TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Informaatikainstituut

IDU70LT

Aarne Vasarik 142019IABM

LOGIDE HALDUSE ANALÜÜS IT ÜHENDASUTUSE NÄITEL

Magistritöö

Juhendaja: Margus Noormaa
MSc
IT asutuse juht
Juhendaja: Ants Torim
PhD
Lektor

Tallinn 2016

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Aarne Vasarik

09.05.2016

Annotatsioon

Täna on riigi IT ühendasutuses peale selle loomist tekkinud olukord, kus on ajalooliselt kasutusel mitmed erinevad logimise meetodid ning lahendused. Need on edasise jätkusuutlikkuse tagamiseks vaja ühtlustada ning selge ja ühtne uus loogika välja töötada. Samuti on probleemne logide suure mahu tõttu logides sisalduva informatsiooni seire ning ei ole rakendatud automaatset logide analüüsi lahendust.

Käesoleva magistritöö eesmärgid:

- Kaardistada edasise analüüsi sisendiks, riigi IT ühendasutuse näitel, kasutusel olevad logimise meetodid, kehtestatud korrad ja juhendid, logisid vajavad osapooled, kitsaskohad ning vajadused.
- Analüüsida seadusandlusest tulenevaid kohustusi, erinevaid logimise tehnilisi lahendusi, raamistikke ja nende vastavusi vajadustele. Sünteesida eelneva põhjal nõuete ja piirangute koondülevaade.
- Välja töötada jätkusuutlik optimaalne logide halduse kontseptsioon, mis rahuldab kõiki osapooli ning arvestab nõuete ja piirangutega.
- Välja töötada kontseptsiooni rakendamise etapiline tegevuskava.

Lõputöö teema on aktuaalne eelkõige konkreetse asutuse logide halduse korrastamise, täpsuse tagamise, mustrite otsingu, muutmiskaitse tagamise, ajatembeldamise jmt osas, kuid on ka rakendatav mujal analoogsete probleemide lahendamiseks.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 57 leheküljel, 5 peatükki, 4 joonist, 2 tabelit.

Abstract

Log Management Analysis by Example of Shared IT Services Centre

Almost every information system or device enables some sort of event logging, but in order to get immediate overview of the events or activities present, the logs must be centrally managed, analysed and archived. In addition, change safety and approval value of the data must be ensured.

Currently there are already some means of log management in use in the Shared IT Services Centre so, the existing solutions implemented in that environment should be considered while creating the new concept. Furthermore, the optimal use of supplementary resources (development and hardware needs, paid external services, etc) will be considered important in developing the improved solution.

At the moment one of the drawbacks is the present situation which arose from combining the institutions with various methods and solutions to logging. These must be homogenized and a clear and common new logic must be created. Another problem is the huge volume of log information and the surveillance of them, neither is there an automated log analysis.

The aims of the current Master's thesis are:

- Map (for the further input) the implemented logging methods, validated procedures and guides, interested stakeholders, drawbacks and needs, based on the example of the Shared IT Services Centre.
- Analyse responsibilities, various technical solutions of logging, frameworks and their suitability for the needs implied by the legislation; based on the information, compile a summative overview of the requirements and restrictions.
- Elaborate a sustainable and optimal log management conception, which would satisfy all the stakeholders and comply with requirements and restrictions.
- Elaborate a step-by-step action plan for the implementation of the conception.

As a result of the thesis a log management conception and its implementation plan will be elaborated.

The research topic is relevant mostly for arranging log management, accuracy, pattern search, modifying prevention, time-stamping, etc. in a specific institution, but the results could also be utilised elsewhere to solve similar problems with log management.

The thesis is in Estonian and contains 57 pages of text, 5 chapters, 4 figures, 2 tables.

Lühendite ja mõistete sõnastik

IHO	IT ühendasutuse infosüsteemide hooldusosakond
ITA	IT ühendasutuse infosüsteemide arendusosakond
ITO	IT ühendasutuse infosüsteemide teenuste osakond
ISKE	Infosüsteemide kolmeastmeline etalonturbe süsteem
ITIL	*Information Technology Infrastructure Library*, infosüsteemide käitlemise parimate praktikate kogu
MFN	IT ühendasutuse mittefunktsionaalsete nõuete dokument
LHJ	IT ühendasutuse logide halduse tehniline juhend
TAJ	IT ühendasutuse turvalise aluskonfiguratsiooni juhend
ISKK	IT ühendasutuse infosüsteemide kasutamise kord
ITP	IT ühendasutuse infoturbepoliitika
SLA	IT ühendasutuse teenustaseme lepingud asutustega
TKJ	IT ühendasutuse töökorralduslikud juhendid
ELOG	IT ühendasutuse elektrooniline logiraamat
RIA	Riigi Infosüsteemi Amet
SSH	*Secure Socket Shell*, turvaline andmevahetusprotokoll
ISP	*Internet Service Provider* ehk interneti teenuse pakkuja
VPN	*Virtual Private Network*, virtuaalne privaatvõrk. Privaatvõrk, mis kasutab avalikku telekommunikatsiooni infrastruktuuri, säilitades samal ajal privaatsuse ja turvalisuse. Turvalisuse tagamiseks kasutatakse tunneldamist ja muid turvaprotseduure.
syslog	Logikannete ülekandeprotokoll
portscan	Järjestikune võrguaadresside või teenuste skanneerimine nõrkuste otsimiseks
IP	Internet Protocol, internetiprotokoll, protokoll ehk reeglistik, mida järgitakse andmepakettide saatmisel ühelt arvutilt teisele üle Interneti
MAC aadress	meediumipöörduse juhtimise aadress. Kohtvõrgus (või mõnes muus võrgus) on MAC-aadress teie arvuti võrgukaardile tootja poolt omistatud unikaalne riistvaranumber

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Peaaegu iga IT süsteem või seade võimaldab mingil kujul logimist. Kuid selleks, et saada operatiivset ülevaadet nendes kajastuvate sündmuste või tegevuste kohta on vaja logisid keskselt hallata, analüüsida ning arhiveerida. Samuti on vajalik tagada muutmiskaitse ja andmete tõestusväärtus.

Töös käsitletaval Riigi IT ühendasutusel endal ning ka asutuse poolt teenindatud institutsioonidel on palju erinevaid kohustusi ja nõudeid, mis tulenevad sisemistest kordadest ja juhenditest, kuid ka mitmeid, mida juhitakse seaduste ja määrustega. IT ühendasutuse logimiskontseptsiooni loomisel tuleb arvestada ka mõnevõrra keerukama ülesandega kui ühe kindla asutuse raames teostatava kontseptsiooni loomisel, kuna tagasiulatuvalt on kasutusel olnud palju erinevaid lahendusi ning parimaid praktikaid. Osaliselt on logimisega seonduv juba konsolideeritud, kuid osaliselt veel lahus. Kuna IT asutuse haldusalas olevad institutsioonid teenindavad väga suurt ja olulist osa riiklike teenuste pakkumisel siis on ilmselgelt logimisvõimekus ka väga oluline aspekt. Üheltpoolt on see seadusandlikult reguleeritud (viited vabariigi valituse seadustele ja määrustele on toodud töö analüüsi osas) ning teiselt poolt on vaja leida ja lahendada kitsaskohad käideldavusega seonduvalt teenuste teenustasemel toimimise tagamiseks võimalikult operatiivselt. Seda kõike saab parandada kvaliteetse logide halduse kontseptsiooni rakendamisega.

Hetkel on käsitletavas IT ühendasutuses juba kasutusel mõningad meetmed logide halduseks ning olemasolevas keskkonnas rakendatud lahendusi tuleb võimalusel arvestada ka kontseptsiooni loomisel. Samuti on täiendavate ressursside (arendusvajadus, riistvara vajadus, tasulised teenused jmt) optimaalne kasutus tähtsal kohal lahenduse väljatöötamisel.

Käesoleva töö eesmärk on analüüsida olemasolevat logide haldust, tehnilisi vahendeid ning luua IT ühendasutusele jätkusuutlik logide halduse kontseptsioon. Töö raames püstitatakse nõuded ja piirangud tuginedes parimatele praktikatele, seadusandlusele,

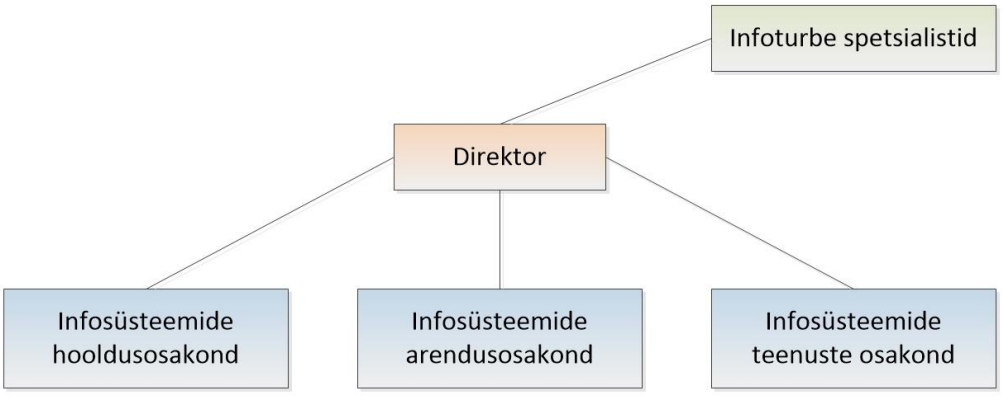
juba kehtestatud kordadele ja juhenditele ning analüüsitakse ja kaalutakse antud nõuete ja piirangute rakendatavust. Luuakse ka kontseptsiooni rakendamise kava.

Töö käsitlusalasse kuulub ärirakenduste (allasutuste äriliseks toimimiseks vajalikud spetsiifiliselt selleks otstarbeks arendatud sisemised- ning välisteenused) ning nende infrastruktuuris toimuva logimise halduse analüüs.

Käsitlusalasse ei kuulu tarkvaralise analüüsivahendi lõplik analüüs ja valik. Vahendile püstitatakse töö käigus nõuded, mida edasisel valikul järgida. Ei käsitleta ka täpseid tehnilisi seadistusi ning konfiguratsioone, nende olemasolule viidatakse üldistades. Töös ei käsitleta valmisrakendusi (valmis kommertstooteid), milledel on reeglina juba sisse ehitatud põhjalik audit funktsionaalsus. Samuti ei käsitleta töös tööjaamade ja neid teenindava infrastruktuuri tasemel logimist (v.a võrgusegmentides toimuv). Käsitlusalast välja jäänud teemasid käsitletakse IT ühendasutuses eraldiseisvalt ning vajadusel lisatakse loodavasse logide halduse kontseptsiooni vastavad täiendused edaspidi.

2 Hetkeolukorra kirjeldus

Viis aastat tagasi loodi ministeeriumi valitsemisala asutuste IT lahenduste haldamiseks üks keskne IT asutus. Formaalselt liideti kõik süsteemid, praktikad ning lahendused, samuti personal ja alustati konsolideerimisega. IT asutuse üldine ülesehitus on võrdlemisi lihtne: asutuse direktorile alluvad kolm osakonda ning infoturbe spetsialistid (Joonis 1).



Joonis 1. Riigi IT ühendasutuse üldstruktuur.

Osakondade vastutusalad on:

- Infosüsteemide hooldusosakond (IHO) – vastutab teenuste, süsteemide ja infrastruktuuri käigus hoidmise eest.
- Infosüsteemide arendusosakond (ITA) – vastutab IT sisearenduste, projektijuhtimise ning analüüsi teemade eest.
- Infosüsteemide teenuste osakond (ITO) – vastutab kasutajatoe, töökohateenuse ja IT teenuste halduse eest.

Täna pakub ühendasutus IT täisteenust seitsmele (ca 3000 töötajaga) riigiasutusele ning kogu haldusalas on kasutusel väga palju erinevaid rakendusi ja andmekogusid, mille puhul tekib operatiivselt suurel hulgal logitud informatsiooni. Käesolevast tööst selgub, et kõikidel IT asutuse osakondadel on selged piirid ja vastutusalad ka infosüsteemide logimisega seonduvalt.

Hetkel on logide maht väga suur (igapäevane logide maht on kümnetes gigabaitides) ning selles leiduva informatsiooni analüüs on väga aeganõudev ja inimese poolt reeglina haldamatu protsess. Andmed on tihti dubleeritud ning mitmed süsteemid logivad samu sündmusi. Huvitatud osapooli logides leiduva informatsiooni tarbimiseks on mitmeid ning kõigil on erinevad vajadused erinevatel logimise tasemetel ja erinevates süsteemides. Sellisel kujul jätkamine ei ole enam jätkusuutlik, sest seoses valitsemisala laienemisega on mahtude kasvu tõttu edaspidi oht erinevaid logimisega seotud kohustusi mitte täita. Et tagada senisest kiirem ja selgem logide haldus, on vaja põhjalikku analüüsi ja vajaduste kaardistust, mille alusel juurutada jätkusuutlik logide halduse kontseptsioon.

IT ühendasutuse poolt osutatava IT teenusega kaetud asutustes on rakendatud infosüsteemide kolmeastmeline etalonturbe süsteem (edaspidi ISKE), millest tulenevalt on väga suur osa logimisega seotud nõudeid ja soovitusi reguleeritud ISKE rakendamise juhendiga. Samuti on IT ühendasutuses parimatest praktikatest rakendatud ITIL raamistikul põhinevad protsessid – intsidendihaldus, probleemihaldus ja muudatuste haldus, milledesse logidest tulenevalt juba saadakse sisendeid. Kui IT asutus plaanib tulevikus laiemalt kasutusele võtta ka ITIL sündmuste halduse protsessi juurutamise siis on väga olulisel kohal monitooringu ja sündmuste sisendite andmisel ka logide haldus.

Käesolevas töö osas kirjeldatakse juba tehtud tegevusi, rakendatud juhendeid ja kordasi, selgitatakse välja huvitatud osapooled ning tuuakse välja suurimad probleemid.

2.1 Logide halduse korraldus IT ühendasutuses

Asutuste logimisloogika konsolideerimise käigus on loodud ühtsed korrad ja juhendid ning rakendatud hulk tegevusi logimise paremaks korraldamiseks.

