TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Fred Matis Teeäär IAAB185131

Automaatse identiteedi- ja ligipääsuhalduse juurutamine Magnetic MRO AS näitel

Bakalaureusetöö

Juhendaja: Edmund Laugasson
MSc

Tallinn 2023

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: Fred Matis Teeäär

16.05.2023

Annotatsioon

Käesoleva bakalaureusetöö eesmärgiks on luua töötab automaatne identiteedi- ja ligipääsuhalduse lahendus ettevõttele Magnetic MRO AS, mis asendaks eksisteerivates personali protsessides IT osakonna poolt teostavate käsitsi tegevuste osakaalu. Lahendus parandab olemasolevaid protsesse ning maandab identiteedi- ja ligipääsuhaldusega seotud riske.

Bakalaureusetöö käigus luuakse konsoolirakendus Python 3 programmeerimiskeeles, mis asendab eksisteerivaid käsitsi tegevusi personali protsessides ja asendab need automatiseeritud tegevustega. Loodud identiteedi- ja ligipääsuhalduse lahendus suudab luua kasutajaid, sulgeda kasutajaid, hoida andmeid ajakohasena ja veenduda ligipääsuda ajakohasuses. Lahendus on jagatud mitmeks osaks, mis tegelevad eraldi äriloogika, logimise ja teavitustega.

Töö rõhk on olemasolevate personali protsesside parandamisel, et vähendada IT-osakonna poolsete tegevuste mahtu, seeläbi vähendades inimfaktorist tulenevate riskide osakaalu. Personali protsessides identiteedi- ja ligipääsu haldusega seotud tegevuste automatiseerimise tulemuseks on töötajate kasutajate andmete ja ligipääsude ajakohasuse tagamine.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 44 leheküljel, 5 peatükki, 5 joonist.

Abstract

Introduction of Automated Identity and Access Management on the Example of Magnetic MRO AS

The aim of current thesis is to create an automated identity and access management solution for the company Magnetic MRO AS which would replace the manual actions of IT department in existing employee related processes. The solution aims to aid existing processes and reduces operational risks in relation to identity and access management.

During the development an automated identity and access management solution is created using Python 3 programming language, which replaces existing manual actions of IT department in employee processes with automated actions. The created automated identity and access management solution is able to create and close accounts and ensure that employee related data and access are up to date. The solution is split into multiple parts that address the business logic of identity and access management, logging and notifications.

The emphasis in the work is on the improvement of existing employee processes to reduce the quantity of manual actions performed by IT department and therefore reducing human factor related risks. Automation of identity and access management ensures that user account related data and accesses are up to date.

The thesis is in Estonian and contains 44 pages of text, 5 chapters, 5 figures.

Lühendite ja mõistete sõnastik

Active Directory	Microsofti loodud kohtvõrgu kataloogiteenus
AIAM	Automaatne identiteedi- ja ligipääsuhaldus
API	Rakendusliides
Azure Active Directory	Microsofti pilvepõhine kataloogiteenus ja analoog Active Directory'le
IAM	Identiteedi- ja ligipääsuhaldus
IT	Infotehnoloogia
LDAP	*Lightweight Directory Access Protocol* ehk kataloogiteenuse ligipääsu protokoll
Python 3	Python 3 programmeerimiskeel
RBAC	Rollipõhine ligipääsude haldus

Sisukord

1 Sissejuhatus **8**

2 Identiteedi- ja ligipääsuhaldus **9**

2.1 Kataloogiteenus 9

2.2 *Lightweight Directory Access Protocol* 10

2.2.1 LDAP operatsioonid 10

2.2.2 Microsoft Active Directory 11

2.2.3 Microsoft Azure Active Directory 12

2.3 Identiteedi- ja ligipääsuhaldus 13

2.3.1 Identiteedi- ja ligipääsuhalduse aktuaalsus 13

2.3.2 Identiteedi- ja ligipääsuhalduse tööpõhimõtted 14

2.3.3 Automaatne identiteedi- ja ligipääsuhaldus 15

2.3.4 Identiteedi- ja ligipääsuhalduse funktsioonid 15

2.4 Identiteedi- ja ligipääsuhaldus lahendused 16

2.4.1 Identiteedihaldusplatvorm MidPoint 16

2.4.2 Programmeerimiskeel Python 3 17

2.5 Personalihaldussüsteem 19

3 Ettevõtte ja protsesside kirjeldus **20**

3.1 Ettevõte Magnetic MRO AS 20

3.1.1 Ettevõtte struktuur 21

3.2 Ettevõtte olemasolev identiteedi- ja ligipääsuhaldus 21

3.2.1 Töötaja identiteet 21

3.2.2 Töötaja ligipääsud 22

3.2.3 Personalihaldussüsteem 22

3.2.4 Personali protsess 23

3.2.5 Kataloogiteenus Active Directory 25

3.2.6 Olemasoleva identiteedi- ja ligipääsuhalduse probleemid 25

4 Automaatne identiteedi- ja ligipääsuhaldus **27**

4.1 Analüüs 27

4.1.1 Riskianalüüs 27

4.1.2 Probleemide ja lahenduste kaardistus 29

4.1.3 Identiteedi- ja ligipääsuhalduse lahenduse nõuete kaardistus . . . 30

4.1.4 Lahenduse valiku põhjendus 31

4.2 Automaatse identiteedi- ja ligipääsuhalduse lahendus 32
4.2.1 Lahenduse moodulid 32
4.2.2 Lahenduse tööprotsessid 36
4.2.3 Uuendatud personali protsessid 38
4.3 Lahenduse väljundi analüüs 39
4.4 Tuleviku arengusuunad 40

5 Kokkuvõte 41

Kasutatud kirjandus 42

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks 44

Joonised

1 *Üldistatud personali protsess: fookuses IT.* 24

2 *Identiteedi- ja ligipääsuhalduse põhimooduli toimimine.* 33
3 *E-posti teavituste saatmine.* 34
4 *Ligipääsude pärimise protsess.* 35
5 *Üldistatud personali protsess: fookuses automaatne identiteedi- ja ligipääsuhaldus* 39

1. Sissejuhatus

Automatiseeritud identiteedi- ja ligipääsuhaldus on kiiresti arenev valdkond, mis on viimastel aastatel saanud märkimisväärset tähelepanu tänu oma potentsiaalile parandada turvalisust ja lihtsustada kasutajate ligipääsude haldust. Üks tähtsamaid osi küberturvalisusest ettevõttetes on tõhus identiteedi- ja ligipääsuhaldus, mis on järjest komplekssem ülesanne kuna kasutajate, identiteetide ja süsteemide maht on pidevas tõusus.

Identiteedi- ja ligipääsuhaldus viitab ettevõtte sisestele protsessidele, millega tagatakse töötajatele ligipääs erinevatele infosüsteemidele ja -varadele. Identiteedi- ja ligipääsuhaldus üks põhieesmärkidest on kindlustada, et kasutajatel oleksid õiged ligipääsud ja valed inimesed ei saaks ligipääsu ressursidele, mida neil vaja ei ole.

