RIIGI INFOSÜSTEEMI AMET

Juhend avalike pilveteenuste turvaliseks kasutamiseks avalikus sektoris

August 2019

Sisukord

Lühikokkuvõte pilveteenustest

Pilveteenusest kui nähtusest on nüüdseks kõik juba kuulnud ning asjade pilves hoidmine on üha populaarsem. Pilves tundub kõik lihtsam, kiirem, kergem ja soodsam. Kohati võib see isegi nii olla, kuid avalike pilveteenuste kasutamise juures tuleb tähelepanu pöörata mitmele olulisele asjale. Käesoleva juhendi eesmärgiks ongi kirjeldada erinevaid pilveteenuseid ning selgitada miks ja milliseid turvameetmeid peab pilveteenuste kasutamisel rakendama.

Kui püüda lühidalt kokku võtta, siis pilveteenus on andmete hoidmine kellegi kolmanda käes. Tegemist on teenuse sisseostmisega, kus tavaliselt üks asutus ostab mõnelt ettevõttelt andmete hoidmise või töötlemise teenust. Sellise teenuse loomus (nt SaaS, PaaS, IaaS mudelid) ja sisu (failiserver, meiliserver, domeen, dokumendihaldus jne) võivad varieeruda, olemuslikult on siiski tegemist välise osapoole teenusega, mida osutatakse üle avaliku interneti. Just need kaks asjaolu – väline osapool ja avalik internet – ongi kogu edasise käsitluse alustaladeks. Nendest tulenevalt saab rääkida pilveteenuse kasutamise ohtudest ja riskidest ning neid maandavatest meetmetest.

Oluline on aru saada vastutuse jäämisest teenuse tellija juurde. Jagatud vastutuse kontseptsiooni kohaselt vastutab teenuse osutaja tellija ees lepinguliselt teenuse kvaliteetse ja nõuetekohase osutamise eest, kuid andmete ja süsteemi turvalisuse eest jääb lõplik vastutus alati siiski asutusele kui teenuse tellijale.

Kuna asutusel on seda vastutust praktikas keeruline realiseerida, sest ta enamasti ei saa minna teenuse osutaja juurde kontrollima, kuidas see asutuse andmeid hoiab, siis on asutusel võimalik teenuse osutaja valikul küsida erinevaid sertifikaate, auditi aruandeid vms, mis demonstreerivad teenuse osutaja võimet teenust korrektselt osutada. Kui aga tegemist on konfidentsiaalsuse osas vähemalt keskmise tundlikkusega andmetega (ISKE S1 ja S2 turva-osaklassid, milleks on suur osa isikuandmeid ning muudel alustel asutusesiseseks kasutuseks tunnistatud andmeid), siis on lisaks sellele vaja neid andmeid hoida krüpteeritult. Krüpteering peab olema piisavalt tugev ning krüptovõti peab olema andmete omaniku (teenuse tellija) ainuvalduses. See tagab selle, et teenuse osutaja ei näe nende andmete sisse.

Kuna avalike pilvede kasutamine käib üle avaliku interneti, siis on oluline, et asutuse ja tema pilves olevate andmete vaheline ühendus oleks samuti krüpteeritud. Mõistetavalt peab ka see

krüpteering olema piisavalt tugev ja krüptovõtmed andmete omaniku käes. See tagab selle, et ainult andmete omanikul on ligipääs pilveressursile.

Need kaks kriteeriumit: andmete krüpteerimine nii salvestamisel (*at rest*) kui ka võrgus transportimisel (*in transit*) on sellised, ilma milleta ei ole pilveteenuseid lubatud kasutada (S1 ja S2 turvaosaklasside puhul). Pilveteenuse osutajaid, et kes ei luba kasutada andmete omanikule kuuluvat privaatvõtit, ei saa kasutada. Teenuseosutajad, kes pakuvad *at rest* krüpteerimist, võivad seda teha hinna eest, mis võib kogu pilveteenuse kasutamise projekti ebaatraktiivseks muuta. Sellegipoolest on oluline, et soodsa hinna nimel ei ohverdataks andmete turvalisust.

1. Saateks

Käesoleva Riigi Infosüsteemi Ameti (*RIA*) juhendi eesmärk on anda Eesti avalikule sektorile üldised juhised avalike pilveteenuste turvaliseks kasutamiseks.