IT ühendasutuses on kasutusel järgmised olulisimad logimist reguleerivad korrad ja juhendid:

- Mittefunktsionaalsete nõuete dokument (**MFN**) – väljastatakse arendajatele uute süsteemide väljatöötamisel või vanade süsteemide suurema kaasajastamise korral. Tegu on IT ühendasutuse sisemise dokumendiga, mida ei ole võimalik käesoleva töö raames täies mahus lisada. Vastavast dokumendist on logimisega seotud informatsioon tsiteeritud ja analüüsitud [1];

- Logide halduse tehniline juhend (**LHJ**) – kirjeldab tehnilisi metoodikaid logide salvestamise ning roteerimise kohta, samuti logiserverlahenduse tehnilist kirjeldust. Tegu on IT ühendasutuse sisemise dokumendiga, mida ei ole võimalik käesoleva töö raames täies mahus lisada. Vastavast dokumendist on logimisega seotud informatsioon tsiteeritud ja analüüsitud [2];
- Turvalise aluskonfiguratsiooni juhend (**TAJ**) – reguleerib kasutusele võetavate seadmete ja serverite seadistamist, (sisaldab alajaotusi erinevatele võrguseadmetele, erineva operatsioonisüsteemiga serveritele ning kettamassiivlahendustele). Tegu on IT ühendasutuse sisemise dokumendiga, mida ei ole võimalik käesoleva töö raames täies mahus lisada. Vastavast dokumendist on logimisega seotud informatsioon tsiteeritud ja analüüsitud [3];
- Infosüsteemide kasutamise kord (**ISKK**) – kehtestab reeglid infosüsteemide kasutamise kohta, sisaldab juhiseid logide osas ligipääsu ja väljastamise kohta. Tegu on IT ühendasutuse sisemise dokumendiga, mida ei ole võimalik käesoleva töö raames täies mahus lisada. Vastavast dokumendist on logimisega seotud informatsioon tsiteeritud ja analüüsitud [4];
- Infoturbepoliitika (**ITP**) – raamistik infoturbe korraldamiseks valitsemisalas, kehtestab vajaduse logimisele, turvaintsidentide uurimise raames. Tegu on IT ühendasutuse sisemise dokumendiga, mida ei ole võimalik käesoleva töö raames täies mahus lisada. Vastavast dokumendist on logimisega seotud informatsioon tsiteeritud ja analüüsitud [5];
- Teenustaseme lepingud asutustega (**SLA**) – käsitlevad konkreetsete teenuste, rakenduste ja varundusvajaduste kokkuleppeid allasutustega. Tegu on IT ühendasutuse sisemise dokumendiga, mida ei ole võimalik käesoleva töö raames täies mahus lisada. Vastavast dokumendist on logimisega seotud informatsioon tsiteeritud ja analüüsitud [6];
- Töökorralduslikud juhendid (**TKJ**) – kirjeldavad töökorraldust, kus on ka viide erinevaid süsteeme haldavatele isikute loetelule. Tegu on IT ühendasutuse sisemise dokumendiga, mida ei ole võimalik käesoleva töö raames täies mahus lisada. Vastavast dokumendist on logimisega seotud informatsioon tsiteeritud ja analüüsitud [7].

Täpsemalt on eelpool loetletud dokumentides käsitletud logimisega seotud teemad toodud punktide kaupa töö analüüsiosas, kus iga logimisele rakendatud tingimust, nõuet või piirangut selgitatakse ja analüüsitakse.

Kõik ärirakendusi teenindavad serverid (koormusjaoturid/veebifrondid, rakendusserverid, andmebaasiserverid), võrguseadmed (tulemüürid, marsruuterid, kommutaatorid) ning muud olulised nendega seotud seadmed (SAN võrk, kettamassiivid) logivad olulisi seadmete, operatsioonisüsteemide ning rakenduste (rakendusserveri tarkvara, erinevad veebirakendused, andmebaasid jmt) tehnilisi sündmusi. Info turvalise aluskonfiguratsiooni kohta on toodud TAJ-s ning hilisema seadistuse käigus tehtav logide konfigureerimine ja tehniline lahendus on dokumenteeritud LHJ-is. Logisid koondatakse osaliselt kesksetesse logiserveritesse, kuhu on osapooltel (välised partnerid, asutuste sisekontrolliüksused – täpsemalt toodud osapooli kirjeldavas peatükis 2.2) tagatud ligipääs. Osadel süsteemidel on logid siiski ka ainult seadmes endas eraldiseisvalt. Mõne keerukama sündmuse otsimine on raskendatud, kuna peab mitmetel seadmetel logisid analüüsima ning nendevahelisi seoseid otsima käsitsi.

Rakendusserveritel toimivad rakendused ning andmebaasi äriloogikaga seotud rakendused logivad vastavalt MFN-is kirjeldatud juhistele.

Samuti on täpsemaks analüüsiks tarvilikud andmestikud veel:

- Elektrooniline logiraamat (**ELOG**) – kirjeldatakse oluliste teenuskomponentide muudatused ja võimalikud seosed vastava muudatuse teostaja poolt;
- Tööaja info – personalisüsteemist on võimalik saada vastava tarkvaraliidese abil asutuste puhkuste ning eemalolekute info.

Lisaks süsteemsetele logimismehhanismidele on kasutusel muudatuste jälgimiseks ELOG, millest saab samuti tulla seos süsteemi muudatuse ning logis kajastuva vahel.

Samuti on mustrite jälgimisel vajalik rakendada logide analüüsiks ametnike tööaega sisaldavaid andmeid. Osalt on need võimalik olemasolevatest süsteemidest saada, osalt tuleb lahendus välja töötada (näiteks inimeste tööl olemise vahetuste info jms).

Osaliselt rakendatud on ITIL sündmuste halduse protsess mille sisendiks on muuhulgas logide analüüsist tulenevalt protsessi sisendi andmine. Rakendatud on rakenduste (java

rakendused, andmebaasipäringud) siseelu monitooringlahendus, mis tugineb sisemise logimise analüüsile ja mustrite otsingule. Lisaks on rakendatud ka süsteemide monitooringuks IT asutuse tarbeks kohandatud vahend, mis tagab monitooringuinfo asjakohasuse alates serveriruumi sisekliima monitooringust lõpetades seadmete ressursside täituvuse jälgimisega.

2.2 Huvitatud osapooled

Kuna logisid kasutatakse mitmetel erinevatel põhjustel siis on ka huvitatud osapooled väga erinevate nõudmistega.

Tehniliste huvidega, näiteks süsteemide käideldavus, probleemide otsing jmt vajadustega, osapooled on alljärgnevad:

- **Süsteemiadministraatorid** – vajavad logisid seadmete ja serverite halduse paremaks tagamiseks ning vigade tuvastamiseks:
    - Linux süsteemiadministraatorid – Operatsioonisüsteemilogid ja vajadusel ka rakenduste süsteemsed logid;
    - Süsteemide administraatorid – Halduses olevate süsteemide ja rakenduste (veebilahendused, rakendusserverid, andmebaasid jmt) süsteemsed logid;
    - Võrguadministraatorid – Võrguseadmete logid ja seosed erinevate seadmete logide vahel.
- **Rakendusadministraatorid** – vajavad rakenduste logisid vigade analüüsiks ja tuvastamiseks.

Infoturbe eest vastutavad osapooled:

- **Infoturbe spetsialistid** – vajavad logisid tegevuste tuvastamiseks süsteemides ning kasutus- ja käitumismustrite analüüsimiseks.

Äripoole osapooled:

- **Asutuste sisekontrolliüksuse ametnikud** – vajavad logisid mustrite tuvastamiseks ja järelanalüüsiks inimeste tegevuste tuvastamisel, samuti ka välistele õiguskaitseorganite päringutele vastamiseks.
- **Asutuste ametnikud** – vajavad rakenduste tegevuslogisid teabepäringutele vastamise tagamiseks.

2.3 Logide haldamisega seotud probleemid

Logisid on süsteemide lõikes täna reeglina liialt palju, andmestik on mõnes osas dubleeritud, seosteta ning puudub sügavam analüüsivõimekus. See omakorda on tinginud olukorra, kus inimese poolt tehes muutub haldamine kas liiga ajamahukaks või on isegi teostamatu etteantud ajaraamis (näiteks teabenõudele reageerimine on nõutud viie tööpäeva jooksul). Samuti on selge, et inimene ei suuda väga paljude erinevate andmete pealt süsteemide kasutusmustreid kokku panna (näiteks inimese tööaja ja rakenduse/töövahendi kasutamise võrdlus jmt).

Põhilised logide haldusega seonduvad probleemid:

- **Logitavaid süsteeme on palju** ja süsteemide lõikes on vajadused reguleerimata. Logitakse pigem kõike, mis omakorda on lisamaht ning mida osapooled ei vaja. Samas tuleb neid siiski aegajalt töödelda ja käidelda ning regulaarselt varundada;
- Tihti on erinevates **logides kajastuvad sündmused dubleeritud**. Samu sündmusi käsitletakse mitmes erinevas logis, enamasti ei ole see aga tarvilik;
- Erinevate süsteemide ja seadmete **logimise meetodid ja logikujud on väga erinevad**;
- Huvitatud **osapoolte vajadused on erinevad** ja tihti on vaja ligipääse mitmetesse kohtadesse, et tagada ligipääs vajalikele logidele. Kogu oluline logide kogumine ei ole konsolideeritud logiserveritesse;
- Kuna **logid on** erinevates süsteemides **hajutatud ja formaat ebaühtlane** siis on mingi konkreetse sündmuse või seose otsimine väga ajamahukas;
- **Puudub mitmete** (osaliselt rakendatud) **logide tervikluse ja muutmiskaitse tagamise kontroll** (krüptoaheldamine, ajatembeldamine);
- **Puudub automaatne halduse ja analüüsivahend**, mis tagaks järgneva:
    - Analüüsist tulenevate eelseadistatud hoiatuste peale aktiveerumine ja teavitamine (näiteks kahtlane normaalsest kõrvalekalduv tegevus mõnes infosüsteemis);
    - Vaatleja õiguste jagamise kindlate logide lõikes;
    - Asutuste monitooringusüsteemidesse logidest tulenevate sisendite andmise;

- Võimalusel ka mustrite otsimise võimekuse vastavalt eeldefineeritud reeglitele üle mitmete logide või muude etteantud sisendite (tööajatabel, inimeste asukoht vms).

3 Logihalduse analüüs

Antud töö osas analüüsib autor etapiti edasistes alampeatükkides toodud logihaldusega seotud teemasid, põhjendab ning kirjeldab kasutatavaid logide haldamise metoodikaid. Analüüs on teostatud kompleksmeetodil, kus sisenditeks on nii varasemad teemakohased teadustööd, riigi seadusandlus, asjakohased raamistikud ning hetkel IT asutuses juba toimivad parimad praktikad.

3.1 Nõuded ja piirangud

Antud töö osas kirjeldatakse nõuded valdkonniti ja analüüsitakse ühisosi. Nõudeid ja piiranguid on mitut tüüpi - seadusandlusest tulenevad, turvateemalised, tehnilised, sisekordadest ja juhenditest tulenevad ning osapoolte vajadustest tulenevad. Järgnevates alajaotustes kirjeldatakse neid põhjalikumalt, viidatakse vajadusele, soovitusele või vastavas dokumendis kehtestatule. Samuti analüüsitakse nõude või piirangu käsitlemise staatust (rakendatud, rakendamisel, rakendamata).

Nõuete ja piirangute tekkimine on kirjeldatud igas alampeatükis vastavalt sisenditüübile, tähistatud unikaalse tähisega ning toodud koondtabelina valdkonnapõhiselt grupeerituna peatüki lõpus.

3.1.1 Seadusandlusest tulenevad nõuded ja piirangud

IT ühendasutus on riigiasutusi teenindav asutus ning seoses sellega on ka rakendatud mitmeid seaduslikke regulatsioone, et tagada riigi tõrgeteta ning turvaline toimimine. Antud alapeatükis käsitleb autor seadustest ja määrustest tulenevaid nõudeid ja piiranguid mis logide halduse kontseptsiooni loomisel on vaja täita.

ISKE

Üheks suurimaks logimise nõudeid ja piiranguid käsitlevaks raamistikuks on infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE), mis on vastavalt Vabariigi

Valitsuse määruses nr 252 kehtestatule riigiasutustel andmekogudele kohustuslik rakendada. Antud määruses on öeldud:

§ 2. Turvameetmete süsteemi rakendamine

Turvameetmete süsteemi rakendamine seisneb infoturbe eesmärkidele vastavate turvaklasside määramises ja nendele vastavate turvameetmete valimises vastavalt infosüsteemide kolmeastmelise etalonturbe süsteemi (edaspidi ISKE) rakendamisjuhendile ja nende rakendamises ning rakendamise auditeerimises [8].

ISKE dokumentatsiooni ja juhendmaterjale koondab ja uuendab Riigi Infosüsteemi Amet (RIA), kes kirjeldab ISKE-t järgnevalt:

ISKE väljatöötamisel ja arendamisel on aluseks võetud Saksamaa BSI (saksa k. Bundesamt für Sicherheit in der Informationstechnik, inglise k. Federal Office for Information Security) avaldatav infoturbe standard – IT Baseline Protection Manual (saksa k. IT-Grundschutz).

ISKE rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. Süsteem on loodud eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks [9].

ISKE rakendamiseks on loodud rakendusjuhend, kus on kirjeldatud ISKE rakendamise meetmed ning suunised ja ettepanekud meetmete paremaks rakendamiseks [10].

Alljärgnev nõuete analüüs on rakendusjuhendi meetmete põhjal tehtud logimisega seotud nõuete loetelu, kus analüüsis on käsitletud nendest olulisimad (näiteks ei ole käsitletud kõiki samaliigilisi) logimist puudutavad lõigud (üldnõuded, võrk, serverid, rakendused, muud seotud seadmed) ning on, analüüsitud soovitusi ja kontrollküsimusi. Kuna IT ühendasutuse klientasutused ei oma andmekogusid, mis vajaksid kõrge turbeastme (H) meetmete rakendamist siis käsitletakse meetmeid tasemega madal (L) kuni keskmine (M). Autor analüüsib meetmeid ning soovitusi, et järgnevalt koostada nõuete ja piirangute kooslus meetmete rakendamisel. Samuti tuuakse välja tehtud tegevustega juba kaetud nõuded ja piirangud. Iga meetme juures toodud kirjeldus on autori kokkuvõte meetmes käsitletavast logimisega seotud osast.

B 5.22 – Logimine

Meede annab üldised suunised alates planeerimisest kuni kasutusest kõrvaldamiseni, viitab paljudele alltoodud meetmetele ning aitab suunata lahenduseni, mis hõlmab kogu valdkonda. Suunistega on arvestatud ning toodud alamkomponentide valikuga arvestatakse edasises analüüsis.

M 2.64 - Logifailide kontroll

Meetmes toodud logide seire ning administraatori tegevuste kontrolli suunised on osaliselt rakendatud kuid käsitsi tegevuste või skriptidega. Tagamaks paremat nõude täitmist on vaja tagada analüüsivahendi rakendamine (**ISKEN1**).