Traditsiooniliselt on identiteedi- ja ligipääsuhaldus olnud käeline protsess, mis nõuab süsteemi administraatoritelt kasutajate ja ligipääsude käsitsi haldamist. Paraku on selline lähenemisviis aeganõudev, veaohtlik ja kulukas. Lähtudes kasvavast vajadusest tagada ettevõtte infovarade turvalisust on vajalik identiteedi- ja ligipääsuhaldus automatiseerida.

Bakalaureuse töö eesmärgiks on automaatse identiteedi- ja ligipääsuhaldus protsesside loomine ja juurutamine ettevõtte Magnetic MRO AS näitel. Tähtis on tagada kasutaja andmete ajakohasus, kindlustada, et kasutajal on ainult talle vajaminevad ligipääsud, logida automatiseeritud tegevusi ja vähendada käelisi tegevusi.

Esimeses osas antakse ülevaade identiteedi- ja ligipääsuhaldus tehnoloogiatest, mõistetest ja turul olevatest lahendustest, mis on seotud identiteedi- ja ligipääsuhaldusega.

Teises osas antakse ülevaade ettevõttest, kus lahendust juurutatakse, personali protsessist, kasutuselolevatest tehnoloogiatest, tutvustatakse probleeme olemasolevates protsessides ja püstitatakse lähteülesanne.

Kolmandas osas tegeletakse lähteülesande lahendamisega. Lahenduse saavutamiseks teostatakse riskianalüüs, kaardistatakse probleemid ja potentsiaalsed lahendused, valitakse lahendus, mis ühtib ettevõtte spetsiifikaga, lahendus juurutatakse ning analüüsitakse lahenduse kasulikkust.

2. Identiteedi- ja ligipääsuhaldus

Tänapäeva info- ja kommunikatsioonitehnoloogia keskkond on muutnud ligipääsu haldamise segaseks ja keeruliseks. Haldusmaastik on muutunud, sest igal kasutajal on igal pool ja igal ajal olemas veebipõhine ligipääs. Lisaks on äridel tekkinud vajadus omada ligipääsu rohkematele teenustele ja süsteemidele mis on hajutatud platformide ja võrguteenuste pidevalt muutuvas infrastruktuuris. Ettevõtteid sunnitakse lisama personali süsteemide haldusse või investeerima tehnoloogiapõhistesse protsessimuudatustesse. Samal ajal muutuvad kasutajad märkimisväärselt, tekitades uusi ootusi teenuse kvaliteedile. Lisaks nõuavad reguleerivad institutsioonid kinnitust, et ligipääsu võimaldavaid protsesse kontrollitakse ja dokumenteeritakse. Keset kasvavaid nõudmisi, keerukust ja ootusi on kasutajate ligipääsu haldamise vahendeid ja tehnikaid saadaval lugematul hulgal ning igaühega kaasnevad juhtkonna jaoks erinevad probleemid ja katsumused. [1]

2.1 Kataloogiteenus

Kataloog on spetsialiseeritud andmebaas, mis on loodud kasutajate, kasutajaobjektide, rühmade ning arvutite ja palju muu otsimiseks ning sirvimiseks lisaks põhiliste otsingu- ja värskendusfunktsioonide toetamisele. [2]

Kataloogid sisaldavad tavaliselt kirjeldavat, atribuudipõhist teavet ja toetavad keerukaid filtreerimisvõimalusi. Kataloogid üldiselt ei toeta keerulisi tehingu- või tagasipööramisskeeme, mis on kasutusel andmebaasihaldussüsteemides. Neid kasutatakse andmebaasihalduses suuremahuliste ning keerukate värskenduste käsitlemiseks. Kataloogivärskendused on tavaliselt lihtsad kõik-või-mitte-midagi muudatused, kui need on üldse lubatud. Kataloogid on üldiselt häälestatud, et anda kiire vastus suuremahulistele otsingu- või otsinguoperatsioonidele. Neil võib olla võime paljundada teavet laialdaselt, et suurendada kättesaadavust ja usaldusväärsust, vähendades samal ajal reageerimisaega. [2]

Kataloogiteenuse pakkumiseks on palju erinevaid võimalusi. Erinevad meetodid võimaldavad salvestada kataloogi erinevat liiki teavet, esitada erinevaid nõudeid selle kohta, kuidas seda teavet saab viidata, küsitleda ja ajakohastada, kuidas see on kaitstud volitamata ligipääsu eest, ja palju muud. Mõned kataloogiteenused on kohalikud, pakkudes teenust piiratud kontekstis. Teisel käel on ka globaalsed kataloogiteenused, mille haare võib ulatuda üle terve interneti. Globaalsed teenused on tavaliselt hajutatud - kataloogiteenuses sisalduvad andmed on jaotatud mitme masina vahel. Selleks, et kataloogiteenust pakkuda, teevad

masinad omavahel koostööd. Tavaliselt määratleb globaalne teenus ühise nimeruumi (ingl. keeles *namespace*). Tänu nimeruumile ei ole kasutajal vahet, kuidas ta andmetega seoses paikneb, ta näeb alati samasugust ülevaadet. [2]

2.2 *Lightweight Directory Access Protocol*

Lightweight Directory Access Protocol (edaspidi LDAP) on kataloogiteenus, mille uusim versioon on LDAPv3 ning on defineeritud RFC 4511 dokumendis. Kataloog on hulk avatud süsteeme, mis teevad omavahel koostööd, et pakkuda kataloogiteenust. Kataloogiteenusele saavad ligi nii inimesed kui ka süsteemid kataloogi ligipääsu protokolli abil. [3]

Igal kirjel on unikaalne tunnus, milleks on eristatav nimi (ingl. keeles *Distinguished name*). See koosneb kirje suhtelisest eristatavast nimest. Eristatav nimi koostatakse mõne kirje tunnuse põhjal - näiteks nimi. Viimasele lisatakse kirjet sisaldava struktuuriüksuse eristatav nimi. Eristatav nimi määrab objekti asukoha kataloogis. [3]

2.2.1 LDAP operatsioonid

LDAP protokoll teeb saadavaks hulga operatsioone, mida saab kasutada andmetele ligipääsuks ja redigeerimiseks. [3]

Põhiliste operatsioonide hulka kuuluvad[3]:

1. *Bind*: Sidumisoperatsiooni ülesanne on võimaldada autentimist kliendi ja serveri vahel. Sidumisoperatsiooni tuleks pidada ühenduse loomise operatsiooniks.
2. *Search*: Otsinguoperatsiooni kasutatakse, et taotleda serverist andme kirjete tagastamist vastavalt otsingukriteeriumitele ning võttes arvesse ligipääsu. Operatsiooni saab kasutada atribuutide lugemiseks ühest kirjest, kindlale kirjele vahetult alluvatest kirjetest, või tervest kirjete alajaotusest.
3. *Add*: Lisamisoperatsioon võimaldab kliendil taotleda kirje lisamist kataloogi.
4. *Modify*: Muutmisoperatsioon võimaldab kliendil taotleda kirje attribuutide muutmist kataloogis.
5. *Delete*: Kustutamisoperatsioon võimaldab kliendil taotleda kirje kustutamist kataloogist.
6. *Modify DN*: Eristatava nime muutmisoperatsioon võimaldab kliendil taotleda kirje eristatava nime muutmist kataloogis. Tegu on objekti liigutamise operatsiooniga.

