliselt kõrge protsent neid kasutajaid, kes on probleemidega kohtunud. Siinkohal puudub täpsem info, mis laadi intsidentidega oli tegemist ning kui ulatuslik oli mõju. Et vastused ei andnud täpsustusvõimalust, on võimalik, et kasutajad on kokku puutunud muude IT probleemidega (veebihosting, serverimajutus vms), mida on kohati lihtne pilveteenustega segi ajada. Sihiteadlikke riskide maandajaid on suhteliselt vähe.

14) Kust pärineb Teie ettevõttes pilveteenuste alane teave?

| | | |
|---|---|---|
| Teenusepakkujate kodulehed | 37 | 38.5% |
| Internetist leitavad teenusepakkujatest sõltumatud võrdlused ja uuringud | 35 | 36.5% |
| Partnerettevõtted | 23 | 24% |
| Vastav(ad) töötaja(jad) endal olemas | 19 | 19.8% |
| Ei oska öelda | 9 | 9.4% |
| Ei soovi avaldada | 3 | 3.1% |

Kommentaar: küsimuse eesmärk oli saada ülevaade infoallikatest, mida küsitletavad pilveteenuste kohta käiva teabe hankimiseks kasutavad. Napilt aga kindlalt on põhiliseks infoallikaks teenuste kodulehed, mis ei ole liialt informatiivsed, vähemalt andmeturbe

seisukohast. Siit järeldub, et teenusepakkujad saavad ise väga palju ära teha oma maine ja kvaliteedi tõstmiseks, klientide infootsingu allikad on teada.

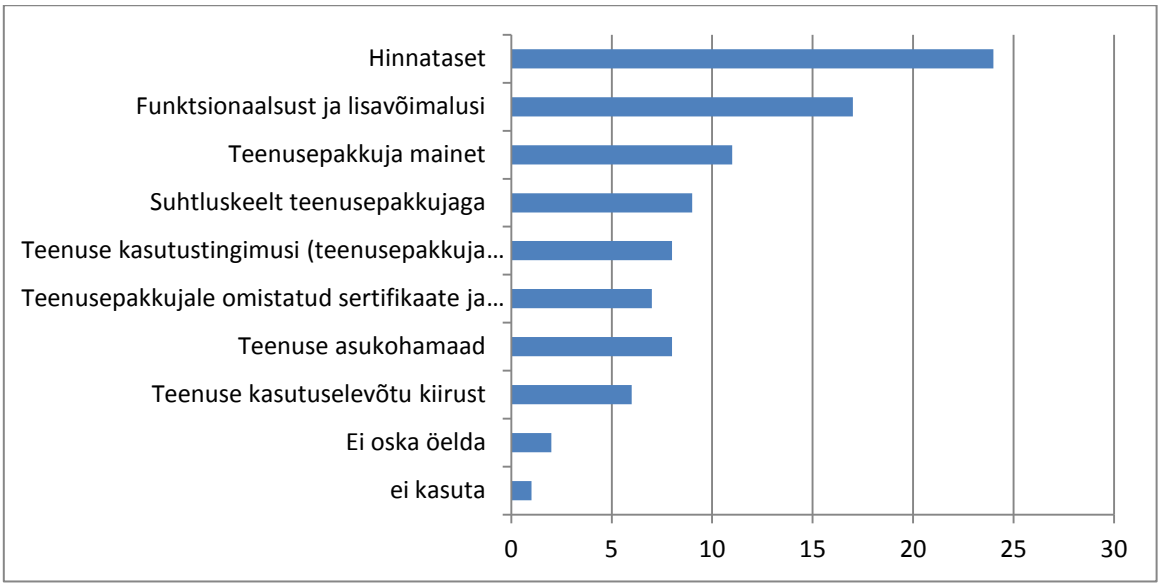
Uuringutulemustest saadud vastuste andmete analüüsi põhjal pidas autor võimalikuks omakorda leida vastused küsimustele:

Kas riskide maandusele on mõelnud pigem IaaS, PaaS või SaaS lahenduste kasutajad?

Riske on maandanud või sellele mõelnud 72 vastajat. Neist kolm on riskid maandanud täielikult, pilveteenuseid mitte kasutades. Nende seast, kes kasutavad või kasutaksid pilveteenuseid, on riskide maandusele mõelnud kõige rohkem SaaS lahenduste kasutajad (51), seejärel IaaS lahendused (15) ja kõige vähem mõeldakse PaaS'i riskide maandamise peale (3 kasutajat).

Mida peavad oluliseks teenusepakkuja valikul need kasutajad, kes eelistavad Eesti pilveteenuseid?