M 2.83 – Tüüptarkvara testimine

Meede käsitleb tarkavara kasutuselevõtul logimise seadistamise reguleerimist ning kontrolli. Hetkeseisuga on seadistamine tagatud MFN ning LHJ dokumentides sätestatuga, kuid pole tagatud kõigi logide muutmiskaitse rakendamine. Paremaks nõude tagamiseks on vaja rakendada muutmiskaitse (**ISKEN2**).

M 2.110 – Andmeprivaatsuse suunised logimisprotseduurides

Meede käsitleb logides kajastatavate oluliste sündmuste detailsemat logimist ning juhiseid nende tagamiseks. Osaliselt on teemad käsitletud juba kehtestatud juhendites kuid paremaks tagamiseks tuleb LHJ kaasajastada (**ISKEN3**).

M 2.133 – Andmebaasisüsteemi logifailide kontroll

Meetmes on toodud suunised andmebaasides toimuva logimise kohta. Praeguseks on rakendatud oluliste sündmuste audit informatsiooni kogumine. Vaja on andmed tõsta logiserverile, et tagada samade isikute halduses olevate seadmete lahusus. Samuti on vaja tagada logide täiendav seire ning analüüs (**ISKEN4**).

M 2.215 – Tõrkekäsitlus

Meede annab suunised tagamaks erinevatest infosüsteemides toimuvatest intsidentidest ning muudatustest sündmuse kohta jääva kande. Andmeid saab kasutada ka logide analüüsis. Hetkeseisuga on rakendatud ELOG kuid sealseid logikandeid kasutatakse

ainult manuaalseks seireks. Vajalik on rakendada automatiseeritud analüüsivahend (**ISKEN5**).

M 2.262 - Arhiivisüsteemide kasutamise reguleerimine

Meede käsitleb arhiivisüsteemide ja selle kasutajate sündmuste logimist. Meetmes toodud nõuded on täidetud vastava süsteemi seadistamisjuhendis (TAJ) ning logimine on reguleeritud LHJ-s (**ISKEN6**).

M 2.279 - Marsruuterite ja kommutaatorite turvapoliitika koostamine

Meede käsitleb marsruuterite ja kommutaatorite turvapoliitikas nõutud sündmuste kajastamise logimisvajadusi. Meetmes toodud nõuded logimisele on täidetud vastava süsteemi seadistamisjuhendis (TAJ) ning logimine on reguleeritud LHJ-s (**ISKEN7**).

M 2.280 - Sobivate marsruuterite ja kommutaatorite ostmis- ja valimiskriteeriumid

Meetmes selgitatakse vajadust valida vastav võrguseade järgides asutuse erinõudeid ning andmekaitsest tulenevaid nõudeid. Vastavad nõuded on täidetud ja dokumenteeritud TAJ-s (**ISKEN8**).

M 2.299 - Turvalüüsi (tulemüüri) turvapoliitika koostamine

Meede käsitleb tulemüüri turvapoliitikas nõutud sündmuste kajastamise logimisvajadust. Meetmes toodud nõuded logimisele on täidetud vastava süsteemi seadistamisjuhendis (TAJ) ning logimine on reguleeritud LHJ-s (**ISKEN9**).

M 2.315 - Serveri kasutuselevõtu planeerimine

Meetmes käsitletakse serveri süsteemsete sündmuste logimise planeerimist. Antud tegevus on tehtud, TAJ-s kirjeldatud ning logide haldus on reguleeritud LHJ-s (**ISKEN10**).

M 2.316 - Serveri turvapoliitika kehtestamine

Meetmes käsitletakse serveri ja selle kasutajate sündmuste logimise planeerimist. Antud tegevus on tehtud, TAJ-s kirjeldatud ning logide haldus on reguleeritud LHJ-s (**ISKEN11**).

M 2.419 - Sobivate VPN-toodete valimine

Meetmes selgitatakse vajadust valida vastav võrguseade järgides asutuse erinõudeid ning andmekaitsest tulenevaid nõudeid. Vastavad nõuded on täidetud ja dokumenteeritud TAJ-s (**ISKEN12**).

M 2.496 - Logimisserveri korrakohane kasutusest kõrvaldamine

Meetmes käsitletakse logiserveri käigust kõrvaldamise puhul andmekandjatelt andmete hävitamist. Antud meede on täidetud asutuse varade halduse korras kehtestatud tingimusega, et andmekandjad eemaldatakse seadmetest ning hävitatakse eraldi protsessi kasutades (**ISKEN13**).

M 2.497 - Logimise turbekontseptsiooni koostamine

Meetmes käsitletakse tsentraalse logiserveri turbekontseptsiooni ning paiknemist võrgutsoonis, samuti aja sünkroniseerimist. Antud kontseptsioon on juba eelnevalt loodud ja kuulub LHJ koosseisu (**ISKEN14**).

M 2.499 - Logimise planeerimine

Meede käsitleb kogu logimist hõlmava kontseptsiooni loomist, mis on ühtlasi ka antud töö eesmärk. Lisaks veel ka logiserveri tehnilist platvormi ning haldusloogikat. Osad tehnilised sammud on tehtud, juhendites ja kordades on kehtestatud nõuded ning toodud erinevad meetodid logihalduseks. Puudub süstematiseeritud logihalduse kontseptsioon. Antud magistritöö eesmärkide täitmine täidab ka selle meetme nõuded (**ISKEN15**).

M 2.500 - IT-süsteemide logimine

Antud meetmes toodud suunised tuginevad suures osas terviklikule logihalduse kontseptsioonile, mis on eelmise nõude all toodult loomisel. Antud nõue saab täidetud kui kontseptsioon on valmis. Hiljem saab kontseptsioonis määratud meetmeid kasutada erinevat tüüpi IT süsteemide logimise korraldamisel (**ISKEN16**).

M 3.90 - Tsentraalse logimise põhitõed

Logimise metoodikaid kirjeldav meede, mida tuleb silmas pidada logide halduse kontseptsiooni luues. Osaliselt on erinevad meetme suunised rakendatud, kuid ühtse

kontseptsiooni loomise käigus tuleb veel kasutusele mõningaid rakendamata osasid (**ISKEN17**).

M 4.25 - Logimine Unix-süsteemis

Meetme sisu on vastava serversüsteemi varunduse suuniste andmine. Antud teema on kaetud TAJ-s ja LHJ-s kehtestatuga (**ISKEN18**).

M 4.41 - Sobivate IT-süsteemide turvatoodete valimine

Meetme sisu on administreerimistegevuste logimise vahendi valik ning analüüsivahendi valik. Meetme täitmiseks on tarvilik rakendada logide analüüsivahend (**ISKEN19**).

M 4.47 - Turvalüüsi operatsioonide logimine

Meede käsitleb turvalüüsi ja selle kasutajate sündmuste logimist. Meede on täidetud TAJ-s kehtestatuga ning logihaldus on reguleeritud LHJ-s (**ISKEN20**).

M 4.81 - Võrgutoimingute audit ja logimine

Meede käsitleb võrguliikluse ja selle kasutajate sündmuste logimist. Meede on täidetud TAJ-s kehtestatuga ning logihaldus on reguleeritud LHJ-s (**ISKEN21**).

M 4.205 - Marsruuterite ja kommutaatorite töö logimine

Meede käsitleb marsruuterite ja kommutaatorite ning nende kasutajate sündmuste logimist. Meede on täidetud TAJ-s kehtestatuga ning logihaldus on reguleeritud LHJ-s (**ISKEN22**).

M 4.225 - Logiserveri kasutamine turvalüüsis

Meetmes on toodud logiserveri turvalisse võrgusegmenti paigalduse soovitused, liiasusega salvestamise soovitus jmt. Logiserverid on paigaldatud vastavalt TAJ-s ja LHJ-s toodule ning salvestusmeedia liiasus ning varundus on tagatud vastavalt asutuse varunduskorrale (**ISKEN23**).

M 4.320 - VPNi turvaline konfigureerimine

Meede käsitleb VPN seadmete ja nende kasutajate sündmuste logimist. Meede on täidetud TAJ-s kehtestatuga ning logihaldus on reguleeritud LHJ-s (**ISKEN24**).

M 4.397 - Veebirakenduste turvet puudutavate sündmuste logimine

Meede käsitleb veebirakenduste sündmuste detailset logimist. Osalt on kirjeldatud NFR-s, osalt on vaja kirjeldada teenusserverite seadistamise sektsioonis TAJ-s (**ISKEN25**).

M 4.430 - Logiandmete analüüs

Meede annab suunised analüüsivahendi valiku teostamiseks. Logihalduse kontseptsiooni loomine käsitleb antud suuniseid ning analüüsivahendi rakendamine tagab meetme parema täitmise. Hetkeseisuga on suunised kaetud käsitsi ja skriptide poolt tehtava analüüsiga (**ISKEN26**).

M 4.431 - Logimise jaoks oluliste andmete valik ja töötlemine

Meetmes käsitletakse kontseptsiooni loomiseks vajalikke suuniseid andmekoosseisu ning prioriteetide kohta. Meede on paremini kaetud kui kogu logimisvajadus on dokumenteeritud ja reguleeritud, samuti on keerulisemate seoste loomiseks ja jälgimiseks tarvilik rakendada analüüsivahend. Hetkel on dokumentatsioon hajutatud mitmetesse kohtadesse ning puudub üks ja ühtne kontseptsioon (**ISKEN27**).

M 5.171 - Turvaline andmeside keskse logiserveriga

Meetme käsitluses on logiandmete liigutamine kesksele serverile üle turvalise kanali ning muutmiskaitse tagamine. Hetkel on logide liigutamine teostatud kasutades turvalist kanalit (SSH) ning see on dokumenteeritud LHJ-s. Vaja on rakendada muutmiskaitse lahendus kõikidele logidele (**ISKEN28**).

M 5.172 - Turvaline aja sünkroniseerimine keskse logimise korral

Meede käsitleb vajadust kõikide logiserveritele (server kaasaarvatud) sisendit andvate seadmete kellaaeg sünkroniseerida kindla ja ühtse allika vastu. Antud meede on täidetud TAJ-s toodud nõudega sünkroniseerida kõikide seadmete kellaaeg välise internetiteenusepakkuja (ISP) ajaserveri teenusega (**ISKEN29**).

M 5.9 - Serveri logi

Meede käsitleb serverite süsteemsete sündmuste logimise suuniseid, et oleks tagatud kasutajatunnusega seonduvad sisselogimiskatsete, süsteemsete veateadete ning ülekoormusteadete logimised. Antud meede on tagatud TAJ-s kehtestatuga (**ISKEN30**).

M 6.151 - Logimise häirepoliitika

Meetme käsitluse all on logimisanalüüsi tulemusel tekkivate häirete protsessi kirjeldamine. Antud meetme täitmiseks on vaja rakendada logide analüüsisüsteem (**ISKEN31**).

Vabariigi Valitsuse seadused ja määrused.

Tagamaks logimislahenduse vastavuse kõikvõimalikele seadusest tulenevatele logimist puudutavatele nõuetele on ISKE rakendamisega seotult enamust neist käsitletud, autor toob siinkohal mõned näited (loetelu ei ole täielik) logimiskohustusest, mille kohta võib tulla teabepäringuid ning mille vastavasisulised logid peavad olema tagatud.

Avaliku teabe seadus.

§ 43. Asutusesisese teabe kaitse

(1) Teabevaldaja peab rakendama organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid, et kaitsta asutusesisese teabe:

1) terviklust – juhusliku või tahtliku volitamata muutmise eest;

2) käideldavust – juhusliku hävimise ja tahtliku hävitamise eest ning õigustatud isikule andmete kättesaadavuse takistamise eest;

3) konfidentsiaalsust – juhusliku või tahtliku volitamata juurdepääsu eest.

§ 45. Andmekaitse Inspektsiooni järelevalvepädevus

(1) Andmekaitse Inspektsioon teostab teabevaldajate üle riiklikku ja haldusjärelevalvet nende poolt:

3) andmekogude asutamisel, kasutuselevõtmisel, pidamisel, ümberkorraldamisel ja lõpetamisel.

§ 531. Riigi Infosüsteemi Ameti järelevalve

(1) Riigi Infosüsteemi Amet teostab haldus- ja riiklikku järelevalvet infosüsteemide turvameetmete süsteemi rakendamise ning infosüsteemide andmevahetuskihiga liitumise üle [11].

Infoühiskonna teenuse seadus.

§ 11. Jälgimiskohustuse puudumine

(4) Teenuse osutaja peab esitama prokuratuurile ja uurimisasutusele tõe tuvastamiseks kriminaalmenetluse seadustikus ettenähtud alustel ja korras ning julgeoleku- ja jälitusasutusele seaduses ettenähtud alustel ja korras nende määratud tähtajaks olemasolevat teavet teenuse kasutaja kohta, kellele ta osutab andmete talletamise teenust.

(5) Teenuse osutaja peab esitama kohtule tema kirjaliku üksikpäringu alusel tõe tuvastamiseks tsiviilkohtumenetluse seadustikus ettenähtud alustel ja korras ning kohtu määratud tähtajaks olemasolevat teavet teenuse kasutaja kohta, kellele ta osutab andmete talletamise teenust. Üksikpäring käesoleva paragrahvi mõttes on päring teenuse kasutaja isikuandmete ja teenuse kasutaja edastatud teabe edastamise fakti, kestuse, viisi ja vormi kohta seoses konkreetse elektronkirja, konkreetse elektroonilise kommentaari või muu üksiksõnumi edastamisega seotud sideseansiga [12].

Infosüsteemide andmevahetuskihi määrus.

§ 19. Tehnilised ja andmeturbenõuded

(4) Talitlusteenuse päringud logitakse teenuse osutaja infosüsteemi turvaserveris ja vastused päringu sooritanud X-tee osalise infosüsteemi turvaserveris [13].

Maksukorralduse seadus.

§ 26. Maksusaladuse kaitse

(1) Maksuhaldur, tema ametnikud ja töötajad on kohustatud hoidma saladuses maksukohustuslast puudutavat teavet, sealhulgas kõiki andmekandjaid (otsused, aktid, teated ja muud dokumendid) maksukohustuslase kohta, teavet andmekandjate olemasolu

kohta, äri- ja pangasaladust, mida nad teavad seoses maksude tasumise õigsuse kontrollimise, maksu määramise, maksuvõla sissenõudmise, maksuõigusrikkumise asja menetlemise või muude teenistus- või töökohustuste täitmisega (edaspidi maksusaladus) [14].

Finantsinspektsiooni seadus.