2.2.2 Microsoft Active Directory

Microsoft Active Directory on Microsofti välja töötatud kataloogiteenus, mis on osa Windows Serveri operatsioonisüsteemist. Active Directoryt kasutatakse arvutite, kasutajate, printerite, failijagamise, turvarühmade ja rühmapoliitikate halduseks. Active Directory põhineb kataloogiteenuse protokollil LDAP. Active Directory andmebaasides olevatele objektidele pääseb ligi LDAP protokolli abil.[4]

Active Directory Domain Services kataloogiteenus on Microsoft Windows Serveri operatsioonisüsteemidega kaasas olev hajutatud kataloogiteenus. Active Directory Domain Services võimaldab kogu võrgu tsentraliseeritud ja turvalist haldamist, mis võib hõlmata hoonet, linna või mitut asukohta kogu maailmas. [5]

Hajutatud arvutivõrkudes suhtlevad arvutid ja muud seadmed internetiühenduse kaudu, et täita ülesandeid kliendi-, serverirakendustes. Hajutatud keskkonna toimimiseks on vaja keskset teabehoidlat ja integreeritud teenuseid, mida kasutatakse võrgu kasutajate, teenuste, seadmete ja lisateabe haldamiseks. [5]

Microsoft Active Directory skeem

Skeem on Active Directory komponent, mis määratleb kõik objektid ja atribuudid, mida kataloogiteenus andmete salvestamiseks kasutab. [5]

Active Directory salvestab ja hangib teavet mitmesugustest rakendustest ja teenustest. Selleks, et saaks salvestada ja kopeerida andmeid potentsiaalselt lõpmatust hulgast allikatest, standardiseerib Active Directory andmete kataloogi salvestamise. Andmete salvestamise standardiseerimisega saab kataloogiteenus andmeid hankida, värskendada ja kopeerida, tagades samas andmete terviklikkuse. [5]

Kataloogiteenus kasutab objekte salvestusüksustena. Kõik objektid on määratud skeemil. Iga kord, kui kataloog tegeleb andmetega, pärib kataloog skeemi sobiva objektimääratluse jaoks. Skeemi objektimääratluse põhjal loob kataloog objekti ja salvestab andmed. [5]

Objektimääratlused kontrollivad andmete tüüpe, mida objektid saavad talletada, samuti andmete süntaksit. Selle teabe abil tagab skeem, et kõik objektid vastavad nende standardmääratlustele. Selle tulemusena saab Active Directory talletada, tuua ja valideerida andmeid, mida ta haldab, sõltumata andmete algallikaks olevast rakendusest. Kataloogis saab salvestada ainult andmeid, millel on skeemil olemasolev objekti määratlus. Kui on vaja talletada uut tüüpi andmeid, tuleb esmalt luua skeemile uus andmete objektimääratlus.[5]

Microsoft Active Directory objektid

Active Directory kasutab teabe talletamiseks objekte. Objektid on andmestruktuurid, mis koosnevad mitmest atribuudist. Atribuudid talletavad nii andmeid kui ka nendega seotud metaandmeid. Metaandmed on andmed, mis kirjeldavad teiste andmete omadusi. Näiteks objektil, mis salvestab kasutajakonto, on atribuudid, mis sisaldavad kasutaja sisselogimisnime, eesnime, perekonnanime ja parooli. Igal atribuudil on täiendavad atribuudid, mis sisaldavad metaandmeid atribuudis talletatava teabe kohta. Näiteks sisselogimisnime atribuudil on mitu oma atribuuti. Üks sisselogimisnimega seotud atribuut määrab, et sisselogimisnimi on nõutav atribuut, seega kasutajaobjekt kehtib ainult siis, kui selles on olemas sisselogimisnime atribuut. Teine sisselogimisnime atribuut määrab atribuudis talletatava väärtuse süntaksi. See tagab, et atribuut sisaldab väärtust kehtivas vormingus. Mõlemad atribuudid sisaldavad sisselogimisnime atribuudi metaandmeid, see tähendab, et need määratlevad sisselogimisnime atribuudi omadused. [5]

Skeemi objektimääratlused loetlevad kõik objektiatribuudid ja määratlevad, kuidas need atribuudid omavahel seotud on. Mõned objektid on lihtsad ja sisaldavad ainult mõningaid atribuute, samas on ka objekte, mis on üsna keerulised ja sisaldavad sadu atribuute. Uute objektide määratlemiseks on väiksemad objektid omavahel seotud, et määratleda uute objektide vajalikud atribuudid. [5]

2.2.3 Microsoft Azure Active Directory

Azure Active Directory on Microsofti pilvepõhine identiteedi- ja ligipääsuhalduse lahendus. See pakub autentimis- ja volitamisteenuseid pilvepõhistele rakendustele, samuti muudele Microsofti teenustele, nagu Office 365, Dynamics 365, ja Azure. Azure Active Directory eesmärk on pakkuda kasutajatele ühtset sisselogimiskogemust kõigis nende rakendustes, olenemata sellest, kas need on pilvepõhised või kohapealsed. [6]

Azure Active Directory toetab paljusid autentimismeetodeid, sealhulgas paroolipõhist autentimist, mitmefaktorilist autentimist (MFA), kiipkaardi autentimist ja sertifikaadipõhist autentimist. See pakub ka mitmesuguseid turvaelemente, nagu tingimusligipääsu poliitika, riskipõhine autentimine ja identiteedi kaitse. [6]

Azure Active Directory Connect

Objekte ja mandaate Azure Active Directory domeeniteenuste hallatavas domeenis saab luua kohalikult domeeni piires või sünkroniseerida Azure Active Directory rentnikult. Azure Active Directory Domain Services esmakordsel juurutamisel konfigureeritakse automaatne ühesuunaline sünkroniseerimine ja alustatakse Azure Active Directory objektide

kopeerimist. See ühesuunaline sünkroniseerimine jätkub taustal, et hoida Azure Active Directory hallatav domeen ajakohasena Azure Active Directory muudatustega. Azure Active Directory Domain Services'lt Azure Active Directory'le tagasi sünkroniseerimist ei toimu. [7]

Hübriidkeskkonnas saab objektid ja volikirjad kohapealsest Active Directory Domain Services domeenist sünkroniseerida Azure Active Directory Connecti abil Azure Active Directory'ga. Kui need objektid on edukalt sünkroonitud Azure Active Directory'ga, teeb automaatne taustsünkroonimine need objektid ja mandaadid hallatava domeeni abil rakendustele kättesaadavaks. [7]