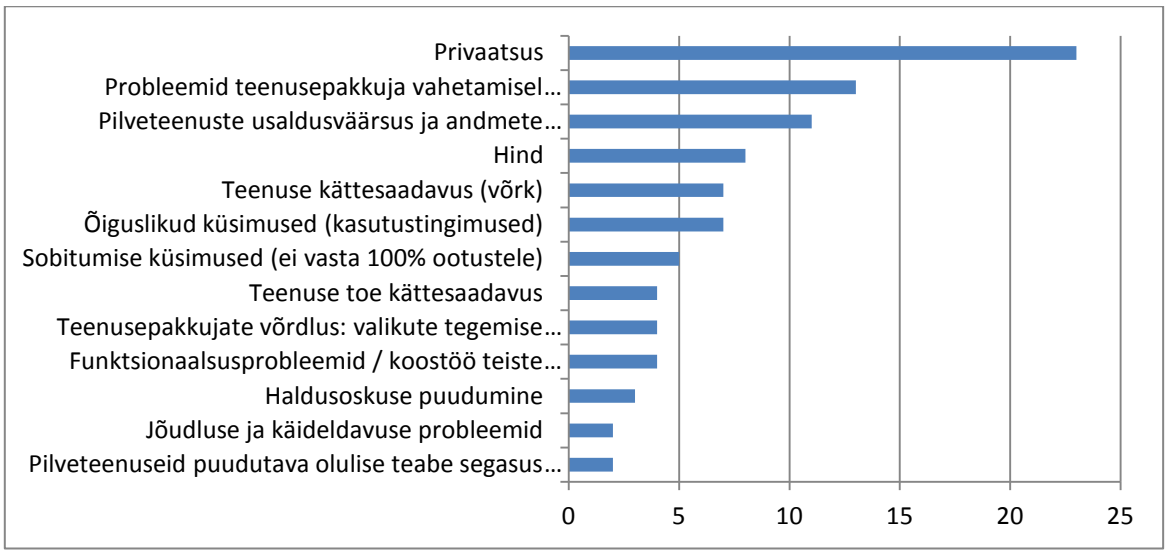
Nende vastajate seas, kes eelistasid Eesti teenusepakkujaid oli enim äramärgitud põhjuseks ülekaalukalt hind (24 vastust), järgnes funktsionaalsus (17 vastust) ning kolmandana peeti oluliseks teenusepakkuja mainet (11 vastust). Teenuste kasutustingimused ja töökindluse tõendid jäid tahaplaanile (vastavalt 8 ja 7 äramärkimist).




**Joonis 6: Eesti teenusepakkujaid eelistavate klientide põhjendused**

Milliseid pilveteenuste riske näevad need kasutajad, kes eelistavad Eesti teenusepakkujaid?

31 Eesti teenusepakkujaid eelistanud klientide hirme vaadates selgus, et kõige rohkem kardetakse privaatsuse pärast (23 vastust), järgnes tootjalõksu risk (13 vastust) ning kolmandana nähakse pilveteenuste ja nende paiknevate andmete turvalisust (11 vastust). Kõige vähem kardeti, et teenuse jõudluse probleeme ning olulise info leitavust ei peetud samuti väga probleemiks. Sarnaselt eelmisele küsimuse vastustele on näha, et riskidena nähakse erinevaid asjaolusid, mitte mõnda üksikut.




**Joonis 7: Eesti teenusepakkujaid eelistavate klientide riskihinnangud**

# 5. Kliendipoolsed riskimaandusvõimalused

Iseenesest ei ole riskide maandamine kohustuslik tegevus, kuid sellistel puhkudel ei tasu probleemide ilmnedes ka süüdlasi otsida. Kui tegemist on ettevõtte kasutatavate pilveteenuste toimeprobleemidega või mingil moel andmekadudega, tekib paratamatult vajadus kasutatav teenus või andmed taastada ning ka teada, kes oli juhtunu eest vastutav. Üldine reegel on, et teenusepakkujad loovad keskkonna ja muid kohustusi väga võtta ei soovi.Klientidele jääb vastutus andmete eest (Carstensen, Golden, & Morgenthal, 2012).

Riski saab vaadelda kui suhet ärivõimaluste ja riskitolerantsi vahel ehk mõnikord kompenseerib võimalik saadav kasu sellega kaasneva riski (Catteddu, 2010). Sellest

tulenevalt võib aru saada, kui mõnda teenust või keskkonda kasutatakse heas usus ilma riskide avaldumisele mõtlemata. Ent kui teenus omandab püsivama koha ettevõtte töös, on mõistlik enda jaoks olulisemad riskid kaardistada ning leida võimalusi nende maandamiseks.

Tuginedes käesoleva töö eelnenud osadele, pakub autor välja variandid, kuidas võimalikult turvaliselt rakendatud pilveteenuseid kasutada, millele teenusepakkuja valikul tähelepanu pöörata, kuidas peale valiku tegemist kasutatava teenusega ringi käia, kuidas olla valmis probleemideks/riskide realiseerumiseks ning mida nende avaldumise korral siiski teha.