§ 2. Riiklik finantsjärelevalve ja kriisilahendamine

(1) Riiklik finantsjärelevalve (edaspidi finantsjärelevalve) käesoleva seaduse tähenduses on järelevalve riikliku finantsjärelevalve subjektide (edaspidi finantsjärelevalve subjekt) üle ning käesolevas seaduses, krediidiasutuste seaduses, krediidiandjate ja -vahendajate seaduses, kindlustustegevuse seaduses, investeerimisfondide seaduses, kogumispensionide seaduses, väärtpaberituru seaduses, liikluskindlustuse seaduses, makseasutuste ja e-raha asutuste seaduses ja Eesti väärtpaberite keskregistri seaduses ning nende alusel kehtestatud õigusaktides sätestatud tegevuse üle.

§ 481. Inspektsiooni abistamise kohustus

(1) Riigiasutused ja kohaliku omavalitsuse üksused on oma pädevuse piires kohustatud Inspektsiooni abistama.

(2) Inspektsioonil on õigus tutvuda kriminaalmenetluses ning väärteoasja menetluses kogutud tõenditega, mis viitavad käesoleva seaduse § 2 lõikes 1 nimetatud õigusakti rikkumisele [15].

3.1.2 Sisemistest kordadest ja juhenditest tulenevad nõuded ja piirangud

IT ühendasutuses on mitmed olulised kehtestatud sisemised korrad ning juhendid (loetletud peatükis 2.1) milledest tulenevad logimisele erinevad tehnilised ning korralduslikud nõuded. Autor toob iga korra ja juhendi kohta eraldi välja vastavad nõuded koos selgitustega.

Mittefunktsionaalsete nõuete dokument (MFN)

- *Rakendus peab logima sessiooni algamise ja lõppemise, kasutaja IP, autentimismeetodit (ID-kaart, mobiil-ID vms), eduka autendi puhul tuleks logida*

ka kasutaja isikukood ja mobiil-ID puhul telefoninumber. Turva logi peab olema võimalik suunata eraldi faili.

Antud nõue on tagamaks, et kogu kasutaja sessiooniga seotud infokooslus saaks turvalogisse kirjutatud ning see oleks eraldi kasutatav. Nõue on uute rakenduste puhul täidetud, kuid vanad on väga erinevate logimislahendustega, mistõttu on vaja kohati logikannete eraldamist ja normaliseerimist (**MFN1**).

- *Rakendus peab suutma logida kõiki välja ja sisse tulevaid (ka X-tee teenuste kaudu liikuvaid) päringuid. Peab olema võimalus logimist sisse-välja lülitada. Vajalik eelkõige debuggimiseks ja toodangu keskkonna probleemide lahendamiseks.*

Antud nõue on tagamaks kõikide päringute logimine. Nõue on uute rakenduste puhul täidetud, kuid vanad on väga erinevate logimislahendustega, mistõttu on vaja kohati logikannete eraldamist ja normaliseerimist (**MFN2**).

- *Rakendus peab logima kõiki rakenduses tekkivaid tehnilisi vigu kas faili või andmebaasi. Logi peab sisaldama minimaalselt (toodud järjekorras) vea tekkimise aega, veakoodi, veakirjeldust (stack trace, traceback vms), võimalusel kasutaja andmeid (nimi, ID, IP ja URL), HTTP-, GET- ja POST-parameetrid ja nende väärtusi.*

Antud nõue on tagamaks kõikide veasituatsioonide logimist. Nõue on uute rakenduste puhul täidetud, kuid vanad on väga erinevate logimislahendustega, mistõttu on vaja kohati logikannete eraldamist ja normaliseerimist (**MFN3**).

- *Logi tabelid peavad olema arhiveeritavad operatiivbaasist välja. Ka krüptoaheldatud logi korral.*

Antud nõue on tagamaks logide eemaldamisvõimaluse logiserverile, et tagada tööülesannete lahusus ning logide muutmiskaitse. Nõue on uute rakenduste puhul täidetud, kuid vanad on väga erinevate logimislahendustega, mistõttu on vaja kohati logikannete eraldamist ja normaliseerimist (**MFN4**).

- *Kasutajakontode puhul peab olema tagatud funktsioonide lahusus. Konkreetse kasutajatunnuse alt infosüsteemis sooritatud andmeuuendused ja -muudatused peavad olema üheselt seotavad selle kasutajatunnusega.*

Antud nõue on tagamaks kasutajakontode funktsioonide selge logimine. Nõue on uute rakenduste puhul täidetud, kuid vanad on väga erinevate logimislahendustega, mistõttu on vaja kohati logikannete eraldamist ja normaliseerimist (**MFN5**).

- *Rakenduse loomisel tuleb lähtuda toodud logitasemete kirjeldustest. Toodud logitasemed on Fatal, Error, Warning, Info, Debug ja Trace koos kirjeldustega.*

Antud nõue on tagamaks ühetaoline logitasemete seadistamise võimalus. Nõue on uute rakenduste puhul täidetud, kuid vanad on väga erinevate logimislahendustega, mistõttu on vaja kohati logikannete eraldamist ja normaliseerimist (**MFN6**).

Logide halduse tehniline juhend (LHJ)

Antud juhendis on toodud logimise tehnilised nõuded mis kirjeldavad erinevate vahendite kasutamist ning juhiseid erinevatele süsteemidele nende rakendamise kohta. Samuti sisaldab dokument tehnilisi konfiguratsioonidetaile mille täpsem analüüs antud töö käsitlusalasse ei kuulu. Alljärgnevalt toob autor neist olulisimad nõuete ja piirangute tarbeks välja.

- *Kasutusel on kaks keskset logiserverit, millest ühel hoitakse toote- ja testkeskkondade logisid (edaspidi logsrv1) ning teisel arenduse- ning koolituskeskkondade logisid (edaspidi logsrv2).*

Antud piirang on tingitud asjaolust, et väga suur osa arendustest luuakse välispartnerite poolt. Sellest ka arenduskeskkonna logide vajadus antud arenduspartneritele. Turvakaalutlustel (testi ja tootekeskkonna andmestik sisaldab isikuandmed ning muid seadustest tulenevaid delikaatseid andmed) ei looda ligipääse partneritele ühelgi juhul toote võrgusegmenti (**LHP1**).

- *Logide vaatamisõiguse määramine käib kasutajagruppide kaudu läbi keskse intsidendihalduse ning kokkulepitud kooskõlastusringi.*

Antud nõue tagab ühetaolise menetluse kõikidele asutuse poolt tehtavatele õiguste taotluse vajadustele ning on hiljem üheselt tuvastatav ja jälgitav (**LHN1**).

- *Logidele ligipääs on võimalik pöördudes logiserveri poole ssh, https või smb ühenduse kaudu (test- ning tootekeskkondade puhul kasutusel ainult ssh ühendus), kasutaja loomisel tuleb määrata ka vajalik ühendumisviis mis antud kasutajale lisatakse.*

Antud piirang on loodud tagamaks erinevatele osapooltele mugavam pöördumisviis enamkasutatavate turvaliste pöördumisviisidega vähemdelikaatsetele andmetele ning tagamaks maksimaalne turvalisus delikaatsete andmete kasutamisel (**LHP2**).

- *Arendus- ning koolituskeskkondade logisid säilitatakse kuu aega, peale mida kustutatakse, ei arhiveerita.*

Nõue on tingitud kokkuleppest välispartnerite ning äripoolega, vaja on kajastada ka teenusleppes (**LHN2**).

- *Testkeskkondade logisid säilitatakse kuu aega peale mida kustutatakse, ei arhiveerita.*

Nõue on tingitud kokkuleppest välispartnerite ning äripoolega, vaja on kajastada ka teenusleppes (**LHN3**).

- *Tootekeskkondade logisid säilitatakse üks aasta (eraldi defineeritud logide puhul ka kuni 7 aastat), vanemad kui kahe kuu vanused logid arhiveeritakse lindile.*

Nõue on tingitud kokkuleppest välispartnerite ning äripoolega, vaja on kajastada ka teenusleppes (**LHN4**).

- *Toote- ja testkeskkonna logidest genereeritakse kontroll räsid, iga logirea kaupa.*

Nõue on tingitud turvalisuse vajadusest, ISKE nõuded (ISKEN2, ISKEN28), osaliselt juba rakendatud (**LHN5**).

- *Arendajatele (s.h. välistele arendajatele) tagatakse ligipääs vastavalt vajadusele logsrv2 peale. Juhul kui on vajalik edastada tootelogisid siis tõstetakse vastavalt kooskõlastatud taotlusele tootelogi logsrv2 peale.*

Antud piirang on rakendatud tagamaks maksimaalne turvalisus testi ja tootelogide edastamisel ning, et tagada võimalikult paindlik edastamismeetod arenduse ja koolituse logidele (**LHP3**).

Turvalise aluskonfiguratsiooni juhend (TAJ)

Antud juhendis on logimisega seonduvalt kirjeldatud vajadus seadistada aja sünkroniseerimine internetiteenusepakkuja ajaserveriga ning süsteemse logimise seadistamise kohustus järgnevatele seadmetüüpidele (**TAJN1**):

- Võrguseadmed (tulemüürid, marsruuterid, kommutaatorid);
- Serverid (koormusjaoturid/veebifrondid, rakendusserverid, andmebaasiserverid);
- Kettamassiivlahendused (SAN võrguseadmed, kettamassiivid).

Logide andmekoosseisu, roteerimise, krüptoaheldamise, logiserverisse tõstmise jmt reguleerib LHJ.

Infosüsteemi kasutamise kord (ISKK)

Infosüsteemi kasutamise korra eesmärk on kehtestada IT asutuse töötajatele ühtsed reeglid infosüsteemide kasutamisel. Samuti käsitletakse dokumendis kasutajate tegevuste logide korraldust ning erinevate õiguste taotlemist.

Antud korras on logimist puudutava kohta järgnev:

3. INFOSÜSTEEMI KASUTAJA KOHUSTUSED

Töötaja on kohustatud:

arvestama, et tema võrguliiklus logitakse ja salvestatakse. Infoturbe juhil ja infoturbe spetsialistil on teenistusalasest vajadusest tulenevalt õigus ette teatamata tutvuda kasutaja võrguliikluse logidega.

Sellest antud korras sätestatud nõudest tulenevalt on vaja sisemiste kasutajate võrguliiklus logida vajalikus andmekoosseisus (**ISKKN1**).

Infoturbepoliitika (ITP)

ITP eesmärk on luua raamistik infoturbe korraldamiseks, et tagada valitsemisala infovarade käideldavus, terviklus ja konfidentsiaalsus kokkulepitud tasemel.

ITP sõnastab infoturbe põhimõtted, nende saavutamise suunised, infoturbe korralduse loogika ning peamiste infoturbemehhanismide rakendamise valitsemisalas.

Antud dokumendis on toodud logimist käsitlevad punktid:

2.39. Juurdepääsude haldus peab olema regulaarselt kontrollitud, tuvastatav ja jälgitav. Infosüsteemidele juurdepääsude seire eest vastutab IT asutuse infoturbejuht.

Selle punkti nõude tagab täna kas manuaalne või skriptide kaudu logide seiramine. Paremaks nõude tagamiseks on vaja rakendada analüüsivahend (**ITPN1**).

2.40. IT asutus logib ressursside poole pöördumisi või pöörduskatseid, mis sisaldavad minimaalselt infot nende tegija, aja ja lähtekoha kohta. Logide säilitamine on kooskõlastatud asjasse puutuvate teenuse omanikega. Logidel on ajatembeldamise ning krüptoaheldamisega tagatud tõestusväärtus (ehk nn logiandmete muutmise lukustamise võimalus) kõikjal, kus see on tehniliselt võimalik ja andmete iseloomust tulenevalt põhjendatud.

Antud punktist tuleneb nõue tagada krüptoaheldamine ning ajatembeldamine, nende teemade laiendamine on vajalik (**ITPN2**).

Teenustaseme lepingud asutustega (SLA)

Hetkel SLA-d ei sisalda logimise kohta ei nõudeid ega piiranguid, kuid kontseptsiooni loomisel tuleb sinna kindlasti fikseerida ka logimistingimused iga märgitud teenuse kohta, vaikimisi (SLA-s eraldi fikseerimata) logide säilitusajad on toodud LHJ-s.

Töökorralduslikud juhendid (TKJ)

Kord ei sisalda logimisega seonduvalt muud kui haldurite määramist logisüsteemile. Töökorralduse osas on teatud süsteemide puhul logiserveri ja logitava süsteemi administraator sama isik, antud töökorda tuleb kontseptsiooni loomisel sellekohased muudatused sisse viia.

3.1.3 Osapoolte ülesannetest tulenevad piirangud

Seoses mitmetest eeltoodud turvalisust tagavatest nõuetest (seotud on kõik muutmiskaitset tagavad nõuded) on alljärgnevad piirangud vaja kontseptsiooni loomisel kindlasti arvesse võtta.

- Linux süsteemiadministraatorid, süsteemide administraatorid, võrguadministraatorid ja rakenduste administraatorid ei tohi olla samaaegselt ka logiserveri haldurid. Infrastruktuuri arhitekt on samas sobiv kandidaat logiserveri halduriks (**OYP1**).
- Varundusadministraator ja logiserverite administraator peavad olema erinevad isikud (**OYP2**).

3.1.4 Standardid ja raamistikud

Käesolevas töö osas analüüsib autor ka mõningaid logimist puudutavaid standardeid ja raamistikke ning võrdleb neid juba eelpoolmainitud ISKE nõuete vastu.

- **SANS** Institute on Ameerika Ühendriikide eraettevõte, mille põhiliseks tegevusalaks on küberturvalisuse koolituste tegemine [16]. Antud instituut on välja töötanud standardi (*Information Logging Standard* [17]) katmaks logimisega seonduvad vajadused.

Standardis tuuakse logimise rakendamisel välja olulisimate punktidena asjaolu, et kõik tootesüsteemid ja sellega seonduvad infrastruktuuri komponendid peavad jätma tegevustest maha audit logi mis peab vastama järgmistele küsimustele:

Mis tehti? Kes tegi? Milliselt seadmelt tegevus tehti? Millal tehti? Kuidas tehti? Kas tegevus õnnestus?

Lisaks täpsustab standard ka milline tehniline andmekoosseis peaks logis kajastuma. Võrreldes ISKE erinevates meetmetes kehtestatuga ei paku autori hinnangul raamistik uut ja olulist, mida peaks täiendavalt rakendama.

- Ameerika standardi organisatsioon **NIST** (National Institute of Standards and Technology) pakub välja raamistiku logide halduse korraldamiseks [18][19].