2.3 Identiteedi- ja ligipääsuhaldus

Identiteedihaldus on olemasolevate identiteetide loomise, muutmise ja kustutamise protsess ning nende identiteetidega seotud turvaõiguste haldamine. Kuna süsteemide ja rakenduste arv, kus identiteete ja õigusi tuleb hallata kasvab pidevalt, on mõttekas automatiseerida identiteedi haldamise protsesse identiteedi- ja ligipääsuhaldussüsteemi abil. [8] Identiteedi- ja ligipääsuhaldus on turva- ja äridistsipliin, mis hõlmab erinevaid tehnoloogiaid ja äriprotsesse, aidates õigetel inimestel ja masinatel õigel ajal õigetele varadele ligi pääseda ning takistada volitamata ligipääsu. [9]

Identiteedi- ja ligipääsuhaldus määratleb ja haldab üksikute võrgukasutajate rolle ja ligipääsuõigusi ning tingimusi, mis määravad kasutajate õigused. Identiteedi- ja ligipääsuhaldust kasutatakse selleks, et kontrollida kasutaja ligipääsu kriitilisele teabele organisatsioonis. Iga ettevõtte jaoks on identiteedi- ja ligipääsuhaldus oluline, et olla oluliselt aktiivsem ärialgatuste toetamisel ja pidevalt muutuvate vastavusnõuete täitmisel. [10]

2.3.1 Identiteedi- ja ligipääsuhalduse aktuaalsus

Organisatsioonide jaoks on oluline kasutada identiteedi- ja ligipääsuhaldust, kuna see aitab tagada turvalisuse ja vastavuse ning suurendada organisatsiooni tootlikkust. See ei ole kehtiv vaid inimressursist rääkides, vaid ka mis tahes üksuse kohta, millele on määratud identiteet. Identiteedi- ja ligipääsu haldust muudab veel tähtsamaks asjaolu, et ligipääs rakendustele ja andmetele võib toimuda erinevatelt seadmetelt ja asukohtadest. [11]

Identiteedi- ja ligipääsu haldamine võimaldab ettevõttel hallata ligipääsu gruppide ja rollide põhiselt ning mitte individuaalselt. See lihtsustab oluliselt IT-toiminguid ja annab võimaluse IT-spetsialistidel keskenduda rohkem automatiseerimata projektidele, kus on vaja nende

teadmisi ja tähelepanu. Lisaks hindavad meeskonnaliikmed identiteedi- ja ligipääsuhaldust, sest see annab neile ligipääsu vajalikele tööriistadele, vähendades samaaegselt paroolide kompromiteerimist. [11]

Identiteedi- ja ligipääsuhaldust ei rakendata ainult töötajate, vaid ka töövõtjate, partnerite, klientide, robotite ja isegi koodisegmentide, näiteks APIde või mikroteenuste jaoks. Identiteedi- ja ligipääsuhaldus lahenduse tähtsus ettevõttes ei seisne ainult olulisuses, vaid muutub kriitiliselt tähtsaks vahendiks, kuna see suurendab tõhusust, vähendab kulusid, parandab ettevõtte tootlikkust ja optimeerib tehniliste süsteemide funktsionaalsust. [11]

Andmerikkumised võivad ettevõttele maksma minna miljoneid dollareid. 2019. aastal hindasid eksperdid, et üks andmerikkumine võib ettevõttele tekitada 200 000 dollari suuruse kahju. See on piisav, et väikeettevõte pankrotti viia. See arvestus ei võta arvesse suurte rikkumiste kulusid. *Identity Management Institute* on hinnanud, et andmerikkumised võivad 2024. aastaks ettevõtetele maksma minna koguni 5 triljonit dollarit; enamike ettevõtete jaoks on see rohkem raha, kui nad ühe aasta vältel teenivad. Lisaks võib rikkumine kaasa tuua klientide usalduse kaotuse. Range identiteedi- ja ligipääsukontroll aitab vähendada kompromiteerimise riski, piirates ründajate võimalusi süsteemidele ligipääsuks. [10]

Identiteedi- ja ligipääsuhaldus on olulised ka andmekaitse eeskirjade järgimise tagamisel. Regulatiivsed standardid, nagu GDPR, nõuavad, et organisatsioonid teaksid, millistel isikutel on ligipääs isikuandmetele. Lisaks on nõue, et kõik isikuandmetega seotud tegevused peavad olema logitud. Identiteedi- ja ligipääsuhaldus on siinkohal oluline vahend, sest see võimaldab hõlpsasti jälgida ligipääsu andmetele ning ettevõtted saavad täita oma andmekaitsealased nõuded. [10]

2.3.2 Identiteedi- ja ligipääsuhalduse tööpõhimõtted

Deproviseerimine on toiming, millega eemaldatakse võrgus kasutaja ligipääs rakendustele, süsteemidele ja andmetele. [11] Identiteedi- ja ligipääsu haldamine on küberturvalisuse distsipliin, mille eesmärk on tagada, et ainult volitatud inimesed pääsevad ligi asjakohastele andmetele ja ressurssidele, õigel ajal ja põhjendatud alustel. [11]

Identiteedihaldus on IT-süsteemide ja tarkvara kasutamine kasutajate ligipääsu ja nõuetele vastavuse haldamiseks. Identiteedi provisioneerimine on identiteedihalduse raamistiku põhikomponent, mille eesmärk on hallata kasutajakontosid ning tagada õigeaegne ja asjakohane ligipääs ressurssidele. [11]

Rollipõhine ligipääsuhaldus võimaldab ettevõttel luua ja rakendada täpset ligipääsu kontrol-

li, määrates õiguste kogumi vastavalt kasutaja rollile organisatsioonis. Õigused määratakse selle alusel, millise taseme ligipääsu konkreetsete kasutajakategooriate ülesannete täitmiseks vajavad. Teisisõnu võivad organisatsiooni erinevad inimesed olla täiesti erineva taseme ja ligipääsuõiguste tüüpidega, mis põhinevad ainult sellistel teguritel nagu nende tööülesanded ja -kohustused. [11]

Kasutaja autentimine on identiteedi- ja ligipääsuhaldus süsteemide põhifunktsioon, mille eesmärk on veenduda, et kasutaja on tõesti see, keda ta väidab end olevat, et saada ligipääs süsteemidele ja andmetele. Enamik inimesi teab traditsioonilisest autentimisest, kus kasutaja sisestab kasutajanime ja parooli sisselogimiseks; kaasaegsed kasutaja autentimislahendused ja tulevikulahendused kasutavad tehisintellekti ja muid tehnilisi edusamme organisatsiooni varade paremaks kaitsmiseks. [11]

2.3.3 Automaatne identiteedi- ja ligipääsuhaldus

Automatiseerimine: Madala riskitasemega funktsioonide automatiseerimine võimaldab ekspertidel keskenduda suurematele probleemidele ning äritegevuse kiirendamisele. See võib parandada IT-meeskonna tõhusust ja samal ajal vähendada IT-kulusid. Automatiseerimine lihtsustab kasutajate lisamisel, rollide muutumisel või eemaldamisel ligipääsu vastavat haldamist ning teeb seda sujuvamaks. [11]

Ettevõttesiseste identiteetidega seotud ohtude leevendamine: andmete rikkumisi võivad põhjustada ka hooletud või pahatahtlikud ettevõttesisesed ohud ning ainult töötajate teadlikkusele tuginemine ei ole piisav, kui puudub nõuetekohane tehnoloogia. Ettevõtetel on tarvis tõdeda, et ettevõttesisesed identiteedid ei ole ainult töötajad, vaid ka teised ettevõttega seotud identiteedid, näiteks partnerid, kliendid, serverid ja nutitelefonid. [11]