Alati saab riskide hindamisel minna väga põhjalikuks võttes ettevõttesiseselt kasutusele mõne riskide hindamise metoodika nagu nt CRAMM või OCTAVE (Rabai, Jouini, Aissa, & Mili, 2013). Väiksemate ettevõtete puhul võib selline lähenemine aga probleemne olla liigse keerukuse ja mahukuse tõttu. Kohati piisab, kui põhilised ja ettevõttele olulised riskid on teadvustatud, sobiv jääkriski tase leitud ning maandamistegevused planeeritud. Samas on süstematiseerimata lähenemisel võimalus kas tähelepanematusest, teadmatusest või muudel põhjustel mitte märgata ohte, mis tegelikult eksisteerivad. Teine asjaolu on, et nii nagu pilveteenuste valdkond üldiselt on alles arenemas, pole ka konkreetselt väikeettevõtetele mõeldud riskihaldusraamistikku, mis oleks ühest küljest ülevaatlik, teisest küljest lihtne kasutada ja arusaadav. Seetõttu saab hetkel anda ühe parimate praktikate põhjal koosneva soovituse kuidas riske ja teenusepakkujaid hinnata (Granneman, 2011):

Olulisemad vaatluselemendid:

1) kontrollvahendite efektiivsus

hinnata, kas kaalutava teenusepakkuja teenuse kontrollvahendid tagavad piisava kaitse kliendi andmetele või teenustele. Näiteks kas teenusepakkuja on endale ette näinud õiguse ligi pääseda kliendi andmetele või kasutatavatele keskkondadele.

2) auditid ja ülevaade

hinnata teenusepakkuja auditeerimistulemusi ja uurida, kuidas on korraldatud muudatuste haldus. Näiteks kas varasemad tehtud muudatused on tekitanud probleeme teenusepakkuja töös ning kuidas on probleemid lahendatud.

3) tehniline turvaahitektuur

hinnata olemasolevaid tehnilisi võimalusi nagu näiteks tulemüürid, VPN, sissetungi vältimise vahendid (*intrusion prevention*), võrkude eraldatus. Kas teenusepakkuja tingimused vastavad kliendi turvanõuetele?

4) andmete terviklikkus

uurida, kuidas teenusepakkuja haldab ühise riistvara peal erinevate klientide andmeid. Kas see vastab kliendi turva- ja käitlusnõuetele?

5) andmete krüpteerimine

kas ja kuidas teenusepakkuja kliendi andmeid krüpteerib või on see jäetud täielikult kliendi hallata?

6) opereerimiskindlus

kas teenusepakkujal on olemas taaste- ja teenuse jätkamise kavad? Kui tihti nimetatud kavasid testitakse? Kas teenusepakkuja andmekeskustel on piisav liiasus kõigil komponentidel, et teenus ei katkeks? Vastavate sertifikaatide olemasolu.

7) standardprotseduurid

hinnata teenusepakkuja standardprotseduure. Näiteks andmete varundamise meetodid, uute töötajate hindamisprotseduurid. Samuti kuulub siia alla küsimus, kuidas teenusepakkuja esindab kliendi huve, kui teenusepakkuja satub juurdluse või kohtumenetluse alla.

8) teenusepakkuja stabiilsus

hinnata teenusepakkuja praegust ja varasemat finantsseisu.

9) intellektuaalomand

uurida kuidas käitub teenusepakkuja kliendi andmetega. Muuhulgas jälgida andmete omamisõigust, tagastamist ja kustutamist peale teenuselepingu lõpetamist.

10) leping

tutvuda teenuse lepingu muude tingimustega, mis võib muuhulgas sisaldada ka nõudmisi kliendile.

Hindamaks teenusepakkuja vastavust enese nõuetele ning võrdlemaks erinevate teenusepakkujate kohta saadud tulemusi omavahel võiks võrdlustabel välja näha järgmine:

| Pilveteenuse riskide hindamise näidis | | | |
|---|---|---|---|
| | Olulisus (1-5) | Risk (1-5) | Kokku |
| Kontrollvahendid | 5 | 2,5 | 13 |
| Auditid | 5 | 4 | 20 |
| Arhitektuur | 3 | 3,5 | 11 |
| Andmete terviklus | 5 | 4 | 20 |
| Andmete krüpteerimine | 2,5 | 4,5 | 11 |
| Opereerimiskindlus | 5 | 1 | 5 |
| Standardprotseduurid | 4 | 2,5 | 10 |
| Teenusepakkuja stabiilsus | 5 | 2,5 | 13 |
| Intellektuaalomand | 5 | 4 | 20 |
| Leping | 5 | 2,5 | 13 |
| Teenusepakkuja kogurisk (25'st) | | | 13,43 |

**Tabel 2: pilveteenuse riskide hindamise näidis**

Numbriline väärtus 1 - 5 tähendab olulisust väiksemast suuremaks.

Näiteks Opereerimiskindlus: olulisus = 5 (väga oluline), risk = 1 (madal)

Iga rea kohta tekib tulemus korrutise teel: olulisus x risk = kogusumma

Teenusepakkuja koguriski näitab Kokku tulba liikmete keskmine väärtus.

Koguriski väikseim väärtus oleks 1 (ebaoluline, madala riskiga) ja suurim 25 (väga oluline, väga kõrge riskiga).