Antud raamistik käsitleb kogu logide halduse protsessi viidates mitmetele Ameerika Ühendriikides kehtivatele standarditele ja seadusandlusele ning defineerib väga detailselt kõikvõimalikke logiformaate ning süsteeme. Autori hinnangul on asjasse puutuvate süsteemide lõikes ISKE poolt logimist puudutavad teemad sama detailselt kaetud. Üldine logihalduse korralduse ja planeerimise osa antud raamistikus on kindlasti heaks sisendiks mõningate üldisemate küsimuste lahendamise osas (arhitektuur, funktsioonid, rakendatavate tehniliste vahendite valik jmt). Konkreetse raamistiku täpset ja detailset rakendamist ei pea autor mõistlikuks, kuna ISKE katab antud valdkonda vähemalt sama detailsusega ning vastab paremini Euroopa seadusandlusele ja nõuetele.

- **ISO/IEC 27002:2013** on infosüsteemide turvalisust käsitlev standard, mis kehtestab raamistiku kõigi infovarade ning nende halduse kohta[20].

Antud standardi süsteemide halduse turvalisuse osas käsitletakse logimist põgusalt ning tuuakse välja, milliseid andmekoosseise on vaja süsteemide auditeerimiseks logida. Antud loetelu ei erine ISKE meetmete rakendamise juhendis koondatud nõuetest. Standard käsitleb kogu infoturbevaldkonda ega ole ainult logimist käsitlev. Seetõttu ei ole antud käsitlusala raames standardi suuremahuline rakendamine otstarbekas, sest ISKE katab logimise osas standardile vastavad nõuded.

- Information Technology Infrastructure Library (**ITIL**) on IT protsesside parimaid praktikaid koondav avatud raamistik, täpsemalt on logimisega seonduv käsitletud teenuse opereerimise faasis [21].

ITIL käsitleb logide haldust põgusalt sündmuste halduse protsessi (*Event Management*) koosseisus, kus saab tulla sisend ka logihaldusest peaaegu igale tasemele (sündmuste märkamine ja otsimine, sündmuste filtreerimine, prioriseerimine, reageerimine, sulgemine). Põhiliselt keskendub antud protsess monitooringlahenduste kirjeldamisele ning häireteavituste edastamisele ega käsitle logide haldamisega seonduvat. Seetõttu ei ole antud käsitlusala kontekstis otstarbekas ITIL-i sündmuste halduse protsessi täies mahus rakendada. Logihalduse loodav kontseptsioon peab tagama (nõue ISKEN31) võimekuse erinevatele muudele monitooringvahenditele sisendi andmise osas. See tagab ka võimaluse, et tulevikus saaks antud protsessi vajadusel rakendada.

Täiendavate standardite ja raamistike analüüsi kokkuvõte:

Autor võrdles eeltoodud standardite ja raamistike nõudeid ISKE nõuete vastu kuid kuna ISKE rakendamine riiklikele andmekogudele on igal juhul kohustuslik ning vastavad nõuded katavad ka IT asutuse vajadused, siis autor ei pidanud vajalikuks täiendavat standardit või raamistikku logimise korraldamiseks rakendada ühtse ja selge käsitluse tagamiseks.

3.1.5 Kokkuvõte kõikidest nõuetest ja piirangutest

Alltoodud tabelis (Tabel 1) on toodud koondvaade teemavaldkondade kaupa grupeerituna kõikidest peatükis 3.1 toodud nõuetest ning nende rakendamise staatused IT ühendasutuses. Antud tabelis toodud nõuded kuuluvad käsitlemisele logimise kontseptsiooni loomisel. Rakendamata staatus ei tähenda, et teema ei ole üldse IT asutuse poolt käsitletud, kuid kasutusel on kohmakad ja ebaefektiivsed asendusmeetmed, mis enamik juhtudel tähendavad suurt käsitsi töö mahtu ja ajakulu.

Tabel 1. Koondvaade kõikidest nõuetest ja piirangutest.

	Kontseptsiooni rakendamine	
Nõue/piirang	**Teema**	**Staatus**
ISKEN15	Logimise kontseptsiooni loomine ja rakendamine	Rakendamisel
ISKEN17	Tsentraalse logimise põhitõdedega arvestamine	Rakendamisel
ISKEN16	IT süsteemide logimine vastavalt loodavale kontseptsioonile	Rakendamata
ISKEN27	Logimise jaoks oluliste andmete valiku ja töötlemise kirjeldamine kontseptsioonis	Rakendamata
	Analüüsivahendi rakendamine	
Nõue/piirang	**Teema**	**Staatus**
ISKEN1	Logide kontrolli automatiseerimine	Rakendamisel
ISKEN4	Andmebaasisüsteemi logide keskserverile liigutamine ja analüüsi võimekuse tekitamine	Rakendamisel
ISKEN5	Automaatsele analüüsivahendile seiresüsteemide liidesed	Rakendamisel
ITPN1	Automaatse logide seire rakendamine	Rakendamisel
ISKEN19	Administratiivtegevuste logide analüüsivahendi valikukriteeriumid	Rakendamata
ISKEN26	Automaatse logiandmete analüüsivahendi rakendamine	Rakendamata
ISKEN31	Analüüsivahendi liidestamine teiste protsesside ja seirelahendustega	Rakendamata
	Logide eraldamine ja keskserverile koondamine	
Nõue/piirang	**Teema**	**Staatus**
LHP1	Kahe keskse logiserveri rakendamine turvakaalutlustel	Rakendatud
MFN1	Audit ja turvalogide eraldamine ning keskserverile koondamine	Rakendamata
MFN4	Logiandmed on vaja välja viia operatiivandmebaasist ning koondada keskserverile	Rakendamata
MFN5	Kasutajakontode tegevuste logimine	Rakendamata
	Logide andmekoosseisu määramine	
Nõue/piirang	**Teema**	**Staatus**
MFN2	Logide andmekoosseisu määramine kontseptsioonis	Rakendamisel
MFN6	Logitasemete määramine kontseptsioonis	Rakendamisel

	Kordade ja juhendite täiendamine	
Nõue/piirang	**Teema**	**Staatus**
LHP2	Turvaline pöördumine logiserveritele vastavalt andmetele, reguleeritud LHJ-s	Rakendatud
LHP3	Tootelogide edastamine välistele osapooltele on reguleeritud LHJ-s	Rakendatud
TAJN1	Kõigi logivate tootesüsteemide puhul on TAJ-s nõutud aja sünkroniseerimise seadistamine	Rakendatud
ISKKN1	ISKK-s on toodud sisemise võrguliikluse logimise vajadus	Rakendatud
ISKEN6	Arhiivisüsteemide logimine on reguleertitud TAJ-s ja LHJ-s	Rakendatud
ISKEN7	Marsruuterite ja kommutaatorite logimise turvanõuded on kehtestatud TAJ-s	Rakendatud
ISKEN8	Marsruuterite ja kommutaatorite logimisnõuded valikul on kehtestatud TAJ-s	Rakendatud
ISKEN9	Tulemüüride turvanõuded logimisele on kehtestatud TAJ-s	Rakendatud
ISKEN10	Serverite nõuded süsteemsele logimisele on kehtestatud TAJ-s	Rakendatud
ISKEN11	Serverite turvanõuded logimisele on kehtestatud TAJ-s	Rakendatud
ISKEN12	VPN seadmete logimisnõuded valikul on kehtestatud TAJ-s	Rakendatud
ISKEN13	Logiserveri kasutusest kõrvaldamine on reguleeritud varade halduse korras	Rakendatud
ISKEN14	Logiserveri turvalisuse nõuded ja seaded on dokumenteeritud LHJ-s	Rakendatud
ISKEN18	Unix süsteemide logimisnõuded on reguleeritud TAJ-s	Rakendatud
ISKEN20	Tulemüüride nõuded logimisele on kehtestatud TAJ-s	Rakendatud
ISKEN21	Võrguliikluse logimine on reguleeritud TAJ-s	Rakendatud
ISKEN22	Marsruuterite ja kommutaatorite logimise nõuded on kehtestatud TAJ-s	Rakendatud
ISKEN23	Logiserverid on paigaldatud vastavatesse tsoonidesse ja dokumenteeritud LHJ-s	Rakendatud
ISKEN24	VPN seadmete logimisnõuded on kehtestatud TAJ-s	Rakendatud
ISKEN29	Kõigi logivate tootesüsteemide puhul on TAJ-s nõutud aja sünkroniseerimise seadistamine	Rakendatud
ISKEN30	Serverite nõuded süsteemsele logimisele on kehtestatud TAJ-s	Rakendatud
ISKEN3	Kajastada LHJ-s detailselt oluliste sündmuste logimine logiserveril	Rakendamata
OYP1	Viia sisse muudatused TKJ-i haldurite erisuse tagamiseks logiserveril	Rakendamata
OYP2	Viia sisse muudatused TKJ-i haldurite erisuse tagamiseks logiserveril	Rakendamata
ISKEN25	Veebirakenduste sündmuste logimine kajastada teenusserverite osas TAJ-s	Rakendamata
LHN1	Reguleerida ISKK-s logidele ligipääsude taotlemine ja andmine	Rakendamata
LHN2	Arendus ja koolituskeskkondade logide säilitusajad SLA-sse	Rakendamata
LHN3	Testkeskkondade logide säilitusajad SLA-sse	Rakendamata
LHN4	Tootekeskkondade logide säilitusajad ja tingimused SLA-sse	Rakendamata
	Muutmiskaitse rakendamine	
Nõue/piirang	**Teema**	**Staatus**
ISKEN2	Uute rakenduste kasutuselevõtul rakendada logidele muutmiskaitse	Rakendamisel
ISKEN28	Rakendada muutmiskaitse kõigile keskserverile koondatavatele logidele	Rakendamisel
LHN5	Muutmiskaitse rakendamine test ja tootekeskkonna logidele	Rakendamisel
ITPN2	Muutmiskaitse rakendamine test ja tootekeskkonna logidele	Rakendamisel
	Normaliseerimine	
Nõue/piirang	**Teema**	**Staatus**
MFN1	Kõikide varem loodud rakenduste muutmisel arvestada normaliseerimisega	Rakendamata
MFN2	Kõikide varem loodud rakenduste muutmisel arvestada normaliseerimisega	Rakendamata
MFN3	Kõikide varem loodud rakenduste muutmisel arvestada normaliseerimisega	Rakendamata
MFN4	Kõikide varem loodud rakenduste muutmisel arvestada normaliseerimisega	Rakendamata
MFN5	Kõikide varem loodud rakenduste muutmisel arvestada normaliseerimisega	Rakendamata
MFN6	Kõikide varem loodud rakenduste muutmisel arvestada normaliseerimisega	Rakendamata

3.2 Logide haldamise tehnilised lahendused

Käesolevas töö osas selgitab ja analüüsib autor logide halduse tehnilisi lahendusi, mida arvestab edaspidi logide halduse kontseptsiooni väljatöötamisel nõuete ja piirangute (peatükk 3.1) täitmisel.

3.2.1 Logide periodiseerimine, roteerimine ja koondamine

Tagamaks logide ühetaoline käitlemine kõikides logitavates IT süsteemides, on tarvilik reguleerida logide tekkimisel nende käitlemine (nõuded ISKEN15-17, ISKEN27). Antud tegevuste reguleerimine ja kirjeldamine aitab selgelt ja ühetaoliselt logisid käidelda.

- **Periodiseerimine** on kokkulepe logi kindla perioodi sammuga (näiteks üks ööpäev) tükeldamine ning on sisendiks roteerimisele.
- **Roteerimine** tükeldab ette määratud sammuga logi eraldi failideks mille täiendavalt pakib ja tõstab eraldi kataloogi. Antud tegevus on sisendiks logiserverile koondamisel.
- **Koondamine** logiserverile on tegevus, kus roteeritud ja pakitud logifailid kopeeritakse logiserverile. Antud tegevus ei ole eeldus, et seadmest endast failid samaaegselt kustutatakse, kuna teatud juhtudel on otstarbekas süsteemsed logid kas veatuvastuse või analüüsi eesmärgil hoida alles ka seadmes.

Kogu eelnev ahel peab olema automatiseeritud ning peab tagama kindla perioodi roteeritud logi liikumise vastavale logiserverile.

Olulisimaks eelduseks on kõikide seotud segmentide ajaserverist sünkroniseeritud aeg (nõue TAJN1).

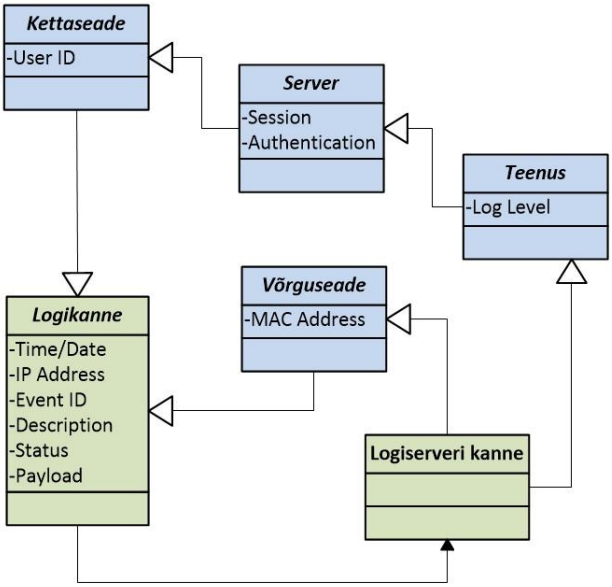
Teatud seadmete logide (võrguseadmed, mõned süsteemsed logid) puhul on kasutusel *syslog* protokoll, mille eesmärk on transportida vajadusel iga logikanne selle tekkimisel koheselt logiserverile [22]. Juhul kui logikanded liiguvad koheselt logitavast seadmest logiserverile, tuleb periodiseerimine ning roteerimine rakendada logiserveril.