Nõuetele vastavuse lihtsustamine: Identiteedi- ja ligipääsu haldamine aitab organisatsioonidel reguleerida ligipääse, jälgida kasutamist ning tagada kõigi kasutajate, rakenduste ja andmete poliitikate jõustamine. See võimaldab automatiseerida regulatiivset jõustamist ja tõestada nõuetele vastavust. [11]

2.3.4 Identiteedi- ja ligipääsuhalduse funktsioonid

Kasutaja identiteedihaldus: hõlmab identiteetide loomist, muutmist ja kustutamist, mida saab teha nii iseseisvalt kui ka teiste kataloogidega integreerides. Lisaks saab uusi identiteete luua ka kasutajatele, kes vajavad erilist ligipääsu ettevõtte süsteemidele ja tööriistadele. [11]

Kasutajate loomine ja kustutamine: ligipääsu määramine hõlmab vajalike tööriistade ja ligipääsutasemete määramist kasutajale. Identiteedi- ja ligipääsuhalduse abil saab ligipääsu anda rolli, osakonna või mõne muu identiteedi kategooria alusel. See protsess säästab aega, kuna kasutaja ligipääs määratakse vastavalt tema rollile (RBAC - role-based access control) ning iga kasutaja jaoks seda eraldi tegema ei pea. [11]

Identiteedi- ja ligipääsuhaldus kasutab rollipõhist ligipääsu kontrolli (RBAC), kus kasutajad saavad ühe või mitu rolli vastavalt ametikohale või muudele kriteeriumitele. Sel viisil on võimalik vähendada kasutajate individuaalsete õiguste määramisega seotud aega ja riske ning samuti lihtsustada uute kasutajate lisamist ja nende õiguste määramist. Samuti võimaldab identiteedi- ja ligipääsuhaldus ettevõttel turberiskide minimeerimiseks kiiresti kasutajaid eemaldada. [11]

Auditeerimine ja aruandlus: Ettevõtted saavad identiteedi- ja ligipääsuhaldust auditeerida ning monitoorida. See hõlbustab vigade ja kahtlustäratava kasutajakäitmise tuvastamist ning seega kiirendab reageerimist. Kasutajate tegevusi salvestatakse ning sinna kuuluvad näiteks sisse- ja väljalogimise ajad, ressurssidele ja süsteemidele ligipääsemise ajad ning see, millisel viisil kasutaja end autentis. Seeläbi toetavad identiteedi- ja ligipääsuhaldus lahenduse aruanded kogu süsteemi turvalisust ja vastavust. [11]

2.4 Identiteedi- ja ligipääsuhaldus lahendused

Turul leidub mitmeid identiteedi- ja ligipääsuhalduse lahendusi, mis ühilduks Active Directory'ga. Enamik saadaolevatest lahendustest on kas tasulised või suletud lähtekoodiga. [12, 13, 11, 14]

1. MidPoint
2. OpenIAM
3. ForgeRock
4. SailPoint IdentityIQ

2.4.1 Identiteedihaldusplatvorm MidPoint

MidPoint on avatud lähtekoodiga identiteedihaldusplatvorm. MidPointil on suur hulk erinevaid funktsioone ja võimalusi. MidPointi haldab ja arendab avatud lähtekoodiga arendusele pühendunud ettevõte Evolveum. Kuna tegu on avatud lähtekoodiga projektiga on ka partnereid ja teisi arendajaid, kes aitavad kaasa MidPointi arengule. [14]

Üks peamisi erinevusi MidPointi ja teiste identiteedi- ja ligipääsuhaldus süsteemide vahel on see, et MidPoint on loodud pidades silmas praktilisust. Praktilisuse all peetakse silmas, et sagedased tegevused on hõlpsasti seadistatavad ja on võimalikult lihtsad, samas komplekssemad tegevused ja konfiguratsioonid on raskemad seadistamiseks, aga siiski tehtavad. Lisaks ei seata funktsionaalsusele piiranguid, kõik vajalik peaks olema kasutajal võimalik konfigureerida, isegi kui selleks on vajalik programmeerida lisamooduleid. [14]

Lihtsaid lahendusi, mis ei erine tavapärastest nõuetest, on lihtne rakendada. Enamik identiteedi- ja ligipääsuhaldus lahendusi on lihtne üles seada, lahendades levinud probleeme. Kiiresti juurutades võib kasu saada väga kiirelt, kuid muutub peagi kulukaks, kui nõuded muutuvad keerulisemaks ja ebatavalisemaks. [14]

MidPointi funktsioonide hulka kuuluvad:

1. Rollid ja rollipõhine ligipääsuhaldus
2. Organisatsiooniline struktuuri haldus
3. Kasutaja elutsükli haldus
4. Attribuutide haldus
5. Paroolide haldus
6. Ligipääsupoliitikate haldus
7. Kasutajate andmete ajakohasus
8. Kinnitusteprotsess
9. Automaatteavitused
10. Auditeerimine

Kuigi kogu see funktsionaalsus on olemas, on vaja seda vastavalt ettevõtte nõuetele konfigureerida. [14]

2.4.2 Programmeerimiskeel Python 3

Python 3 on programmeerimiskeel, mis on mõeldud lihtsaks ja efektiivseks koodi kirjutamiseks. See on üldotstarbeline programmeerimiskeel, mida kasutatakse mitmesugustes valdkondades, näiteks veebiarendus, andmeteadus, tehisintellekt, masinõpe ja automaatika. Python 3 on selle programmeerimiskeele kolmas peamine versioon, mis pakub mitmeid täiustusi ja muudatusi võrreldes eelmiste versioonidega. [15]

Pythoni keel on loetav ja kompaktne, mistõttu on see paljude programmeerijate jaoks eelistatud valik ning seda soovitatakse tihti algajatele esimese programmeerimiskeelena. Python 3 on objektorienteeritud programmeerimiskeel, mis tähendab, et seda saab kasuta-

da andmete modelleerimiseks ja struktureerimiseks kasutades klasside ja objektide abil töötavaid abstraktseid mudeleid. See aitab suurendada koodi taaskasutatavust ja lihtsustab keerukamate programmide loomist. [15]

Pythoni kogukond on äärmiselt aktiine ja toetav. Pythoni arendajatele on saadaval lai valik teeke ja tööriistu, mis teevad arendusprotsessi kiiremaks ja lihtsamaks. Pythoni peamine eelis on selle suur ja laienev standardteek, mis sisaldab paljusid kasulikke mooduleid, mille abil on võimalik kiiresti lahendada keerukaid probleeme ilma liigset koodi kirjutamata. [15]

Python 3 automatiseerimisplatvormina

Kuna Python on rajatud lihtsuse ja kasutusmugavuse põhimõtetele, on see hea tööriist, mida automatiseerimiseks kasutada. Selle loetav ja kompaktne süntaks kiirendab arendusprotsessi ning vähendab vigade esinemist. Automatiseerimise puhul on see eriti oluline, sest skriptid peavad töötama väga täpselt ning ilma tõrgeteta. [15]