Praegusel kujul peaks näitena toodud riskide hindamise tabel oma lihtsusatud kujul ära katma enamuse töö punktis 2.5 välja toodud riskidest, võimaldades teenusepakkujaid omavahel võrrelda. Samuti on võimalik tabelit vajaduspõhiselt muuta.

On olemas ka veebis leitavaid lahendusi, mis võimaldavad analoogse riskihindamise läbi viia. Näitena võib tuua ENISA poolt loodud väikese - ja keskmise suurusega ettevõtetele suunatud turbekalkulaatori *SME Cloud Security Tool*[42].

Riskide hindamine ei ole ühekordne tegevus, vaid seda tuleks vastavalt ettevõtte vajadustele ja nõuetele regulaarselt läbi viia, mis on omakorda üks probleeme ennetav meede.

Teenusepakkujate võrdluse ajal ei saa ära unustada, et pilveteenuste puhul on väga oluline osa ka teenuse kasutajatel. See tähendab, et infotehnoloogilised oskused pilveteenuseid turvaliselt hallata ja kasutada on samuti turvalisuse üks aspekte. Kas see puudutab siis nt turvaliste VPN ühenduste loomist teenuse ja kliendi vahel, täiendavate varunduslahenduste teostamist, virtuaalmasinate - ja keskkondade haldust, kasutajate ja nende õiguste haldust.

# 6. Järeldused, teema edasiarendused

Lähtuvalt magistriöö valdkonna ja teema edasistest võimalikest arengutest, töö käigus kokku puututud teemat puudutavatest materjalidest ning tehtud uuringute tulemustest näeb töö autor, et pilveteenuste riskijuhtimise valdkond on väga lai ning oluline. Riskide identifitseerimist ja haldust vajavad väga erineva profiiliga ettevõtted ja asutused. Omakorda on võimalik riske käsitledes väga sügavale ja detailseks minna. Kuigi on teatav ühisosa tava IT riskijuhtimisega, on pilveteenuste puhul spetsiifilisi erinevusi.

Sissejuhatavas osas antud ja käsitletud ülevaated ja seletused võisid kohati tunduda üldiselt teadaoleva infona, kuid sellegipoolest pidas autor vajalikuks valdkonda ja järgnevat tööd puudutava info lahtiseletamist. Seda põhjusel, et nii koondus ülevaade teemast ühe töö raamesse ning lihtsustas järgnenud osade käsitlemist. Olulise ja üldise info lahtikirjutamine oli oluline veel seetõttu, et valdkonda veel mitte tundvatel lugejatel oleks võimalik end taustainfoga kurssi viia. Arvestades töö sissejuhatuses välja toodud Eurostati andmeid, kus valdkonna mittetundmine oli probleemiks 42% kasutajatest, on üldinfo käsitlus omal kohal.

[42] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/sme-guide-tool

Magistritöö raames teostatud uuringute tulemused olid autori hinnangul huvitavad ning loodetavasti leiavad kasutust või annavad vähemalt mõtlemisainet.

Teenusepakkujaid vaadelnud uuringu tulemused ei olnud Eesti teenusepakkujate kohapealt eriti rõõmustavad. Kuigi pilveteenuseid pakutakse, tehakse seda siiski segase terminoloogia abil ning klientidele müüakse peamiselt funktsionaalsust ja hinda, jättes muu olulise klientidele (ja võimalik, et teenusepakkujal ka iseendale) selgitamata. Et IT lahendusi ja sealhulgas pilveteenuseid peetakse tihti ettevõtete oluliseks ja igapäevaseks osaks, ei tohiks teenusepakkujad oma teenuse korralduse tasemesse ning töökindluse tagamisse ja selle tõestamisse nii kergelt suhtuda. Nagu uuringu kokkuvõttes välja toodud, on väga suurtel ja edukatel teenusepakkujatel hulgaliselt sertifikaate ja vastavustunnistusi. Kas nende edukus võib osaliselt olla tingitud oma teenuste kommunikeerimisest kui usaldusväärsetest, töökindlatest ja selle vastavast tõendamisest või mitte, igatahes võimaldab see olla rahvusvaheliselt hinnatum ja klientidele arusaadavam. Et töö autor ei märganud Eesti teenusepakkujate tutvustustel viited, et ollakse suunatud vaid Eesti turule, siis võib eeldada, et teenindataks ka mujalt pärinevaid kliente. Oma taseme avalik veenev tõestamine võiks olla üheks seda soodustavaks meetmeks.

Autor jääb oma hinnangutes seisukohale, et kuigi kohalikud teenusepakkujad püüavad kliente veenda (nende) pilveteenuseid laialt kasutama, siis töö kirjutamise ajal julgeks teenusepakkujate poolt ette antud tingimuste valguses teenusepakkujate kätte usaldada vaid testkeskkondi või väiksema tähtsusega IT lahendusi, mis teenuse katkemisel ei mõjutaks ettevõtte tööd otseselt ja vahetult.