Pilveteenuse kasutamisel usaldab pilveteenuse klient oma andmed kolmanda osapoole valdusesse, jagab sama riist- ja tarkvara teiste klientidega ning haldab oma süsteeme üle avalikku interneti. Seetõttu tekivad pilveteenuse kasutamisel uued turvariskid ning tuleb kasutusele võtta ka uued turvanõuded ja -meetmed.

Juhendis loetletud nõuded ja piirangud avaliku pilveteenuse kasutamiseks tulenevad:

- **küberturvalisuse seadusest**, mis sätestab nõuded võrgu- ja infosüsteemi riskianalüüsi läbiviimiseks ja turvameetmete rakendamiseks;
- **avaliku teabe seadusest**, mis nõuab halduslike ja tehniliste meetmete rakendamist, et juurdepääsupiiranguga teave ei satuks juurdepääsuõiguseta inimeste kätte;
- **hädaolukorra seadusest**, mis sätestab nõuded infosüsteemide piiriüleste sõltuvuste arvestamiseks ja hädaolukorra plaanide koostamiseks;
- **isikuandmete kaitse seadusest**, mis piirab isikuandmete edastamist välisriiki. Isikuandmete edastamine on lubatud Euroopa Majanduspiirkonna lepingu riikidesse[1];
- **Euroopa Liidu uuest isikuandmete kaitse üldmäärusest 2016/679** (*GDPR*), mis asendab alates 25.05.2018 andmekaitsedirektiivi 95/46 ja Eesti isikuandmete kaitse seadust;[2]
- **ISKE**-st ehk riigi andmekogude turvameetmete süsteemist;[3]
- **Euroopa Komisjoni andmete asukohariigi piirangute hoidmise algatusest, mis kaotab põhjendamatud piirangud andmete hoidmisel ja töötlemisel**. [4]

2. Pilveteenuse kasutamise viisid ja mudelid

Erinevad pilvekeskkonnad on täpsemalt kirjeldatud ISKE vastavas meetmes M 4.462z "Sissejuhatus pilveteenuse kasutamisse."[5] Teine, rahvusvaheliselt tunnustatud pilveteenuste definitsioon on väljaandes "NIST 800-145 - The NIST Definition of Cloud Computing".[6] Peamiselt jaotatakse pilveteenused avalikeks-, privaat- ja hübriidpilvedeks.

[1] http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm
[2] http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=ET
[3] https://iske.ria.ee
[4] https://ec.europa.eu/digital-single-market/en/building-european-data-economy
[5] https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M4/M_4.462
[6] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Käeoleva juhendi fookus on avalikel pilvedeteenustel, mida iseloomustavad:

- avatus kõikidele klientidele,
- juurdepääsetavus üle avaliku interneti,
- kõikide ressursside (taristu, riistvara ja tarkvara) jagatud kasutus.

Avaliku pilveteenuse kasutamiseks on kolm mudelit:

a) pilve kui infrastruktuuri mudel,
b) platvormi mudel;
c) tarkvara kasutamise mudel.

Inglise keeles on need vastavalt:

a) "Infrastructure as a Service" ehk IaaS;
b) "Platform as a service" ehk PaaS;
c) "Software as a Service" ehk SaaS.

Mudelite kirjeldus ja omavahelised erinevused on olemas eelpool viidatud ISKE ja NIST-i allikates. Käesolev juhend käsitleb avaliku pilveteenuse kasutamise tingimusi kõigi kolme mudeli kohaselt.

Käesolevas juhendis kasutatakse järgmisi olulisi mõisteid:

- *pilveteenuse klient* - mõiste hõlmab asutusi kui andmekogude vastutavaid töötlejaid ning infosüsteemide ja andmete omanikke;
- *teenuse osutaja* - pilveteenuse eest vastutav ettevõte või asutus. Ühe pilveteenuse erinevaid komponente või alamteenuseid võivad hallata erinevad ettevõtteid, kuid teenuse leping sõlmitakse ühe, vastutava osutajaga;
- *suletud süsteemid* - kõik tavalisel viisil hallatud infosüsteemid. See ei tähenda, et neil ei võiks olla avalikke liideseid või et kõik pilvetehnoloogiat mitte kasutavad süsteemid oleksid omavahel sarnased - selle väljendiga vastandatakse pilveteenuse kasutust muudele tehnoloogiatele.