Pythoni rikkalik standardteek sisaldab mitmesuguseid mooduleid ja funktsioone, mis võimaldavad programmeerijatel kiiresti lahendada keerukaid ülesandeid vaid mõne koodireaga. Need teegid sisaldavad ka palju tööriistu, mis on spetsiaalselt loodud erinevate automatiseerimisülesannete jaoks, näiteks failide töötlemine, e-kirjade saatmine ja ajastatud ülesannete haldamine. [15]

Pythoni aktiivne ja toetav kogukond on veel üks põhjus, miks just see programmeerimiskeel on ideaalne automatiseerimiseks. Tänu kogukonna panusele luuakse Pythonile pidevalt uusi teeke, tööriistu ja muid ressursse. See muudab automatiseerimisprojektide loomise veelgi lihtsamaks. Lisaks on kogukonna tugi väärtuslik algajaile ning neile, kes õpivad automatiseerimise põhimõtteid ja tavasid. [15]

Python on paindlik ning seda on lihtne integreerida teiste tehnoloogiatega, näiteks veebiserverid, andmebaasid ja operatsioonisüsteemid. See omadus mängib automatiseerimisprojektide puhul võtmerolli, mistõttu on Python automatiseerimisega seotud ülesannete lahendamisel mitmetes tööstusharudes eelistatuim valik. [15]

LDAP3 on RFC 4510 nõuetele vastav LDAP v3 Pythoni klienditeek. Kogu LDAP3 teek on kirjutatud nullist ja sama koodibaas töötab Python 2, Python 3, PyPy ja PyPy3 mis tahes süsteemis, kus see saab ligipääsu võrgule Pythoni ja selle standardteegi kaudu. [16]

2.5 Personalihaldussüsteem

Elektrooniline personalihaldussüsteem on paberivaba süsteem, mida kasutatakse ettevõttesiseste protsesside hõlbustamiseks ning paberipõhise süsteemi ja sellega kaasnevate probleemide lahendamiseks. Lisaks aitab elektrooniline personalihaldussüstee vähendada kulusid ja aega, mis pabersüsteemi ülalpidamisele kuluksid, sealhulgas personalijuhtide koormust. Ühtlasi paraneb teenuse kvaliteet, andmete täpsus ning ettevõte suurendab oma konkurentsieelist. [17]

Eriti suured muutused on toimunud personalijuhtimise protsessides ja tavades viimase paarikümne aasta vältel. Tehnoloogia areng on muutnud personaliprotsesse - personali planeerimine, värbamine, tulemusjuhtimine, töövoog ja kompensatsioon on muutunud ning seeläbi on vähenenud juhtide koormus töötajate haldamisel ja motiveerimisel. Taolistest arengutest saavad kasu kõik osapooled ning see parendab personalijuhtimise teenuse kvaliteeti. [18]

3. Ettevõtte ja protsesside kirjeldus

3.1 Ettevõte Magnetic MRO AS

Magnetic MRO AS (edaspidi ettevõte) on Euroopa Lennundusohutusameti ja Ameerika Ühendriikide Föderaalse Lennuameti poolt sertifitseeritud kommertslennukite parandus-, hooldus- ja ümberehitusteenust pakkuv ettevõte [19]. Magnetic MRO AS asutati aastal 1995 hooldusosakonnana Estonian Air AS-is. Aastal 2002 eraldus hooldusosakond Estonian Airist ning sellest sai eraldi seisev ettevõtte Maersk Air Maintenance Estonia. Maersk Air Maintenance Estonia vahetas oma nime aastal 2014 ning sellest sai Magnetic MRO AS. Hetkel on ettevõttel käsil järgmine nimemuutus, mille on tinginud suur rahvusvaheline kasv ja erinevate filiaalide asutamine ja ostmine üle maailma. Alates aastast 2018 kuulub Magnetic MRO AS Hiina aviatsiooni hiiule Guangzhou Hangxin Aviation Technology. [20]

Magnetic MRO AS pakub suurt hulka erinevaid tooteid ja teenuseid lennukioperaatoritele üle maailma. Peamised teenused on õhusõiduki baas- ja liinihooldus Airbus 320 ja Boeing 737 tüüpi lennukitele, kuid pakutakse ka varuosade müüki, lennuki mootorite remonti, hooldust, müüki ja hoiustamist, lennukihoolduse oskusteabe müüki ja interjööri tootearendust. [19, 20, 21]

Baashooldus kujutab endast erinevate tasemete tehnilist kontrolli, parandus-, kere-, interjööri- ja värvitöid ning seda tehakse Tallinna lennuväljal asuvas angaaris. Ettevõttel on Tallinnas EASA sertifitseeritud angaarid baashoolduse teostamiseks. [21]

Liinihooldus on lennuki kiirhooldus EASA direktiivi 145 järgi. Erinevalt baashooldusest ei ole see põhjalik ja selle raames ei teostata parandustöid. Liinihooldust pakub Direct Maintenance filiaal Eestis, Lätis, Norras, Poolas, Saksamaal, Taanis, Hollandis, Iirimaal, Sambias, Tansaanias, Keenias ja Ugandas. [21]

Ettevõttel on kontorid Eestis, Leedus, Serbias, Venemaal ja Austraalias ning liinihoolduseks vajalikud hooned Euroopas ja Aafrikas [21]. Ettevõttes töötab kõikide filiaalide peale kokku 534 töötajat, kellest umbes 100 töötab Tallinnas kontoris [22].

Magnetic MRO AS kogu käive tuleb ekspordist ning turul positsioneeritakse olema üks sihtpunkt õhusõidukitega seotud teenuste jaoks. [22] Teenuseid pakutakse enamasti Air-

bus 320 ja Boeing 737 lennuki tüüpidele. [19] Airbus 320 on Euroopas enim levinud lennukitüüp, mis tõttu on ettevõte turul heas positsioonis. [23]

3.1.1 Ettevõtte struktuur

Magnetic MRO AS koosneb neljast sektorist, mis omakorda koosnevad osakondadest. Kokku on osakondi ligi 30, mis on jagatud üle maailma paiknevate kontorite ja hooldusjaamade vahele ära.

Igal osakonnal on omad süsteemid ja andmed, millega töötatakse ja millele on vaja tagada ligipääsu, samal ajal kindlustades, et valedel töötajatel ei oleks ligipääsu andmetele, mida neil tööks vaja ei ole. Kokku on erinevaid süsteeme üle 100 ning need omakorda varieeruvad, osad on kohtvõrgu ressursid, teised on pilve ressursid.

3.2 Ettevõtte olemasolev identiteedi- ja ligipääsuhaldus

Ettevõttes on kasutusel identiteedi- ja ligipääsuhaldus protsessid, mis tuginevad suurele hulgale käsitsi tegevustele. Töötajate identiteedid ja ligipääsud paiknevad Active Directory kataloogiteenuses, kuhu neid luuakse käsitsi. Käesolev peatükk annab ülevaate ettevõttes kasutusel olevatest identiteedi- ja ligipääsuhaldusega seotud protsessidest, mõistetest ja tehnoloogiatest.