Pilveteenuste kasutajate seas tehtud uuring oli samuti huvitavate tulemustega. Autoril oli hea meel, et vastuseid kogunes piisaval hulgal, et nende põhjal saaks näha eelistusi, arengusuundi ja põhjendusi. Uuringu käigus selgus, et Eesti väikeste - ja keskmise suurusega ettevõtete seas on pilveteenused tuntud nähtus. Vastajate seas oli 59% neid, kes väitsid end avaliku pilve teenuseid kasutavat, täiendavalt oli 27% vastajatest seda meelt, et kuigi teenuseid ei kasutata, on huvi nende vastu täiesti olemas. Pilveteenuste kasutamist ei pidanud vajalikuks vaid 14% vastajatest. 61% vastajatest leidsid, et pilveteenused on nende ettevõtte jaoks kasulikud ja mõttekad. Kahjuks ei käsitlenud uuring, milles uuringu sihtgrupi jaoks kasulikkus avaldub. Teisest küljest ei olnud see ka antud uuringu eesmärk. Samuti

selgus, et pilveteenused on leidnud oma koha ettevõtete töös. Nimelt oli vaid oma ettevõttesiseseid IT lahendusi eelistavate ettevõtete osakaal 22%, samal ajal kui ülejäänud pidasid võimalikuks oma IT vajadused pilveteenustega katta kas osaliselt või täielikult. Üks kolmandik vastanutest eelistas Eesti teenusepakkujaid, teine kolmandik eelistaks samuti kui vajalik funktsionaalsus olemas oleks ning kolmas kolmandik ei pööranud teenusepakkuja päritolule tähelepanu, pidades oluliseks vaid teenuse funktsionaalsust. Funktsionaalsus ja teenuse kasutusmugavus olidki põhilised, mida pilveteenusest otsiti, järgnes haldusmugavus ning kolmandana peeti oluliseks hinda. Jälle jagunesid arvamused kolme enam-vähem võrdsesse ossa, kui küsiti arvamust pilveteenuste riskantsuse kohta: kolmandik pidas riskantseks, kolmandik ei pidanud ning kolmandik ei olnud oma seisukohta veel välja kujundanud. Kahjuks ei käsitlenud uuring küsimust, millistel põhjustel ja kaalutlustel pilveteenuseid turvaliseks peetakse. Arvestades, et päris paljud vastajad eelistasid Eesti teenusepakkujaid, kuid nimetatute tase on selline nagu eelnevas uuringus kirjeldatud, oleks põhjuseid väga huvitav teada. Igal juhul ei ole pilveteenuste turvalisus ja riskantsus konstandid, vaid nende osas saavad kasutajad nii mõndagi ise ette võtta. Nii väitsidki end teinud olevat 30% vastanutest, sellele lisaks oli 45% neid, kes olid mingil määral riskide maandamise peale mõelnud. Neid vastanuid, kes oma pilveteenuste riskide maandamise osas midagi ei osanud ette võtta, oli päris vähe, alla 10%. Samas oli vastajate seas tervelt 56% neid, kes tunnistasid, et võimalike riskide realiseerumise tagajärgedega pole tulnud tegeleda läbi hea õnne. Vaid 12% vastajatest olid tegelenud riskide ennetamise ja maandamisega. Uuringu tulemuste kohaselt nähti ülekaalukalt suurima pilveteenuseid puudutava riskina privaatsusküsimusi, järgnes pilveteenuste üldine usaldusväärsus ja andmete turvalisus. Kolmanda riskina nähti tootjalõksu tekkimist, mis tähendab, et teenusepakkuja vahetamine on kasutatava teenuse eripärade ja mitteuniversaalsuse tõttu raskendatud või võimatu. Taaskord, võttes arvesse teenusepakkujate alast uuringut, on nimetatud hirmud põhjendatult omal kohal. Üheks levinuimaks hirmuks peetav teenuse kättesaadavus andmesidevõrgu probleemide korral asetus riskide edetabelis alles 7. kohale.

Kasutajate seas tehtud uuringu üldistusena saab öelda, et avaliku pilve teenuste kasutamine selle eri vormides on üsna levinud ja vajalik funktsionaalsus leitakse üles. Et teenused olulisel hetkel siiski ei katkeks on kasutajate seas palju neid, kes tuleks teenuse turvalisuse osas tööd teha.

See töö kujutab endast enda ettevõtte jaoks oluliste riskide kaardistamist, tehtud kaardistuse alusel põhjalikumat teenusepakkuja valikut. Käesolev töö annab muu seas ülevaate ka põhilistest pilveteenustega seotud riskidest ning pakub välja meetodi, kuidas väiksemad ettevõtted, kellel suurem IT võimekus puudub, saaksid vajadusel iseseisvalt enda olukorda ennetavalt või jooksvalt hinnata.