2.1. Vastutuse jaotus eri pilveteenuse mudelite korral

Pilveteenuse kasutamisel jaguneb vastutus infosüsteemi turbe eest kliendi ja teenuse osutaja vahel. See jaotus on erinevate pilveteenuse mudelite korral erinev.

Üldine skeem vastutuse jaotuse kohta on allolevas tabelis, milles roheline värv tähendab, et süsteemi vastava kihi turbe peab tagama pilveteenuse osutaja.

Süsteemi kiht	**SaaS mudel tarkvara teenusena**	**PaaS mudel platvorm teenusena**	**IaaS mudel taristu teenusena**
Andmed	klient	klient	klient
Rakendused	teenuse osutaja	klient	klient
Rakendusplatvorm	teenuse osutaja	teenuse osutaja	klient
Virtualiseerimiskiht	teenuse osutaja	teenuse osutaja	teenuse osutaja
Riistvara	teenuse osutaja	teenuse osutaja	teenuse osutaja
Andmekeskus	teenuse osutaja	teenuse osutaja	teenuse osutaja

Täpne jaotus on iga pilveteenuse ja alamteenuse korral erinev. Süsteeme pilves majutades peab klient seda mõistma ning oma turbe vastavalt korraldama. **Lõplik vastutus süsteemi turbe eest on alati kliendi kui andmekogu või infosüsteemi omaniku kanda**.

3. Pilveteenuse kasutamisega seotud riskid

Pilves majutatud ja suletud infosüsteemi turvariskid on erinevad. Enamik tavalise süsteemi andmeturbe aspekte - operatsioonisüsteemide, rakendusplatvormide ja veebisüsteemide turve, organisatsiooni ja turvajuhtimisega seotud teemad jne - jäävad pilve kasutamisel samaks. Taristu turve läheb üle pilveteenuse osutajale, kuid klient peab suutma hinnata teenuse osutaja pädevust ja garantiisid.

Lisanduvad uued riskide tüübid, mis on seotud konkreetselt pilvetehnoloogia, avalike võrkude ja väljaspool Eestit olevate süsteemide kasutamisega. Need on lühidalt alljärgmised.

1. **Sõltuvus teenuse osutaja lepingutest ja tingimustest**

Kliendil tekib sõltuvus teenuslepingu tingimustest, mis pilveteenuse puhul üldiselt ei ole kergesti läbi räägitavad ega muudetavad. Lisaks lepingule sõltub klient ka teenuse osutaja reaalsest turvalisusest ja töökindlusest ning tema muudest tehnilistest ja organisatsioonilistest riskidest.

2. **Andmete töötlemise asukoha riskid**

Suurte avalike pilveteenuste andmekeskused asuvad üldiselt Eestist ning tihti ka Euroopa Liidust väljaspool. Andmete töötlemine ja hoidmine väljaspool Eestit peab olema kooskõlas Eesti ja Euroopa andmekaitse nõuetega.

3. **Piiriülesed sõltuvused**

Avalike teenuste osutamisel ja asutuste tööprotsesside korraldamisel pilvesüsteemide kaudu peab arvestama piiriüleste sõltuvustega. Kui andmed on salvestatud või teenust osutav infosüsteem asub väljaspool Eesti riigi piire, siis tuleb need sõltuvused riskianalüüsides, hädaolukorra lahendamise plaanides ja taasteplaanides selgelt välja tuua.

4. **Ressursside jagatud kasutuse riskid**

Pilveteenuse kliendid jagavad samu ressursse - servereid, võrku, salvestusruumi. Erinevate klientide eraldamine on pilveteenuse osutaja ülesanne ning sõltub tema süsteemide ja protsesside turvalisusest. On võimalik, et kliendid saavad teatud tingimustel infot teiste klientide teenuste, andmevahetuse või salvestatud andmete kohta.

5. **Avalike liideste kasutamise riskid**

Pilve kasutamisel võivad kõik loodud süsteemid ja nende liidesed olla avalikud. Seda ka arendus- ja testimis-etappidel, kui turvameetmed on alles rakendamata või kui süsteemi enda olemasolu pole veel avalik.

6. **Avalike võrkude kasutamise risk**

Pilveteenuseid kasutatakse üldjuhul üle avaliku interneti. Nii lõppkasutajate andmed, pilveteenuse haldusoperatsioonid ning andmevahetus kliendi suletud süsteemide ja pilveteenuse vahel liiguvad avalikes võrkudes.