3.2.2 Normaliseerimine

Et tagada kiire ja võimalikult paljusi erinevaid lõike hõlmav otsing erinevatest logidest, siis on otstarbekas logiandmete kuju normaliseerida ning kanda andmed seejärel kesksesse logide andmebaasi. Normaliseeritud keskne andmebaas peab olema eraldiseisev nn puhaste andmete hoidla, mille pealt toimub otsing ja edasine analüüs. Algandmed peavad olema täiendavalt eraldi ning millelt saab vajadusel algse kande originaalkujul ja tagatud tõestusväärtusega (peatükk 3.2.3 ja 3.2.4). Uute rakenduste

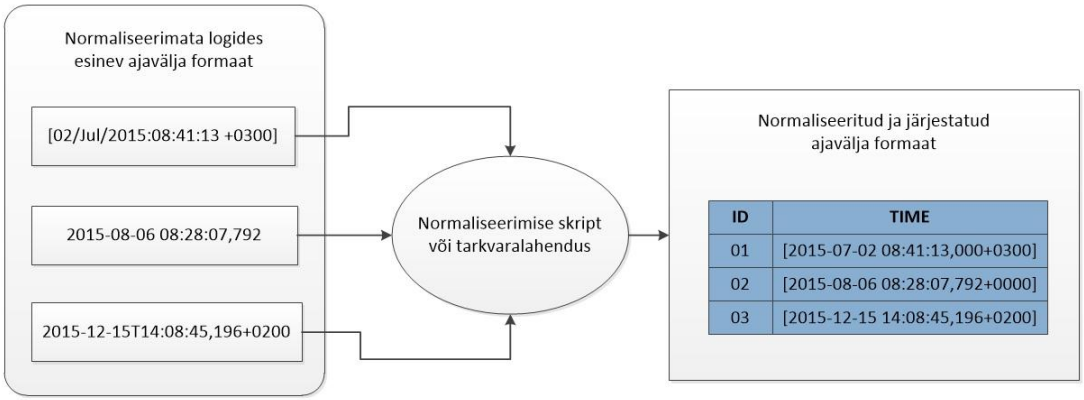
puhul reguleerib normaliseeritud andmete olemasolu NFR, olemasolevate rakenduste logide puhul tuleb rakendada kirjeldatud normaliseerimislahendust.

Logide ühtsele kujule viimine eeldab kokkulepitud andmekoosseisu olemasolu. Andmekoosseisu on analüüsinud ja kirjeldanud täpsemalt näiteks Tiit Hallas oma magistritöös, milles toodud (käesoleva töö käsitlusala raames) näidistega autor tutvus ning veendus, et olulised komponendid (lisaks ISKEN27 nõudes toodule) saaks kontseptsiooni loomisel arvesse võetud [23]. Alltoodud joonisel (Joonis 1) visualiseerib autor näite andmekoosseisu normaliseerimisest. Lisaks ühistele logikande komponentidele on erinevate seadmetüüpide lõikes logitavad lisa atribuudid välja toodud. Antud kannete koond on aluseks logiserveris kasutatava normaliseeritud andmekoosseisu rakendamisel.



Joonis 2. Normaliseeritud andmekoosseisu näide

Kõikidele andmeväljadele defineeritakse normaliseeritud formaat, mille näide on autori poolt visualiseeritud alljärgneval joonisel (Joonis 3). Normaliseerimisprotsess käivitub logiserveris kas logi tekkimisel (roteerimisel) serverile või vastav eraldi käivituv protsess (näiteks öine automaatprotsess). Antud protsess käivitab igat eri tüüpi logi kohta skripti, mis eeldefineeritud väljad viib kokkulepitud kujule ning salvestab andmebaasi. Hiljem on võimalik andmebaasist teha kiireid otsinguid näiteks kasutajatunnuse, toimumise aja, logitaseme või mõne muu parameetri järgi.



Joonis 3. Normaliseerimisprotsessi näide

3.2.3 Krüptoaheldamine

Tagamaks logide muutumiskaitse on vastavalt sisemistele nõuetele (nõue ITPN2), kasutusel olevatele juba realiseeritud parimatele praktikatele ja ISKE suunistele (nõuded ISKEN2 ja ISKEN28) tuginevalt tehnoloogiliselt esimeseks sammuks vaja rakendada krüptoaheldamine.

Krüptoaheldamine on tehnoloogia, mille kaudu saab tagada andmete muutumatuse kasutades räsifunktsiooni, mille puhul on tagatud andmete ühesuunalise (räsist ei ole võimalik tuvastada andmeid, millelt see on arvutatud) nn identifikaatori tekitamine. Andmestikult loodud räsi on iga erineva andmehulga pealt arvutades erinev (kasutades turvalist algoritmi, näiteks SHA-256 [24]) ning vastavalt algoritmile uuesti ja alati samadelt andmetelt arvutades sama.

Logide puhul on mõistlik krüptoaheldada logikande või kannete (näiteks 1-5tk) kaupa väikestes osades, kuna suuremates osades seda tehes (näiteks päevase intervalliga) on sellel mitu probleemi. Esiteks on probleemiks olukord, kus terve päeva logikanded on kuni räsi arvutamiseni muudetavas seisus ning nende õigsust saab tagada ainult päevase sammuga. Teiseks on näiteks teabenõudele vastamisel kogu räsiga kaetud segment vaja anda vastuseks, mis on aga isikuandmete seisukohalt mõeldamatu (tuleb väljastada oluliselt rohkem andmeid kui küsitakse ning seda ka isikute kohta, kelle kohta ei küsitud). Logimise puhul krüptoahela näitena võiks olla lahendus, kus iga rea logisse tekkiva kirje pealt arvutatakse räsi, mida omakorda kasutatakse järgneva logirea räsi arvutamisel ühe komponendina (tekib nn räsikett ehk ahel). Antud lahendus tagab olukorra, kus rakenduse ja süsteemsete logide puhul rakendatud krüptoahela muutmisel kogu ahel katkeb ning väärtustejada ei klapi enam. Isegi kui peaks toimuma pahatahtlik

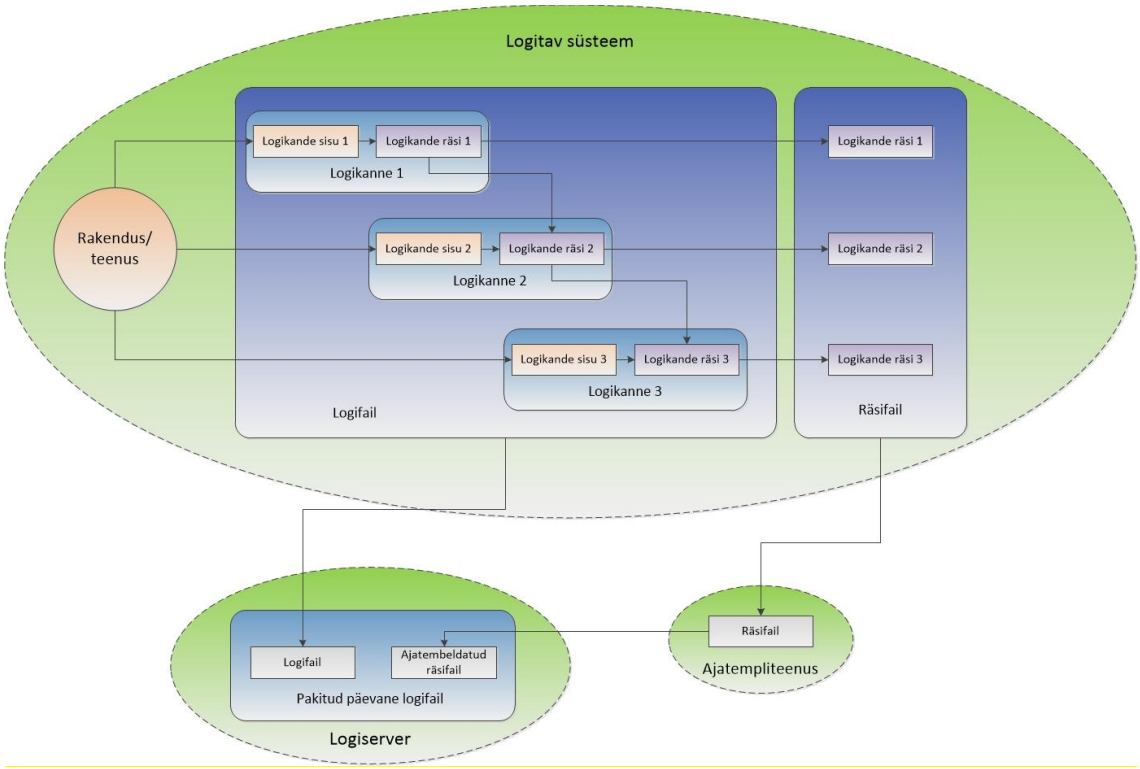
logikande muutmine või kustutamine, siis ei ole keerukat ahelat (rakendus logib ja arvutab uusi räsisi kaasates eelnevat, mis omakorda sõltub eelnevast jne) täies mahus muutmata ja logimist katkestamata võimalik seda jälge jätmata teha. Edasi roteeritakse päevase sammuga logid logiserverisse (logiserveri ja logitava serveri haldurid peavad olema erinevad isikud, sellisel juhul ei saa üks isik andmeid lihtsalt manipuleerida) koos eraldi ainult räsisid sisaldava failiga. Antud eraldi räsifaili olemasolu tagab olukorra, kus tõestusväärtuseks saab edasta räside faili (täielikuks tõestusväärtuse tagamiseks koos ajatempliga, peatükk 3.2.4) ning küsitud logikande või logikanded, ning nende andmete alusel on tuvastatav logide muutumatus.

Andmete õigsuse kontrollimine on võrdlemisi lihtne protseduur. Kui räside uuesti arvutusel saadakse samad tulemused kui räsifailis toodud, siis ongi tõestatud andmete muutumatus. Kui aga antud räsikomplekt on kuskil muutunud, siis tuleb ka edasisel räsiarvutusel erinev tulemus ning koos logidega salvestatud räside võrdlusel saab jälile millises konkreetses reas on muudatus tekkinud. Ehk siis on tuvastatav, millist logikannet algse tekkimise järgselt on muudetud. Krüptoaheldamise rakendamiseks on vaja mõningate rakenduste puhul arenduse käigus vastava funktsionaalsuse tagamine, sest operatsioonisüsteemi vahenditega logide krüptoaheldamine ei pruugi olla piisavalt efektiivne. Antud rakendusi käsitletakse käesolevast tööst eraldi ning nõuded lisatakse vajadusel NFR-i.

Syslog protokolli kasutavate lahenduste puhul on võimalik rakendada krüptoaheldamine kasutades vastavat antud protokolli lisafunktsionaalsust [25].

3.2.4 Ajatembeldamine

Kuna täieliku muutmiskaitse seisukohalt on oluline, et mitte keegi ei saaks logiandmeid manipuleerida, siis tuleb lisaks krüptoaheldamisele ka väliselt turvaliselt teenusepakkujalt vastavatele räsikettidele võtta ajatempel (antud lahenduse loogikat kirjeldatakse ka erinevates raamatutes. Näiteks „How to Time-Stamp a Digital Document“ [26]), mis kinnitab, et sellel konkreetsel ajahetkel oli antud räsiketi tulemus just täpselt selline (nõuded LHN5, ITPN2, ISKEN28). Sellisel juhul välistatakse olukord, kus näiteks logiserveri administraator arvutab kogu räsiketi tulemuse uuesti ja kogu kett oleks justkui õige ja muutumatu. Lahenduse tehniline loogika on näitlikult autori poolt visualiseerituna toodud alloleval joonisel (Joonis 4).



Joonis 4. Logide krüptoaheldamine ning ajatembeldamine

Eestis pakub ettevõte Guardtime riigiasutustele koostöös RIA-ga tasuta lüüsiteenusena ajatempliteenust [27]. Guardtime poolt kasutatava lahenduse puhul publitseeritakse räsiahelate kontrollräsid üldkasutatavas meedias (näiteks ajalehes), mis on tõendusväärtuse tuvastamiseks sõltumatu teenusepakkujast. Antud tehnoloogiat on kirjeldatud Guardtime veebilehel põgusalt, kuid on ka käsitletud teadustöös mis kirjeldab tehnoloogiat detailsemalt [28] [29].

3.2.5 Logide automaatne analüüs, seire, mustrite otsing

Teatud tasemeni on võimalik rakendada logide seiret luues käsitsi skripte, kuid jätkusuutliku automaatse analüüsi rakendamiseks on vaja vahendit, mis pakuks võimaluse erinevate logide seosed defineerida ning teostada teavitused teatud päästikute (trigger) rakendumisel. Näiteks kui teatud perioodil ei ole mingit logi tekkinud või logisse ilmub viga kirjeldav kood. Vastava süsteemse kõrvalekalde kohta peab vahendit olema võimalik liidestada olemasoleva monitooringlahendusega tagamaks operatiivne tegutsemine keskse monitooringu teavituse alusel.

Samuti peaks vastavas tarkvaralises vahendis olema võimalik kasutada muud sisendinfot sisaldavaid andmestikke. Näiteks kui tekib ELOG-i kanne mingi kindla serveri või süsteemi kohta ning peale seda muutub mingi tegevuse tegemine logis

aeglasemaks või kui tehakse kasutajapoolne tegevus kasutaja tööaja järgi vabal päeval. Selliste kõrvalekallete ja mustrite otsing peaks vastava kõrvalekalde märkamisel rakendama häireteavituse eeldefineeritud kanalisse (e-mail, SMS vmt) intsidendi algatamiseks.

4 Kontseptsioon ja tegevuskava

Antud töö osas toob autor välja eesmärkidest tulenevad väljundid arvestades töö analüüsiosas toodut. Tuginedes hetkeolukorra kaardistamisele (peatükk 2) ning analüüsile (peatükk 3) koostab autor üldise logihalduse kontseptsiooni, mis arvestab kõikide eelpool kirjeldatud nõuete ja piirangutega (peatükk 3.1) ning rakendab selleks tarvilikke kirjeldatud tehnilisi lahendusi (peatükk 3.2). Samuti toob autor välja hetkel rakendamata nõuete ja piirangute rakendamise tegevuskava, mis on aluseks, et tagada loodud kontseptsiooni rakendamine IT ühendasutuses.

4.1 Logihalduse kontseptsioon

Kontseptsioon on vajalik tagamaks logide halduse optimaalne korraldus ning selle arusaamade ja lähenemiste selgitamine. Kontseptsioon ei sisalda täpseid tehnilisi detaile vaid viitab erinevatele kordadele, juhenditele ja vastutajatele, kus vastavate teemade lõikes on neid käsitletud. Kontseptsioon annab (või vajab) sisendeid erinevatesse kordadesse, juhenditesse või lahendustesse. Kontseptsiooni loomisel on toodud valdkondade juures välja ka nõuded ja piirangud, mida vastav teema reguleerib.

4.1.1 Eesmärk

Logide halduse kontseptsiooni eesmärgiks on tagada asutuse teenuste ja süsteemi komponentide igakülgne ja optimaalne logimine ning kogu logide haldusega seonduva korraldamise kirjeldamine.

4.1.2 Logitavad IT süsteemid

Süsteemikomponendid, mille logide korraldust antud kontseptsioon käsitleb on:

- Võrguseadmed – tulemüürid, marsruuterid, kommutaatorid;
- Serverid – koormusjaoturid/veebifrondid, rakendusserverid, andmebaasiserverid;
- Kettamassiivlahendused – SAN võrguseadmed, kettamassiivid;
- Teenused/rakendused – klientasutustele pakutavad ärirakendused ja nendega seotud infrastruktuur.