Kuigi riskide teemasse on võimalik sügavuti minna, tekkisid autoril töö ja eriti teostatud uuringute käigus teemaga haakuvaid küsimusi, mille osas oleks huvitav edasiarendusi teha. Näiteks pilveteenuste riskiraamistike võrdlus või uuringuna teenuse kasutajate seas: kuidas konkreetselt on väikeettevõtted oma pilve-IT riske maandanud? Samuti millistel alustel tehakse otsus tava IT ja pilveteenuste kasutamise/mittekasutamise vahel? Mille põhjal tehakse teenusepartneri valiku otsus? Ka ulatuslik ja põhjalik teenusepakkujate võrdlus oleks kindlasti väga vajalik.

# 7. Kokkuvõte

Seoses kaasajal väga kiiresti areneva pilveteenuste valdkonna levikuga nägi autor vajadust uurida valdkonnaga kaasnevaid ohte, et neid osata ennetada või tekkinud probleeme lahendada. Sellest lähtuvalt oli magistritöö uurimisprobleemiks: kuidas vähendada pilveteenuste kasutuselevõtul ja kasutamisel erinevaid riske, et kasutatavad teenused töötaksid võimalikult probleemidevabalt. Töö põhieesmärgiks oligi välja selgitada peamised teenustega seotud riskid ning pakkuda välja viise nende maandamiseks. Selle eesmärgi saavutamiseks oli eesmärgiks täita mitmeid alameesmärke: anda ülevaade valdkonnast ja levinumatest riskidest, uurida kliendi seisukohast teenusepakkujate kvaliteeditaset, uurida teenuste (võimalike) kasutajate suhtumist pilveteenustesse, riskide nägemust ja seejärel anda eelneva põhjal ettepanekuid ja soovitusi riskide maandamiseks.

Põhieesmärgi saavutamiseks viidi elektrooniliste allikate põhjal läbi vastava kirjanduse analüüs, kus kasutati artiklites, raamatutes ja veebilehtedel avaldatud teavet. Teenusepakkujate uuringuks viidi läbi kvalitatiivse meetodiga teenuste tutvustuse vaatlus, otsides nimetatute kodulehtedelt olulisi pakutava teenuse kvaliteeti tagavaid tunnuseid. Pilveteenuste kasutajate suhtumist ja riskihinnanguid uuriti kvantitatiivsel meetodil veebipõhise küsitlusena. Eelnenu põhjal anti soovitusi, mida pilveteenuste valikul tähele panna, kuidas teenusepakkujaid omavahel võrrelda ning kuidas kaasnevaid riske hinnata.

Magistritöö olulisemaks tulemuseks peab autor uuringute tulemusi ning riskihindamismeetodite väljapakkumist lähtuvalt väike - ja keskmise suurusega ettevõtete vajadustest lähtuvalt, kellel ei ole liialt suurt IT võimekust. Samuti töö üldist pilveteenuste valdkonda puudutava riskikeskse materjali käsitlemist.

Eelpool kirjeldatut arvesse võttes leiab autor, et magistritöö ja selle täitmiseks plaanitud alameesmärgid said täidetud - sai loodud ülevaade, kuidas vähendada pilveteenuste kasutuselevõtul ja kasutamisel erinevaid riske.

# 8. Summary

**Risk Management in Implementing Cloud Computing**

Master's Thesis

The main objective of this thesis is to aid small and medium enterprises to lower the risks of cloud computing while implementing, or using them so that cloud services could work as problem free as possible. Achievment of the main objective consisted several sub-goals.

To give an overview of cloud computing and the main related risks.

To conduct research from the perspective of - potential - users to find out how well service provicers comply to different 3rd party compliance certifications, and how well useful information is provided.

To conduct research among local SME's to find out their expectations towards cloud computing; and which aspects matters while looking for cloud services provider, as well as cloud related risk awareness.

Based on the previous parts the author of the thesis gave guidelines on how to estimate different cloud providers quality and calculate different risks.

The thesis consists of five main chapters.

Chapter 1 begins with an introduction giving an overview of the reason why this topic was chosen and the research problem.

Chapter 2 describes elements of cloud services, and gives an overview of the main related risks.

Chapter 3 describes the methods of research amongst service providers and includes the research.

Chapter 4 describes the methods of the research amongst cloud service - potential - users and the research itself follows after that.

Chapter 5 gives guidances on how SME's can avoid and mitigate risks whilst implementing and using cloud computing.

Outcomes of the master's thesis are 2 successful researches and risk management guidelines for SME's. The author concludes that the objectives of the thesis were successfully accomplished.

The length of the thesis is 62 pages, it contains 7 figures and 2 tables. The thesis is written in Estonian.

# Kasutatud kirjandus


Aberdeen Group. (20. 08 2011. a.). *Web Security in the Cloud: More Secure! Compliant! Less Expensive!* Kasutamise kuupäev: 06. 04 2015. a., allikas http://www.mcrinc.com/Documents/Newsletters/201108_web-cloud-security-compliance.pdf

AKI. (04 2012. a.). *Pilvandmetöötlus: eraelu puutumatuse ja andmekaitse probleemid.* Kasutamise kuupäev: 11. 04 2015. a., allikas http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Pilvandmetöötlus%20-%20Sopoti%20memorandum.pdf

Carstensen, J., Golden, B., & Morgenthal, J. (2012). Cloud Computing : Assessing the Risks. Kasutamise kuupäev: 28. 04 2015. a.