7. **Avaliku haldusliidese ja administraatorite kontode rünnatavus**

Pilvesüsteemi haldusliides on veebipõhine ja avalik ning seetõttu rünnatav. Kui suletud süsteemide administraatorite paroolid lekivad või on haldusliidestes turvanõrkusi, siis kaitsevad süsteemi muud meetmed - välis-, sise- ja toodanguvõrkude eraldamine, VPN, monitooring jne. Pilveteenuse korral on nii pilve enda kui rakenduste haldussüsteem avatud ning lekkinud paroole võib ära kasutada väga lihtsalt.

8. **Küberrünnete mõju laienemine**

Jagatud ressursside kasutamine tähendab, et ründed ühe majutatud süsteemi või kliendi vastu võivad mõjutada ka teisi samas pilves asuvaid infosüsteeme või andmeid.

9. **Uue tehnoloogia kasutamise riskid**

Mistahes uus tehnoloogia või lahendus on seotud uute ohtudega. Pilvetehnoloogia on Eesti asutuste ning IT-töötajate jaoks alles uus ning selle võimaluste tundmaõppimisel ja

rakendamisel võib ette tulla vigu, mis mõjutavad ka süsteemi turvalisust. Pilvetehnoloogia ise areneb samuti väga kiiresti. Ei saa välistada, et turvavigu teevad ka teenuseosutajad ise. Pilvesüsteemide avatud iseloomu tõttu on vigade kiire ja mastaapse ärakasutamise risk suurem kui suletud süsteemide korral.

10. Töökorralduse muutuste riskid

Koos pilveteenusega võetakse tihti kasutusel ka uus töökorraldus, nn "*DevOps*" mudel.[7] DevOps muudab rollijaotuse süsteemi disaini, arenduse, testimise ning halduse vahel paindlikumaks ning teeb süsteemi muutmise kergemaks. Andmeturbe vaatest võib DevOps töökorraldus aga tähendada vastutuse hajumist ja toodangusüsteemi pääsuõiguste andmist varasemast laiemale kasutajate ringile.

11. Jagatud vastutuse riskid

Vastutuse jagunemine kliendi ja teenuse osutaja vahel võib luua olukorra, kus klient eeldab teenuse osutajalt rohkem kui leping ette näeb. Seetõttu võib süsteemi mõni kiht (näiteks rakendusplatvorm või võrgu juurdepääsureeglid) jääda turvamata või mõni vajalik turvamehhanism (süsteemi seire, DDoS kaitse) rakendamata.

12. Süsteemi puudulik dokumenteerimine

Lihtsad haldusliidesed ning DevOps töökorraldus soosivad süsteemide arendamist ja konfigureerimist ilma korraliku, ajakohase dokumentatsioonita. Korrektne dokumentatsioon on aluseks turva-analüüsile ja -testimisele, monitoorimisele ja intsidentide lahendamisele. Pilvepõhiste infosüsteemide loomisel ja haldamisel tuleb seetõttu dokumenteerimisele pöörata tavalisest rohkem tähelepanu.

Samas võib pilveteenuse kasutamine süsteemi turvalisust ka tõsta. Pilveteenuse osutaja pädevus taristu ehitamisel ja haldamisel, tarkvaraliste turvalahenduste pakkumisel ja turbe korraldamisel võib olla parem kui kliendil.

4. Pilveteenuse kasutamise üldised põhimõtted

4.1. Pilveteenuse osutaja valik

Pilveteenuse osutaja valikul peab hindama vastava ettevõtte tehnilist ja organisatsioonilist usaldatavust, tema teenuse tingimuste sobivust konkreetse infosüsteemi nõuetega ning juriidilisi aspekte - piiriüleseid sõltuvusi, andmekaitse nõudeid jne.

Riskihindamise ja mõjuanalüüside tulemusel võib selguda, et andmed või teenus peavad asuma Eestis.

Täpsemalt on pilveteenuse osutaja valikut kirjeldatud ISKE moodulis B 1.17, "Pilvteenuse

[7] https://en.wikipedia.org/wiki/DevOps

kasutamine".[8]

Lisaks võib pilveteenuse osutaja valikul lähtuda järgmistest materjalidest:

- ENISA - Security Framework for Governmental Clouds [9]
- Cloud Security Alliance Security, Trust and Assurance Registry [10]

4.2. ISKE rakendamine pilveteenuse kasutamisel

Pilveteenuse kliendid ei saa teenuse osutaja taristu, organisatsiooni ega haldusprotsesside turvalisust otseselt hinnata. Rahvusvahelise praktika kohaselt auditeerib pilveteenuse osutaja ennast ise ühe või mitme turvastandardi vastu ning avaldab auditite tulemused, samuti garanteerib ta teenuse kasutamise tingimustes ja kliendilepingutes turvaprotsesside järgimise ka tulevikus.