4.1.3 Logimist reguleerivad dokumendid

Iga dokumendi kirjelduses on toodud rõhutatud fondiga olulisim logimisega seonduv. Lisaks on toodud iga dokumendi juures välja ka põhilised seonduvad nõuded ja piirangud.

- **ITP kehtestab** automaatse **logide seire ning muutmiskaitse nõude** (nõuded ITPN1 ja ITPN2). Korra ajakohastamise ning täitmise eest vastutab IT ühendasutuse infoturbespetsialist ning sisendeid saab kord vajadusel teistest asutuse osakondadest, asjakohasest seadusandlusest ning ärinõuetest.
- **ISKK kehtestab kasutajatele IT süsteemide kasutamise logimise tingimused. Samuti sätestatakse** korras **kasutajaõiguste taotlemise kord, mis puudutab ligipääse logidele** (nõuded ISKKN1 ja LHN1). Antud korra ajakohastamise ning täitmise eest vastutab IT asutuse infoturbe spetsialist ning sisendeid saab kord teistest asutuse osakondadest, seadusandlusest tulenevalt ning ärinõuete muutumisel või lisandumisel.
- **Iga** IT asutuse poolt pakutava **rakenduse ja teenuse kohta on kehtestatud SLA-s** ka **logimisvajadus ning tingimused** (nõuded LHN2-4). SLA ajakohastamise eest vastutab asutuse infosüsteemide teenuste osakond (ITO), sisendeid nõuetesse võib tulla nii asutuse teistest osakondadest kui ka äripoolelt. Juhul kui nõudeid täiendavalt ei kehtestata rakenduvad LHJ-s kehtestatud vaikenõuded logimisele keskkonniti.
- **Logiserveri haldurid on toodud TKJ-s** ning tagatud on olukord, kus logitava süsteemi ja logiserveri haldurid on erinevad isikud (piirangud OYP1 ja OYP2). Antud juhendi ajakohastamise ning täitmise eest vastutab asutuse infosüsteemide hoolduse osakond (IHO). Sisendid antud juhendisse saavad tulla asutuse infoturbe spetsialistidelt, süsteemiadministraatoritelt, seadusandlusest tulenevalt ning ärinõuete muutumisel või lisandumisel.
- **Teenuste/rakenduste loomisel** või ümberarendamisel **on logimisnõuded kehtestatud NFR-is** (juhend kehtestab nõuded: MFN1 – MFN6). Antud nõuete dokumendi ajakohastamise ning täitmise eest vastutab asutuse infosüsteemide arenduse osakond (ITA) sisendeid antud nõuetesse võib tulla ka IHO-st või äripoolelt.
- Kogu **logimisega seonduv tehniline dokumentatsioon** ning ka vaikenõuded logide käitluseks keskkonniti **on reguleeritud LHJ-s**. LHJ saab sisendeid nii

MFN-st kui ka SLA-dest (nõuded ja piirangud: LHP2, LHP3, ISKEN6, ISKEN14, ISKEN23, ISKEN3). LHJ ajakohastamise ning täitmise eest vastutab asutuse infosüsteemide hoolduse osakond (IHO).

- Eeltoodud (peatükk 4.1.2) **seadmete valikut, ettevalmistust ja seadistamist reguleeriv juhend** on TAJ. Antud juhend sisaldab kõikide seadmetüüpide lõikes algset konfigureerimisjuhendit, turvalise seadistamise põhimõtteid ning määrab ka komponentide süsteemsel tasemel logimise seadistamise (nõuded: TAJN1, ISKEN6-12, ISKEN18, ISKEN20-25, ISKEN29, ISKEN30). Juhendi ajakohastamise ning täitmise eest vastutab asutuse infosüsteemide hoolduse osakond (IHO). Sisendid antud juhendisse saavad tulla asutuse infoturbespetsialistidelt, süsteemiadministraatoritelt, seadusandlusest ning ärinõuetest.

4.1.4 Tehniliste lahenduste rakendamine

Vastamaks nõuetele ja piirangutele tuleb rakendada alltoodud tehnilised meetmed. Samuti on toodud välja seotus nõuete ja piirangutega.

- **Delikaatsete tooteandmetega** (toote ja testkeskkond) **logid** ning vähem oluliste andmetega logitavad keskkonnad **peavad olema eraldatud** (piirang LHP1).
- **Kõik asjakohased** eeltoodud (peatükk 4.1.2) seadmete ja nende kasutajate **logid tuleb** vastavalt SLA-s kokkulepitud perioodidele ja tingimustele (näiteks teatud kannete eraldamisnõue, kasutajate tegevuste logimine jmt) **roteerida** päevase sammuga **logiserverile**, et oleks tagatud keskses hoidlas logide olemasolu ning varundus. Vastavad tingimused tuleb kajastada ka LHJ-s erisustena (nõuded ISKEN3, ISKEN16, ISKEN27, MFN1, MFN5).
- **Andmebaasis asuvad logitabelid tuleb** operatiivbaasist **roteerida logiserverile** (nõue NFN4). Andmebaasilogide eraldamise reguleerimine ja kirjeldamine tuleb teha LHJ-s.
- **Logi tekkimisel peab koheselt rakenduma iga rea kohta räsi tekitamine** (*SHA-256 hash*), mis peab arvestama (räsi arvutusel on igal real seos eelnevaga) ka eelneva kande olemasolul (esimesel kandel ainult oma räsi) eelmise kande räsi. Iga rea räsiväärtus tuleb kirjutada ka eraldi räsifaili. Ööpäevase sammuga roteeritakse logifail koos vastava räsifailiga automaatselt logiserverile (veatuvastuseks ja ruumi olemasolul võib süsteemiadministraator vajadusel

logisid ka serveril või seadmel alles hoida, kuid üldjuhul kustutatakse ning seadme konfiguratsiooniga koos neid ei varundata) ning algatatakse uue päeva sündmusteks logifail. **Logiserveril peab rakenduma** tootekeskkonna **logide räside päevasele koondfailile ajatembeldamine**, mis tagab muutmiskaitse logiserveril päevase sammuga. Vastav tehniline lahendus on vaja kirjeldada detailselt LHJ-s ning rakendada (nõuded: ISKEN2, ISKEN28, LHN5 ja ITPN2).

Andmekoosseisu määramine:

Andmete koondamiseks, normaliseerimiseks ning dubleerimise vältimiseks on vaja teostada kindlate vajalike andmeväljade defineerimine tagamaks oluliste sündmuste vajalikul tasemel logimine (nõue ISKEN27). Vaja on tagada logimise puhul vähemalt järgmine andmekoosseis (ning see kirjeldada LHJ-s):

- sündmuse toimumise kuupäev ja kellaaeg;
- sessiooni algus ja lõpp;
- autentimismeetod;
- isiku ID/kasutajanimi;
- IP aadress;
- MAC aadress;
- logitase;
- sündmuse ID/veakood;
- sündmuse kirjeldus;
- sündmuse õnnestumise staatus;
- lisainfo.

Rakenduste logimisel on vajalik ka logitaseme seadistamise võimalus (nõue MFN6), et tagada vajadusel erinevatele osapooltele erineva sisuga logid.

- Fatal;
- Error;
- Warning;
- Info;
- Debug;
- Trace.

Logitasemed ja neid toetavad rakendused tuleb kirjeldada ka LHJ-s.

Normaliseerimine:

Tagamaks operatiivne logidest sündmuste otsimine tuleb rakendada logide normaliseerimine (nõuded MFN1-6). Logide normaliseerimise algsed logifailid säilitatakse krüptoaheldatuna ja ajatembeldatuna tõestusväärtuse tagamise eesmärgil. Normaliseeritud logide informatsioon salvestatakse logiserveril kesksesse normaliseeritud logide andmebaasi.

Normaliseerimiseks luuakse skript (kui on rakendatud automaatne analüüsivahend, siis teostatakse normaliseerimine kasutades vastavat analüüsivahendi seadistamist), mis vastavalt eeltoodud andmekoosseisule viib iga erineva logikuju vastava välja standardsele eelkirjeldatud kujule ning salvestab normaliseeritud kujul andmed andmebaasi päevase sammuga (Joonis 3). Erinevate süsteemide puhul on tegu erinevate andmetega ning puuduvad väljad jäävad osadel süsteemidel katmata, osadel on seevastu kasutatud väljasid rohkem. Kindlasti peab olema igal logikandel toimumise sünkroniseeritud aja väli (nõue TAJN1), mille järgi saab otsingut tehes järjestada. Kõik normaliseerimislahendust puudutav dokumenteeritakse LHJ-s.

4.1.5 Logide kasutuse audit

Logiserveris paikneva andmestiku kasutus tuleb täiendavalt üles logida seal sisalduvate erinevate delikaatsete andmete tõttu (nõue ISKEN27). Tuvastatav peab olema logiserveris asuvate andmete kasutamise aeg, kasutamise meetod (normaliseeritud andmed või algandmed), kasutajatunnus ja andmekoosseis mida kasutati. Logiserveri logimise seadistamine tuleb kirjeldada LHJ-s (nõue ISKEN14).

Kasutajate ja õiguste taotlused logiandmetele ligipääsuks tuleb reguleerida ISKK-s (nõue LHN1) järgnevalt:

Logide ligipääs:

- Ligipääs tootmis- ja testrakenduste, serverite ja andmebaaside logidele on lubatud infoturbejuhile ning rakenduste, serverite ja andmebaasi administraatoritele, kes on määratud vastavate süsteemide peaadministraatoriteks või varuadministraatoriteks.

- Erandkorras võivad logidele püsivat ligipääsu omada infosüsteemi arendusosakonna teenistujad, kellel on selleks infoturbespetsialisti ühekordne või piiratud kehtivusajaga luba.
- Sisekontrolli üksuse teenistujad võivad saada logidele alalise ligipääsu vastavasisulise taotluse esitamisel, mille kinnitavad IT ühendasutuse ja vastava ameti infoturbejuht ja süsteemihoolduse osakonna juhataja.

Logide väljastamine:

- Asutuste ametnikele, kes vajavad väljavõtet logiandmetest, väljastatakse logid ühekordse toiminguna taotluse alusel. Taotluse peab esitama infoturbespetsialistile teenistuja otsene juht, kes peab selle kooskõlastama.
- Välisarendajatele väljastatakse tootmis- või testrakenduste, serverite ja andmebaaside logid arendaja projektijuhi taotluse alusel. Taotluse peab kooskõlastama infoturbespetsialist ja süsteemihoolduse osakonna juhataja.
- Tootmisrakenduste logid väljastatakse ühekordse toiminguna. Tootmisrakenduse logide väljastamiseks esitab avalduse vastava rakenduse rakendusadministraator või muudatuste haldur. Avalduse peab heaks kiitma süsteemihoolduse osakonna juhataja ja infoturbejuht.

4.1.6 Analüüsivahendi rakendamine

Lisaks manuaalsele logide analüüsi teostamisele, tuleb rakendada (nõuded ISKEN1, ISKEN4, ISKEN5, ISKEN19, ISKEN26 ISKEN31) automaatne analüüsivahend. Vahendi valikukriteeriumid ja nõuded kajastatakse LHJ-s (nõue ITPN1). Analüüsivahend peab katma vähemalt järgmisi vajadusi:

- Peab võimaldama teha analüüsi erinevate logikujude pealt (normaliseerima);
- Võimaldama tuvastada dubleerivate logide olemasolu (piisava info olemasolul ka logidega katmata lõigud, näiteks kogu ahelast on mõni samm logimata);
- Võimaldama logide seiret turva ning käideldavusintsidentide otsinguks vastavalt ettedefineeritud kriteeriumitele, nagu näiteks:
  - logide järjepidevuse (katkemine, liigne logimine vms) tagamise analüüs;
  - korduvate liginemiskatsete (*portscan*) või sisselogimiskatsete analüüs;
  - administraatori tegevuste analüüs.

- Võimaldama ettedefineeritud andmestike (ELOG, tööaeg) ja reeglite alusel mustrite otsingut ja analüüsi;
- Võimaldama häirete edastamist teistesse süsteemidesse (monitooring, SMS, e-mail vmt)

4.1.7 Varundus

Logiserveri varundamine on sarnaselt teiste serverlahendusega reguleeritud üldises varunduse ja arhiveerimise juhendis, erisused logide säilitusaegade osas on toodud LHJ-s (nõue ISKEN14).

4.1.8 Kasutusest eemaldamine

Logiserverite kasutusest eemaldamine (nõue ISKEN13) on reguleeritud sarnaselt teistele süsteemidele IT ühendasutuse varade halduse korras, mis kehtestab tootesüsteemide kasutusest eemaldamisel andmekandjate eraldi turvalise hävitamise nõude.

4.2 Kontseptsiooni rakendamise tegevuskava

Antud töö osas toob autor välja eelnevas peatükis 4.1 toodud kontseptsiooni rakendamise kava. Alljärgnevas tabelis (Tabel 2) on toodud rakendamise sammud, tegevused, vastutajad ja kaetavad nõuded. Antud tabelis ei tooda välja juba täidetud nõudeid, kuid tegevuskava rakendamise aluseks on koondtabelis (Tabel 1) juba rakendatud nõuete ja piirangute täitmise täiendav rakendamise kontroll ning vajadusel ajakohastamine. Alltoodud logide halduse kontseptsiooni rakenduskava tagab kõikide juba hetkel rakendamata nõuete ja piirangute täitmise. Samuti ei kirjeldata igat tegevust täiendavalt lahti, kuna eelnevates töö osades on nõuded ja piirangud käsitletud täpsemalt. Antud tegevuskava eelduseks on tehniliste lahenduste (muutmiskaitse, normaliseerimine, analüüsivahend) rakendamine, mis on toodud eraldi valdkonnana, valdav osa nõudeid on sõltuvad antud tehnoloogiate rakendamisest. Tegevuskava täielikuks rakendamiseks on vaja teostada normaliseerimise ning automaatse analüüsivahendi valik.