Catteddu, D. (2010). Cloud Computing: Benefits, Risks and Recommendations for Information Security. Kasutamise kuupäev: 24. 04 2015. a.

Delfi Forte. (27. 01 2015. a.). Kasutamise kuupäev: 29. 04 2015. a., allikas http://forte.delfi.ee/news/tarkvara/mis-toimub-oluline-eesti-hostingupakkuja-katkestas-ootamatult-too?id=70657353

Dutta, A., Choudhary, A., & Peng, A. (2013). Risks in Enterprise Cloud Computing: The Perspective of IT Experts. *Journal of Computer Information Systems*. Kasutamise kuupäev: 06. 04 2015. a.

ENISA. (12 2012. a.). (T. Haeberlen, & L. Dupré, Toim-d) Kasutamise kuupäev: 06. 04 2015. a., allikas Benefits, risks and recommendations for information security: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

Euroopa Komisjon. (22. 07 2013. a.). Kasutamise kuupäev: 29. 03 2015. a., allikas http://ec.europa.eu/dgs/connect/en/content/software-services-cloud-european-cloud-computing-strategy

European Commission Directorate-General for Justice and Consumers. (01. 07 2012. a.). *Arvamus 05/2012 pilvandmetöötluse kohta.* Kasutamise kuupäev: 11. 04 2015. a., allikas http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_et.pdf

Eurostat. (12 2014. a.). *ICT usage in enterprises in 2014.* Kasutamise kuupäev: 04. 04 2015. a., allikas http://ec.europa.eu/eurostat/documents/2995521/6208098/4-09122014-AP-EN.pdf

Gartner. (28. 10 2014. a.). Kasutamise kuupäev: 31. 03 2015. a., allikas http://www.gartner.com/newsroom/id/2889217

Gartner. (01. 10 2014. a.). *The Top 10 Cloud Myths*. (D. M. Smith, Toimetaja) Kasutamise kuupäev: 06. 04 2015. a., allikas gartner.com: http://www.gartner.com/doc/2860422?refval=&pcp=mpe

Granneman, J. (06 2011. a.). *A framework for evaluating cloud computing risk*. Kasutamise kuupäev: 20. 04 2015. a., allikas http://searchcloudsecurity.techtarget.com/tip/A-framework-for-evaluating-cloud-computing-risk

ISACA. (05 2011. a.). *Essential characteristics of Cloud Computing.* Kasutamise kuupäev: 03. 04 2015. a., allikas http://www.isaca.org/groups/professional-english/cloud-computing/groupdocuments/essential%20characteristics%20of%20cloud%20computing.pdf

King, N. J., & Raja, V. (28. 05 2013. a.). What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data. *American Business Law Journal*. Kasutamise kuupäev: 15. 04 2015. a.

Mell, P., & Grance, T. (06 2010. a.). The NIST Definition of Cloud Computing. *Communications of the ACM*, lk 50.

Millard, C. (2013). Cloud Computing Law. Kasutamise kuupäev: 15. 04 2015. a.

Newson, J. (02 2015. a.). The Real Benefits of Cloud Computing. *Recruiter*. Kasutamise kuupäev: 06. 04 2015. a.

Rabai, L. B., Jouini, M., Aissa, A. B., & Mili, A. (01 2013. a.). A cybersecurity model in cloud computing environments. *Journal of King Saud University - Computer and Information Sciences*. Kasutamise kuupäev: 30. 04 2015. a.

Sosinsky, B. (2011). rmt: *Cloud Computing Bible* (lk 7-8). Kasutamise kuupäev: 05. 04 2015. a.

Statistikaamet. (04 2015. a.). *Majanduslikult aktiivsed ettevõtted töötajate arvu järgi*. Kasutamise kuupäev: 28. 04 2015. a., allikas http://www.stat.ee/68771

Õunapuu, L. (2013). *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes.* Kasutamise kuupäev: 14. 03 2015. a.

Yeluri, R., & Castro - Leon, E. (2014). Building the Infrastructure for Cloud Security. Kasutamise kuupäev: 05. 04 2015. a.

# Lisad

## Küsitluse küsimused:

1.04 - 10.04 korraldatud magistritöö küsimustik vastusevariantide originaaljärjekorras

Avaliku pilve teenuseid ja nendega kaasnevaid võimalikke probleeme vaatlev uuring Eesti ettevõtete seas

1) Vastaja roll ettevõttes

- Omanik / juht
- Ettevõtte IT'ga tegelev isik
- Muu
- Ei soovi avaldada

2) Ettevõtte suurus / töötajate arv

- 1 - 5
- 6 - 15
- 16 - 25
- 26 - 100
- 100+
- Ei soovi avaldada

3) Kas Teie ettevõttes kasutatakse avaliku pilve teenuseid?