Uuendatud ISKE rakendusjuhend ja auditeerimisjuhend[11] aktsepteerivad selliseid turvaauditite tulemusi ning lubavad vastavaid kliendilepinguid arvestada. Vastavate ISKE moodulite rakendamise võib asendada auditite või lepingutingimuste kontrolliga.

Alternatiivse võimalusena tuleb pilveteenuse osutajal läbida ISKE vastavusaudit. Nii ISKE kui muu metoodika abil läbitud audit peab ära näitama konkreetselt auditeeritud ja turbestandardile vastavad alamteenused.

Mõned rahvusvaheliselt tunnustatud auditeerimis- või sertifitseerimisskeemid on toodud järgnevas loetelus.

- BSI - Compliance Controls Catalogue (C5) [12]
- Cloud Security Alliance - CSA STAR ja CSA Cloud Controls Matrix [13]
- PCI DSS, Payment Card Industry Data Security Standard [14]
- ISO 27001
- ISAE SOC-2[15]

See nimekiri ei ole lõplik ega ammendav - klient võib pilveteenuse osutaja turvagarantiide kontrollimiseks kasutada ka teisi viise. Pilveteenuste sertifitseerimine kui valdkond on alles kujunemisjärgus ning ISKE ei sea piire sellele, millist skeemi kasutada.

Peab arvestama, et isegi turvasertifikaadi ega auditi olemasolu tingitult viimase ulatuse piiratusest ei taga kogu pilveteenuse ega selle osutaja sisulist ja tõsikindlat turvalisust. Seetõttu lasub kontrollimiskohustus, millistele teenustele või millises ulatuses turvalisuse

[8] https://iske.ria.ee/8_06/ISKE_kataloogid/5_Kataloog_B/B1/B_1.17
[9] https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds
[10] https://cloudsecurityalliance.org/star/
[11] https://www.ria.ee/et/kuberturvalisus/iske/juhendid-ja-materjalid.html
[12] https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html
[13] https://cloudsecurityalliance.org/star/
[14] https://www.pcisecuritystandards.org/
[15] https://www.ssae-16.com/category/isae-3402/

garantiid kehtivad, kliendil.

Pilveteenuse kasutamisel tuleb eriti tähelepanelikult järgida järgmisi ISKE mooduleid:[16]

1) *B 3.304 Virtualiseerimine*
   Pilveteenuse kasutamisel virtualiseeritakse kõik infosüsteemi kihid.
2) *B 1.11 Väljasttellimine (Outsourcing)*
   Pilveteenuse kasutamine on sisuliselt üks väljasttellimise erijuht.
3) *B 1.4 Andmevarunduspoliitika*
   Andmete hoidmisel välise teenuseosutaja juures on varukoopiate tegemise ja taaste korraldamine veelgi olulisem kui suletud süsteemi korral.
4) *B 1.7 Krüptokontseptsioon*
   Pilvepõhise süsteemi puhul on andmeside ja andmete krüpteerimine läbiv nõue. Kuna hajussüsteemi võtmehalduse korraldamine on keeruline, siis peab krüptograafia tehniline lahendus olema teada süsteemi arendamise või pilve migreerimise võimalikult varajases etapis.

4.3. Pilveteenuse kasutamise ja ISKE turvaosaklasside sõltuvus

Pilveteenuse kasutamise eelduseks on plaanitava infosüsteemi või andmekogu riskide analüüsimine ning pilves töödeldavatele andmetele ISKE turvaosaklasside määramine. Lisaks tuleb hinnata ka asutuse ülejäänud süsteemi, teenuste ja töökorralduse sõltuvust pilvesse paigutatavatest andmetest.

Pilveteenuse kasutamise põhilised piirangud tulenevad infosüsteemi turvaosaklassidest.

Järgnev tabel annab andmete avalikus pilves hoidmise põhilised reeglid ja piirangud ISKE turvaosaklasside kaupa.