3.2.1 Töötaja identiteet

Igal töötajal on ettevõtte arvutisüsteemide kasutamise jaoks kasutaja kataloogiteenuses Active Directory. Töötaja kasutaja ja selles sisalduvad andmed moodustavad identiteedi. Töötaja kasutaja annab ligipääsu kõikidele ettevõtte IT ressurssidele nii sisevõrgus kui ka pilveteenustes. Kõik töötajate kasutajad on sünkroniseeritud analoogsesse kataloogiteenuses Azure Active Directory, mille kaudu on kasutajatel ligipääs pilveteenustele. Töötajate kasutajate andmeid kasutatakse osades süsteemides andmeväljade täitmiseks.

Kasutaja ja identiteedi seisukohast tähtsad andmeväljad Active Directorys on:

1. Eesnimi
2. Perekonnanimi
3. E-post
4. Telefoninumber
5. Osakond

6. Ametinimetus
7. Töötaja kood
8. Ülemus
9. Asukoht

Eeltoodud andmeväljad on tähtsad süsteemide toimimise eest. Kõik eeltoodud andmed on talletatud ka personalihaldussüsteemis. Kuna personalihaldussüsteem on töötaja andmete osas autoriteet, peaksid andmed olema uuendatud selle põhjal, kuidas nad on personalihaldussüsteemis. Paraku praeguses töötaja andmete muudatuste protsessis on märkimisväärsed vead andmete ajakohasus pole tagatud.

3.2.2 Töötaja ligipääsud

Ettevõtte ligipääsud on realiseeritud Active Directory turvarühmade kaudu. Enamik süsteeme suudavad päride Active Directory'st läbi LDAP protokolli kasutajaid ja nende turvarühmi ning seeläbi autentida kasutajaid. Turvarühmade kaudu rakendatakse lisaks veel Active Directory grupipoliitikaid süsteemi konfiguratsioonide peale surumiseks ja Azure Active Directory turvapoliitikate rakendamiseks. Azure Active Directory turvapoliitikate alla langevad turvanõuded, mis sätestavad, millistel juhtudel saab IT ressurssidele ligi. Turvanõuded käsitlevad erinevaid muutujaid nagu asukoht, seade, sihtrakendus ja autentimismeetod ja -tugevus.

Väiksem osa IT ressurssidest on sellised, kus peab lisaks Active Directory turvarühmadele, looma eraldi kasutaja või ligipääsu. Sellised süsteemid jagunevad omakorda kaheks, need kuhu IT saab luua vastava ligipääsu ja need, milleks peab võtma vastava süsteemi haldajaga ühendust. Selliste süsteemide puhul on eriti aktuaalne probleemid, mis tõstatuvad käsitsi tegevustest.

3.2.3 Personalihaldussüsteem

Ettevõttes on kasutusel pilvepõhine personalihaldussüsteem BambooHR. Personalihaldussüsteemis on kaetud suur osa personali osakonna protsesse ning toimib ka kataloogina kõikidest töötajatest ettevõttes koos nendega seonduvatest andmetest. Käesoleva töö skoobis on tähtsal kohal töötaja tööülesannetega seotud andmed, milleks on eelkõige osakond, asukoht ja ametinimetus.

Personalihaldussüsteemil on API liides, mille kaudu on võimalik pärida töötajate andmeid. Pärida on võimalik nii üksikuid töötajaid, otsida mingi kriteeriumi alusel või pärida

eelnevalt loodud raportit.

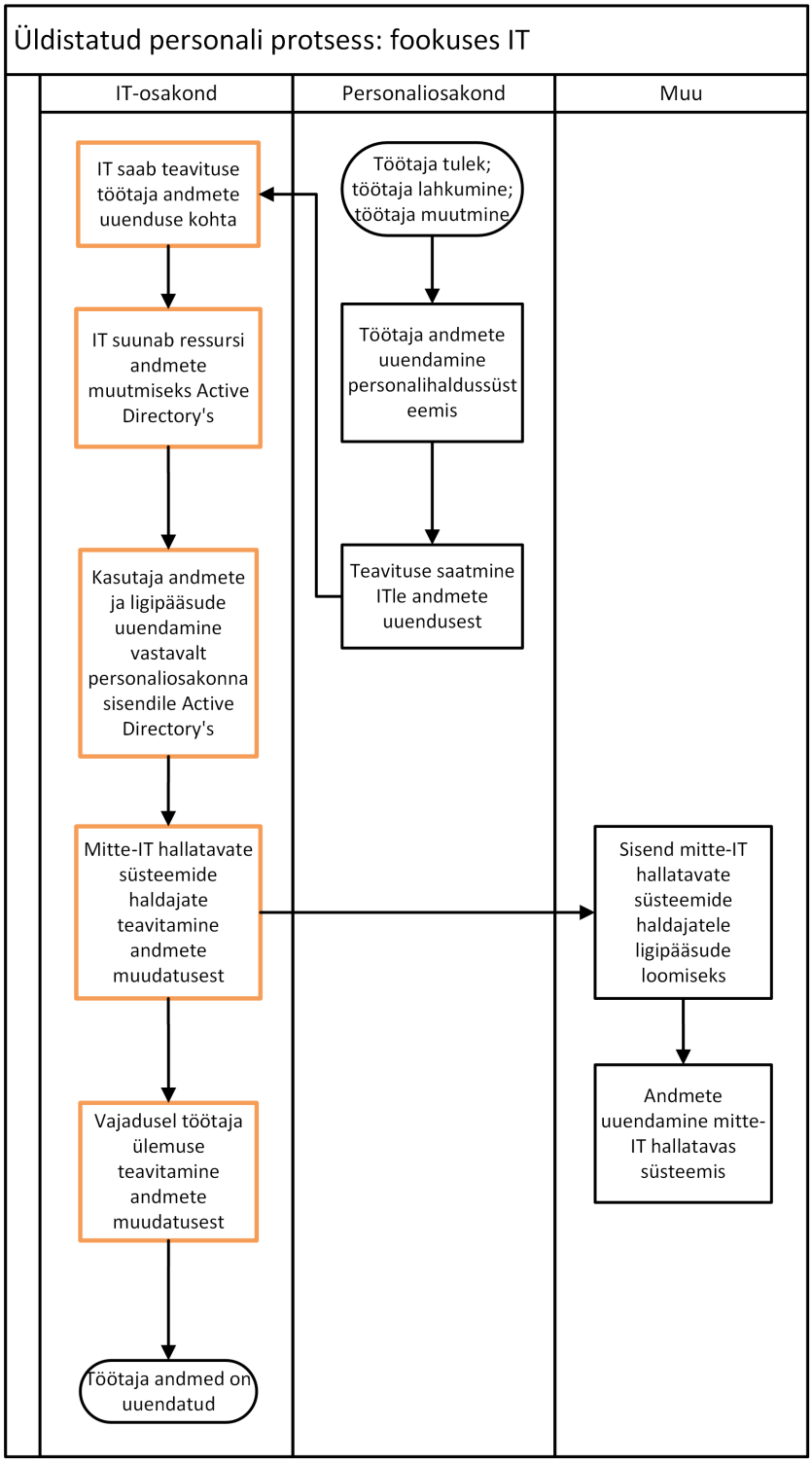
Personalihaldussüsteem on töötaja andmete osas autoriteet, kõikide järgnevate süsteemide andmed peaksid põhinema sellel, mis on määratud personalihaldussüsteemis. Töötaja ja tema identiteedi seisukohast, peaksid olema töötaja andmed Active Directorys samad, mis nad on personalihaldussüsteemis ning uuendama andmeid vastavalt, kui nad muutuvad.