Avalik pilv: teenusepakkuja jagab arvutusvõimsust dünaamiliselt kõigile soovijatele internetis iseteeninduse ga veebirakenduste ja -teenuste kaudu

- Jah, oleme olukorraga rahul
- Jah, kuid näeme vajadust/soovi kasutatavaid teenuseid/mahte suurendada
- Jah, kuid kavatseme kasutatavaid teenuseid/mahte vähendada
- Ei, kuid pilveteenuste vastu tuntakse huvi
- Ei ning ei kavatseta kasutusele võtta
- Ei tea

4) Kas pilveteenuste kasutamine/kasutuselevõtt on/oleks Teie hinnangul teie ettevõttele kasulik ja mõttekas?

- Jah
- Ei
- Lähiaastate jooksul on huvi mõned teenused juurutada
- Ei oska öelda

5) Milliseid teenusetüüpe kasutate/kasutaksite?

Tarkvara teenusena (SaaS - nt raamatupidamistarkvara, kliendihaldus, e-post jt)
Platvorm teenusena (PaaS - nt arenduskeskkonnad, andmebaasid jt)
Taristu teenusena (IaaS - nt taristukomponendid: serverikeskkonnad, andmete salvestusruum jt)
Ei soovi pilveteenuseid kindlasti kasutada

6) Kas kasutaksite pigem:

Vaid oma ettevõttesiseseid IT lahendusi (oma serverid, serveriruumid, tarkvara, haldus jne)
Vaid pilveteenustel põhinevaid lahendusi (serverid, tarkvara teenusena jne)
Kahe eelmise kombinatsiooni

7) Kas Teie jaoks on oluline teenusepakkuja asukohamaa?

Eelistatud on Eesti teenusepakkujad
Eelistatud on Euroopa Liidu teenusepakkujad
Vajatakse funktsionaalsust ja teenuse omadusi, asukohamaa pole oluline
Eelistataks Eesti teenusepakkujaid, kui vajalikud teenused ja funktsioonaalsus oleks saadaval

8) Mis oleks/on pilveteenuste kasutamise puhul Teile kõige olulisemad argumendid (valida 3)?

Kasutusmugavus (funktsionaalsus)
Haldusmugavus (haldusvõimalused, halduse kiirus)
Skaleeritavus (võimalus teenuse mahtu vastavalt vajadusele suurendada-vähendada)
Probleemide ja tööseisakute vähenemine
Maksumus ja maksetingimused
Parem koostöö rakenduste siseselt, rakenduste ja töötajate vahel
Litsenseerimislihtsus
Väiksem vajadus oma IT meeskonna järele
Väiksem vajadus omada täiemahulist IT taristut (serveriruumid, UPS'id jne)
Muu:

9) Kas peate pilveteenuste kasutamist riskantseks?

Jah
Ei
Ei oska öelda

10) Mida peate oluliseks teenusepakkuja valikul (valida 3)?

Funktsionaalsust ja lisavõimalusi
Hinnataset
Teenusepakkuja mainet
Teenusepakkujale omistatud sertifikaate, rakendatud standardeid
Teenuse asukohamaad
Suhtluskeelt teenusepakkujaga
Teenuse kasutustingimusi (teenusepakkuja poolt kirjeldatud õigused, kohustused jne)
Teenuse kasutuselevõtu kiirust
Ei oska öelda
Muu:

11) Mida näete põhiliste probleemidena/riskidena pilveteenuste puhul (valida 3)?

Õiguslikud küsimused (kasutustingimused)
Sobitumise küsimused (ei vasta 100% ootustele)
Privaatsus
Probleemid teenusepakkuja vahetamisel (tootjalõks)
Jõudluse ja käideldavuse probleemid
Funktsionaalsusprobleemid / koostöö teiste rakenduste ja teenustega
Teenuse kättesaadavus (võrk)
Teenuse toe kättesaadavus
Hind
Pilveteenuseid puudutava olulise teabe segasus ja leitavus
Teenusepakkujate võrdlus: valikute tegemise keerukus ja sellele kuluv aeg
Haldusoskuse puudumine
Pilveteenuste usaldusväärsus ja andmete turvalisus
Muu:

12) Kas olete mõelnud enda jaoks oluliste riskide maandamisele või olete seda valmis tegema?

Jah
Ei
Mingil määral
Puudub vajadus
Ei oska midagi ette võtta

13) Kas olete pidanud tegelema realiseerunud riskide tagajärgede kõrvaldamisega?

Ei, sest ei kasuta pilveteenuseid
Ei, intsidente pole õnneks esinenud
Tõsiseid intsidente pole esinenud tänu ennetustegevusele ja riskide maandamisele
Jah

14) Kust pärineb Teie ettevõttes pilveteenuste alane teave?

Vastav(ad) töötaja(jad) endal olemas
Teenusepakkujate kodulehed
Internetist leitavad teenusepakkujatest sõltumatud võrdlused ja uuringud
Partnerettevõtted
Ei oska öelda
Ei soovi avaldada

## Töös esinevate jooniste loetelu



## Töös esinevate tabelite loetelu