Lahtrite värvide tähendused on järgnevad:

- Roheline – avaliku pilve kasutus on Euroopa Liidu piires lubatud.
- Kollane – avaliku pilve kasutus on lubatud allpool toodud tingimuste täitmisel.
- Oranž – avaliku pilve kasutus on lubatud allpool toodud tingimuste täitmisel ja riskide hindamisel ning andmete varundamisel Eestis asuvasse süsteemi.
- Punane – avalike pilveteenuste kasutamine pole lubatud.

Täht (L, M või H) tähendab turvaosaklasside alusel süsteemile määratud ISKE turvaastet.

[16] https://iske.ria.ee/

				KÄIDELDAVUS			
				K0	K1	K2	K3
TERVIKLUS	T0	KONFIDENTSIAALSUS	S0	**L**	**L**	**M**	**H**
			S1	**L**	**L**	**M**	**H**
			S2	**M**	**M**	**M**	**H**
			S3	**H**	**H**	**H**	**H**
	T1	KONFIDENTSIAALSUS	S0	**L**	**L**	**M**	**H**
			S1	**L**	**L**	**M**	**H**
			S2	**M**	**M**	**M**	**H**
			S3	**H**	**H**	**H**	**H**
	T2	KONFIDENTSIAALSUS	S0	**M**	**M**	**M**	**H**
			S1	**M**	**M**	**M**	**H**
			S2	**M**	**M**	**M**	**H**
			S3	**H**	**H**	**H**	**H**
	T3	KONFIDENTSIAALSUS	S0	**H**	**H**	**H**	**H**
			S1	**H**	**H**	**H**	**H**
			S2	**H**	**H**	**H**	**H**
			S3	**H**	**H**	**H**	**H**

Konfidentsiaalsus

S0 – andmeid võib töödelda avalikus pilves ja hoida EU majandusruumis.

S1 ja S2 – avalike pilvede kasutamine on lubatud, kuid nõutud on andmete krüpteerimine nii salvestamisel (*at rest*) kui ka võrgus transportimisel (*in transit*).

S3 – avalike pilveteenuse kasutamine ei ole lubatud.

Krüptograafia peab olema piisavalt tugev tagamaks andmete salajasust nõutud ajahorisondi piires. Peab arvestama ja eeldama, et kuna pilves hoitavad andmed on kolmandate osapoolte

valduses, ei ole nende absoluutne kustutamine tagatud ning võimalikud ründajad võivad andmeid dekrüpteerida hiljem, kui arvutusvõimsus on kasvanud ja algoritmid ise uute rünnete tõttu nõrgemaks muutunud.

Krüptograafiliste algoritmide tugevuse ja sobivuse hindamiseks soovitame kasutada RIA krüptograafiliste algoritmide elutsükli uuringuid [17].

Käideldavus

K0 – andmeid on lubatud töödelda avalikus pilves ja hoida EU majandusruumis.

K1, K2 – avalike pilvede kasutamine on lubatud, kuid andmekogu omanik peab käideldavuse riske eraldi hindama. Vajadusel tuleb tagada andmete regulaarne varundus teise, sõltumatusse süsteemi. Tuleb korraldada pilves asuva teenuse seire ja intsidentide haldus.

K3 – lisaks K1 / K2 meetmetele tuleb korraldada andmete varundus teise, Eestis asuvasse süsteemi. Kui piiriüleste riskide analüüs seda nõuab, siis tuleb korraldada ka süsteemi või teenuse alternatiivne osutamine Eestis oleva infosüsteemis kaudu.

Terviklus

Avalikus pilves ja EU majandusruumis võib hoida kõikide tervikluse turvaosaklassidega andmeid ja süsteeme.

T1 – Tuleb rakendada tavalised tervikluse tagamise meetmed, näiteks pääsukontrolli ja logide olemasolu.

T2 – lisaks T1 meetmetele tuleb korraldada tervikluslogide saatmine teise süsteemi.

T3 – lisaks T1 ja T2 meetmetele tuleb korraldada tervikluslogide saatmine teise, Eestisse asuvasse süsteemi ning tagada nende terviklus tugeva krüptograafiaga.

4.4 Asutusesiseseks kasutuseks mõeldud teabe ja isikuandmete töötlemine

Piiratud juurdepääsuga teabe ning isikuandmete pilves töötlemisel ja hoidmisel tuleb samuti lähtuda nende ISKE turvaosaklassist. Selliste andmete ja ISKE turvaosaklasside vastavus on kirjeldatud ISKE rakendusjuhendis järgmiselt:

Asutusesiseseks kasutamiseks mõeldud andmed - konfidentsiaalsuse turvaosaklass vähemalt S1.