Tabel 2. Logihalduse kontseptsiooni rakendamise tegevuskava

Tegevus	Vastutaja	Nõue
Tehnilised tegevused (eeldus järgnevale)		
Muutmiskaitse rakendamine	IHO, ITA	
Normaliseerimise rakendamine	IHO, ITA	
Analüüsivahendi rakendamine	IHO, ITA	
Tegevus	**Vastutaja**	**Nõue**
Kordade ajakohastamine		
Veebirakenduste sündmuste logimine kajastada teenusserverite osas TAJ-s	IHO	ISKEN25
Arendus ja koolituskeskkondade logide säilitusajad SLA-sse	ITO	LHN2
Testkeskkondade logide säilitusajad SLA-sse	ITO	LHN3
Tootekeskkondade logide säilitusajad ja tingimused SLA-sse	ITO	LHN4
Kajastada LHJ-s detailselt oluliste sündmuste logimine logiserveril	IHO	ISKEN3
Muudatused TKJ-i haldurite erisuse tagamiseks logiserveril süsteemiadministraator	IHO	OYP1
Muudatused TKJ-i haldurite erisuse tagamiseks logiserveril varundusadministraator	IHO	OYP2
Reguleerida ISKK-s logidele ligipääsude taotlemine ja andmine	Turva	LHN1
Tegevus	**Vastutaja**	**Nõue**
Loodud tehniliste lahenduste rakendamine ja dokumenteerimine		
Uute rakenduste kasutuselevõtul rakendada logidele muutmiskaitse	IHO, ITA	ISKEN2
Rakendada muutmiskaitse kõigile keskserverile koondatavatele logidele	IHO, ITA	ISKEN28
Muutmiskaitse rakendamine test ja tootekeskkonna logidele	IHO, ITA	LHN5, ITPN2
Normaliseerimise tehnilise lahenduse kirjeldamine LHJ-s	IHO, ITA	MFN1-6
Analüüsivahendi nõuete dokumenteerimine LHJ-s	IHO, ITA	ITPN1
Logitasemete kirjeldamine LHJ-s	IHO, ITA	MFN6
Audit ja turvalogide eraldamine ning keskserverile koondamine, normaliseerimine	IHO, ITA	MFN1
Kehtestada kontseptsioonis vajalik andmekoosseis, normaliseerimine	IHO, ITA	MFN2, MFN3
Logiandmete väljaviimine operatiivbaasist, normaliseerimine	IHO, ITA	MFN4
Kasutajakontode tegevuste logimine, normaliseerimine	IHO, ITA	MFN5
Kehtestada kontseptsioonis vajalik andmekoosseis, normaliseerimine	IHO, ITA	MFN6
Tegevus	**Vastutaja**	**Nõue**
Kontseptsiooni rakendamistegevused		
Logikontseptsiooni rakendamine	Kõik	ISKEN15
IT süsteemide kaupa logimise kirjeldamine LHJ-s	IHO	ISKEN16
Tsentraalse logimise põhitõdedega arvestamine	Kõik	ISKEN17
Andmete valiku kirjeldamine, keskserverile koondamine, kirjeldada LHJ-s	IHO	ISKEN27
Tegevus	**Vastutaja**	**Nõue**
Analüüsivahendi rakendamistegevused		
Logide kontrolli automatiseerimise rakendamine	IHO, Turva	ISKEN1
Andmebaasisüsteemi logide automaatse analüüsivõimekuse tekitamine	IHO, Turva	ISKEN4
Automaatsele analüüsivahendile seiresüsteemide liideste loomine	IHO, ITA	ISKEN5
Automaatse logide seire rakendamine	IHO, Turva	ITPN1
Administratiivtegevuste logide analüüsi seadistamine analüüsivahendis	IHO, Turva	ISKEN19
Automaatse logiandmete analüüsivahendi rakendamine	IHO, Turva	ISKEN26
Analüüsivahendi liidestamine olemasolevate protsesside ja seirelahendustega	IHO, Turva	ISKEN31

Tabelis toodud tegevuskava rakendamise edasiseks planeerimiseks on vaja igas vastutavas üksuses määrata igale teemale konkreetsed isikulised vastutajad ning tähtajad. Kontseptsiooni rakendamise projektijuhtimise ning tegevuste järelvalve koordineerimise eest vastutab asutuse turvaspetsialist. Lisaks tegevuskava rakendamisele on vaja rakendada ka turvaspetsialisti poolt pidev kordade asjakohasuse ja rakendamise kontroll, tagamaks dokumentatsioonis sisalduva reaalses elus rakendamise.

5 Kokkuvõte

IT ühendasutuse poolt teenindava valitsemisala laienemise ja pideva logide mahtude kasvuga seoses on tekkinud olukord, kus olemasoleva logide halduse lahendusega jätkamine ei ole enam jätkusuutlik. Selleks, et tagada senisest kiirem ja selgem logide haldus, oli vaja läbi viia põhjalik analüüs ja nõuete kaardistamine, mille alusel oli võimalik juurutada IT ühendasutusele jätkusuutlik logide halduse kontseptsioon. Selle teema olulisust tõestab ka see, et üha suurenev küberkuritegevus ning laienev arvutiseerumine eeldavad IT teenuste pakkujatelt võimekust tuvastada võimalikult täpselt intsidentide toimumise põhjuseid.

IT ühendasutuses on tekkinud olukord, kus toimub erinevate süsteemide ulatuslik logimine ja tihti on vajadus tuvastada erinevate sündmuste põhjuseid, aga selleks puuduvad eeldused. Logitakse reeglina nii nagu seadmete või süsteemide tootjad on seda vaikimisi määranud ning paljudel juhtudel ebavajalikus või ebapiisavas ulatuses ja mahus. Lisaks puudub süsteemne automatiseeritud logide analüüs. Juhul kui analüüs on vajalik, siis raiskavad spetsialistid info otsimiseks ebaproportsionaalselt palju tööaega ja saadud tulemused ei ole mitte alati usaldusväärsed. Mis siis sellises olukorras peaks ette võtma?

Magistritöö autori arvates tuli alustada süsteemi loomisest st esmalt tuli selgitada, millised on IT ühendasutuse vajadused, seejärel luua elementaarsed reeglid ehk raamistik, pakkuda välja logide haldust toetav lahenduse kontseptsioon ja selle realiseerimiskava. Kõlab lihtsalt aga siiani pole ükski riigi IT asutus (praeguse parima teadmise põhjal) suutnud seda eeskujulikult ja täielikult lahendada. Töö autor on veendumusel, et IT ühendasutus on esimene omataoliste seas riigis, kes selle olukorra lahendab ja tema poolt pakutud lähenemine loob selleks igakülgsed eeldused.

Käesolevas magistritöös käsitleti logide halduse erinevaid aspekte hõlmavat analüüsi ning selle põhjal olid töö väljunditeks logide halduse kontseptsiooni ning selle rakendamise kava koostamine.

Esmalt kaardistati huvitatud osapooled, rakendatud korrad ja juhendid ning kasutusel olevad tehnilised lahendused. Seejärel analüüsiti ja koostati erinevate seadusandlike regulatsioonide, olemasoleva töökorralduse, tehniliste lahenduste ning vajaduste alusel nõuded ja piirangud. Järgnevalt analüüsiti erinevaid nõuete ja piirangute täitmiseks olulisi tehnilisi lahendusi. Käsitletud tehniliste lahenduste kirjeldused hõlmasid erinevaid aspekte logide tekkimisest kuni nende analüüsini. Viimases töö osas koostati kõikide osapoolte vajadusi rahuldav, nõuetele ja piirangutele vastav logide halduse kontseptsioon ning selle rakendamise tegevuskava. Loodud kontseptsioon oli kõike hõlmav, alates logitavate süsteemide kirjeldusest kuni lahenduse käigust kõrvaldamiseni (näiteks riistvara vahetusel). Kontseptsioon loodi sisenditeks kõikidesse teistesse töökorralduslikesse etappidesse. Kontseptsiooni rakendamise tegevuskava hõlmas endas neljas põhivaldkonnas 30 alamtegevuse kirjeldusi ning tööde läbiviimise eest vastutavaid osapooli.

Magistritöös püstitatud eesmärgid said täidetud, olemasoleva lahenduse kaardistamise ning analüüsi põhjal loodi optimaalsem logide halduse kontseptsioon. Antud kontseptsioon arvestas seejuures seadusandluse ja sisevajaduste poolt püstitatud nõuete ja piirangutega. Samuti sai välja töötatud kontseptsiooni rakendamise etapiline tegevuskava. Käesoleva töö keerukaim osa oli sellise kontseptsiooni loomine, mis arvestaks olemasolevat logimisega seonduvat regulatsiooni ning tehnilisi lahendusi. Kuna juba rakendatud korrad, juhendid, vastutusvaldkonnad, osapoolte vajadused ja tehnilised lahendused seadsid mitmeid piiranguid erinevatele kontseptsioonis kajastatavatele osadele siis tuli kontseptsiooni loomisel nendest lähtuda. Töö käigus oli autoril vaja viia läbi keerukas ja mahukas analüüs nii seadusandluse kui ka sisekordade ja juhendite osas ning samuti luua seosed erinevate logimise tehniliste sammude ja rakendatavuse osas. Ühtlasi selgus, et riigis on tehtud vaid üksikud sellesuunalised teadustööd, mida autor ka analüüsis kasutas.

Antud töö tulemust (välja töötatud kontseptsiooni ning selle rakendamiskava) saab rakendada IT ühendasutuse logimise korraldamisel ning seda laiendada vajadusel teistele logitavatesse, antud töö käsitlusalast välja jäänud teemadele. Üldine kontseptsioonis käsitletud ülesehitus on rakendatav ka teistes sarnaste küsimuste ees olevates asutustes ning vastavaid muudatusi sisse viies (asutuse sisejuhendid ja korrad) on võimalik kontseptsiooni ka teistes asutustes rakendada.

Kasutatud kirjandus

[1] IT Ühendasutus, „Üldised tehnilised mittefunktsionaalsed nõuded 2.1,“ 01 2016. [Võrgumaterjal]. Available: Asutuse Intranet. [Kasutatud 20 04 2016].

[2] IT Ühendasutus, „Logide halduse tehniline juhend,“ 12 2015. [Võrgumaterjal]. Available: Asutuse Intranet. [Kasutatud 20 04 2016].

[3] IT Ühendasutus, „Turvalise aluskonfiguratsiooni juhend,“ 01 2016. [Võrgumaterjal]. Available: Asutuse Intranet. [Kasutatud 20 04 2016].

[4] IT Ühendasutus, „Infosüsteemide kasutamise kord K19,“ 24 08 2015. [Võrgumaterjal]. Available: Asutuse Intranet. [Kasutatud 20 04 2016].

[5] IT Ühendasutus, „Infoturbepoliitika K17,“ 03 08 2015. [Võrgumaterjal]. Available: Asutuse Intranet. [Kasutatud 20 04 2016].

[6] IT Ühendasutus, „Teenustaseme lepingud asutustega,“ 10 2015. [Võrgumaterjal]. Available: Asutuse Intranet. [Kasutatud 20 04 2016].

[7] IT Ühendasutus, „IHO Töökorralduslikud juhendid,“ 03 2016. [Võrgumaterjal]. Available: Asutuse Intranet. [Kasutatud 20 04 2016].

[8] Vabariigi Valitsus, „Määrus nr 252: Infosüsteemide turvameetmete süsteem,“ 29 01 2009. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/13125331?leiaKehtiv. [Kasutatud 20 04 2016].

[9] Riigi Infosüsteemi Amet, „ISKE kirjeldus,“ [Võrgumaterjal]. Available: https://www.ria.ee/ee/iske.html. [Kasutatud 20 04 2016].

[10] Riigi Infosüsteemi Amet, „ISKE Rakendusjuhend,“ [Võrgumaterjal]. Available: https://www.ria.ee/public/ISKE/ISKE_kataloogid/ISKE_rakendusjuhend_7.00.pdf. [Kasutatud 20 04 2016].

[11] Vabariigi Valitsus, „Avaliku teabe seadus,“ 16 01 2016. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv. [Kasutatud 20 04 2016].

[12] Vabariigi Valitsus, „Infoühiskonna teenuse seadus,“ 01 01 2015. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/112072014048?leiaKehtiv. [Kasutatud 20 04 2016].

[13] Vabariigi Valitsus, „Määrus nr 78: Infosüsteemide andmevahetuskiht,“ 18 09 2015. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/115092015011. [Kasutatud 20 04 2016].

[14] Vabariigi Valitsus, „Maksukorralduse seadus,“ 10 02 2016. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/109022016003?leiaKehtiv. [Kasutatud 20 04 2016].

[15] Vabariigi Valitsus, „Finantsinspektsiooni seadus,“ 10 01 2016. [Võrgumaterjal]. Available: ://www.riigiteataja.ee/akt/12898417?leiaKehtiv. [Kasutatud 20 04 2016].

[16] SANS Institute, „About SANS Institute,“ [Võrgumaterjal]. Available: https://www.sans.org/about/. [Kasutatud 20 04 2016].

[17] SANS Institute, „Information Logging Standard,“ 06 2014. [Võrgumaterjal]. Available: https://www.sans.org/security-resources/policies/server-security/pdf/information-logging-standard. [Kasutatud 20 04 2016].

[18] National Institute of Standards and Technology, „NIST,“ [Võrgumaterjal]. Available: http://www.nist.gov/. [Kasutatud 20 04 2016].

[19] National Institute of Standards and Technology, „Guide to Computer Security Log Management,“ 09 2006. [Võrgumaterjal]. Available: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf. [Kasutatud 20 04 2016].

[20] International Standards Organisation, „ISO/IEC 27002:2013,“ 01 10 2013. [Võrgumaterjal]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=54533. [Kasutatud 20 04 2016].

[21] S. Taylor, S. Lacy ja I. Macfarlane, „ITIL: Service Operation,“ Norwich, TSO, 2007, pp. 38-44.

[22] Network Working Group, „RFC 5424: The Syslog Protocol,“ 03 2009. [Võrgumaterjal]. Available: https://tools.ietf.org/html/rfc5424. [Kasutatud 20 04 2016].

[23] T. Hallas, „Logging Requirement Analysis and Specification for Development Based on Governmental Institutions of Estonia,“ Tallinna Tehnikaülikool, Tallinn, 2014.

[24] Internet Engineering Task Force (IETF), „RFC 6234: US Secure Hash Algorithms,“ 05 2011. [Võrgumaterjal]. Available: https://tools.ietf.org/html/rfc6234. [Kasutatud 20 04 2016].

[25] Internet Engineering Task Force (IETF), „RFC5848: Signed Syslog Messages,“ 05 2010. [Võrgumaterjal]. Available: https://tools.ietf.org/html/rfc5848. [Kasutatud 20 04 2016].

[26] W. S. S. Stuart Haber, How to Time-Stamp a Digital Document, Morristown, N.J.: Bellcore, 2001.

[27] Guardtime, „About Guardtime,“ [Võrgumaterjal]. Available: https://guardtime.com/about. [Kasutatud 20 04 2016].

[28] Guardtime, „KSI Blockchain Technology,“ [Võrgumaterjal]. Available: https://guardtime.com/ksi-technology. [Kasutatud 20 04 2016].

[29] A. K. R. L. Ahto Buldas, „Keyless Signatures Infrastructure: How to Build Global Distributed Hash-Trees,“ *Secure IT Systems*, Ilulissat, Lecture Notes in Computer Science, 2013, p. 320.