Tavalised (mittedelikaatsed) isikuandmed - konfidentsiaalsuse turvaosaklass vähemalt S1.

Eriliigilised isikuandmed - konfidentsiaalsuse turvaosaklass vähemalt S2.

Seega võib nii piiratud juurdepääsuga (asutusesiseseks kasutamiseks) mõeldud andmeid kui

[17] https://www.ria.ee/et/ametist/uuringud-analuusid-ulevaated.html

isikuandmeid avalikus pilves hoida ja töödelda, kuid peab rakendama S1 või S2 konfidentsiaalsusklassi korral nõutud turvameetmeid. Loomulikult peab lisaks täitma ka teisi isikuandmete kaitse seaduse ja ISKE nõudeid.

5. Pilveteenuse kasutamise põhilised tehnilised nõuded

Kõige olulisemad tehnilised nõuded avalike pilvede kasutamisel on järgmised.

5.1. Andmete hoidmine Euroopa majandusruumis

Pilveteenuse kasutamisel peavad hoitavad andmed igal juhul asuma Euroopa majandusruumis. Seda ka juhul, kui tegemist on avalike andmetega (konfidentsiaalsuse turvaosaklass on S0).

See nõue rakendub ka tarkvarale (SaaS kasutusmudel) ning tähendab, et kasutada tohib vaid selliseid võrgurakendusi ja teenusi, mis tagavad andmete salvestamise Euroopas.

Ülemaailmsete teenuseosutajate haldusliideses peab olema võimalik andmete asukohta valida või piirata. Lepingud ja pilveteenuse osutamise tingimused peavad tagama, et sellest nõudest peetakse kinni.

5.2. Avalikus võrgus andmevahetuse krüpteerimine

Kogu avalikus võrgus toimuv side ning andmevahetus peab olema krüpteeritud. See kehtib kõikidele pilveteenuse andmeside kanalitele - lõppkasutaja tarbitav teenus, teenuse haldus- ja konfigureerimis-liidesed, andmevahetus muude infosüsteemidega jne.

5.3. Salvestatud andmete krüpteerimine

S1 ja S2 salajasusega andmed tuleb pilves salvestamisel krüpteerida.

5.4. Administraatorite kontode tugev autentimine

Pilveteenuse haldusliidese administraatorite kontod on pilveteenuse kõige kontsentreerituma riski allikas. Seetõttu tuleb administraatorite kontod alati turvata kahetasemelise autentimise vahendiga.

5.5. Varundus ja taaste

Tuleb korraldada varukoopiate tegemine teise, sõltumatusse süsteemi. Tuleb veenduda, et pilveteenuse rike või kompromiteerumine ei saaks kaasa tuua kõikide andmete hävimist.

Kui S1 ja S2 salajasusega andmete varukoopiad asuvad ise avalikus pilves, peavad need olema samuti krüpteeritud.

K3 käideldavusega süsteemide korral peab vähemalt üks varukoopia asuma Eesti territooriumil.
Andmete taaste jaoks peab olemas olema taasteplaan ning seda tuleb regulaarselt testida.

5.6. Haldusliideste ligipääsupiirangud

Kui võimalik, tuleb haldus- ja konfigureerimisliideste ligipääs piirata ära ka võrgutasemel. Kui pilveteenuse osutaja seda võimaldab, tuleb seadistada privaatvõrk (VPN) ning kanaliseerida kõik haldustegevused sellesse.

5.7. Riistvaraline võtmehaldus

Kui pilveteenuse osutaja seda võimaldab, tuleb eelistada ja kasutada riistvarapõhist võtmehaldust ning pilveteenuse osutaja soovitatud võtmehalduse vahendeid.
Samas tuleb hädaolukorra lahendamise plaanides ja taasteplaanides arvestada võimalusega, et pilveteenuse osutaja süsteemides asuvad võtmed on kas kättesaadamatud või hävinud.

5.8. Turvaprotsesside uuendamine

Süsteemi turbega seotud protsessid (turvauuendused, seire, intsidentide haldus jne) tuleb pilveteenuse kasutamisel kindlasti üle vaadata, seda eriti DevOps töökorraldusele ülemineku puhul.