3.2.4 Personali protsess

Ettevõttes on paigas kindlad protsessid töötajaga seotud sündmuste käsitlemiseks. Identiteedi- ja ligipääsuhalduse ja käesoleva töö kontekstis on tähtis vaadelda töötaja tööle tulemise, töölt lahkumise ja positsiooni vahetuse protsesse, kuna nende tegevustega kaasnevad muudatused töötaja identiteedis ning saadaolevates ligipääsudes.

Allpool oleval protsessi joonisel on toodud välja kõikide osapoolte tegevused mingi protsessi täitmiseks. Osapooled töötaja ja ülemus on konkreetsed isikud, IT ja HR on osakonnad, osakondade puhul täidab tegevust osakonna töötaja. Lisaks on joonistel veerg "Muu", mis tähistab kolmandaid osapooli, keda võib, aga ei pea konkreetse protsessi täitmisel olema. Näiteks tähistab "Muu"mingite süsteemide, kuhu IT osakonnal puudub ligipääs, haldajaid, kus selle süsteemi haldaja peab tegema vastavad kasutaja haldusega seotud tegevusi.

Joonisel 1 on näha personali protsessi, mis tegeleb töötaja kasutaja ja teiste IT ressursside haldamisega. Protsessi kujutis on üldistatud kujul ja annab täieliku ülevaate IT osakonna tegevustest. Protsess algab alati personaliosakonnast, mis on ettevõttes autoriteet töötajate ja nende andmete osas. Oranziga märgistatud tegevused hetkel käsitsi teostatavad tegevused, mida saaks automatiseerida.



Joonis 1. *Üldistatud personali protsess: fookuses IT.*

3.2.5 Kataloogiteenus Active Directory

Ettevõttes on kasutusel kataloogiteenus Active Directory, mida käideldakse sisevõrgus jooksvatel serveritel. Erinevad süsteemid, kuhu on loodud ligipääs läbi Active Directory kasutajate ja turvarühmade, saavad üle sisevõrgu autentida kasutajaid. Active Directorys on kõik ettevõtte töötajate kasutajad ja turvarühmad. Active Directory on üles seatud sünkroniseerima kasutajaid ja rühmi Azure Active Directorysse, et tagada töötajate identiteedid ja ligipääsud pilves.

Azure Active Directory pilveteenus on kasutusel kasutajate halduseks ja ligipääsude tagamiseks erinevatesse süsteemidesse, mis asuvad pilves. Erinevalt Active Directoryst on Azure Active Directory pilveteenus, seega piirdub selle funktsionaalsus ainult pilve ja üle avaliku võrgu kättesaadavate teenustega.

Active Directory teeb saadavaks LDAP protokollil põhineva liidese, mille kaudu on võimalik suhelda Active Directory serveriga, teha päringuid kasutajate kohta, muuta kasutajaid ja hallata ligipääsusid. Üle LDAP protokolli on võimalik liidestada erinevaid süsteeme, mis kasutavad Active Directoryt ühel või teisel moel.

3.2.6 Olemasoleva identiteedi- ja ligipääsuhalduse probleemid

Olemasolevate identiteedi- ja ligipääsuhaldus protsesside suurim puudujääk on käsitsi tegevuste tugev ülekaal. Manuaalsete tegevustega on märgatavalt kõrgem veaoht andmete sisestamisel ja tegevuste teostamisel.

Hetkel on väga paljude kasutajatega seotud andmed nagu näiteks positsioon ja osakond vananenud, sest kasutaja andmete muutmise protsessi (joonis 1) järgi, saadetakse ITle teavitus muudatustest, kuid nende täitmine ei ole kontrollitud. Käesolev probleem väljendub valedes andmetes erinevates süsteemides, mis võib kaasa tuua teisejärgulisi probleeme mujal, näiteks erinevad raporteerimis tarkvarad annavad valesid tulemusi, sest sisendandmed on väärad.

Vananenud andmetega kaasneb ka oht, et kasutajale on jäänud valed ligipääsud, mida uuenenud positsiooni või osakonnaga ei ole enam vaja ja on kuritarvitatavad.

Kasutajate ligipääsud, enamikel juhtudest Active Directory turvarühmad, pole ajakohased kuna puuduvad protsessid, mis käsitleks veendumist, et kasutajal on kõiki talle määratud ligipääse vaja ja andmete muutumisel ligipääsud püsiksid ajakohased. Olemasolevate

protsessidega on olukord suuresti selline, et ligipääse lisatakse juurde, kuniks on saavutatud piisavad ligipääsud, millega töötaja saab täita tööülesandeid, aga selline teguviis ei taga, et kasutajale ei jää mittevajalikke ligipääse külge.

4. Automaatne identiteedi- ja ligipääsuhaldus

Käesoleva ettevõtte identiteedi- ja ligipääsuhaldusega seotud probleemide lahendamiseks teostatakse järgnevad tegevused:

1. Riskianalüüsi koostamine
2. Probleemide kaardistamine
3. Nõuete kirjeldamine
4. Lahenduste pakkumine
5. Lahenduste juurutamine
6. Tulemuste analüüs
7. Katse lahenduse toimivusest

Riskianalüüsiga kaardistatakse ära peamised probleemid, mis on hetkeolukorras ja pakutakse nendele probleemidele lahendusi. Probleemidest ja pakutud lahendustest tekivad nõudmised mistahes identiteedi- ja ligipääsuhalduse lahendusele (edaspidi lahendus), mis olemasolevaid probleeme peaks lahendama. Nõudmisi teades, on võimalik valida ja põhjendada, missugune peaks lahendus olema.

Valitud lahendus juurutatakse, hinnatakse sobivust leitud probleemide lahendamiseks ning kirjeldatakse tööpõhimõtted. Lahenduse juurutamisega tekkinud riskidele antakse hinnang. Lahenduse toimivuse kohta uuritakse lahenduse väljundit, näiteks logisid, kontrollimaks, et muudatused personalihaldussüsteemist on peegeldatud Active Directorys. Tähtsal kohal on tulemused uute töötajate ja lahkunud töötajate kasutajatega seotud toimingute kohta.

4.1 Analüüs

4.1.1 Riskianalüüs

Käesolevas peatükis esitatakse riskianalüüs hetke identiteedi- ja ligipääsuhalduse protsessidest tulenevate riskide kohta. Väär identiteedi- ja ligipääsuhaldus võivad luua erinevaid riske organisatsioonile, nagu volitamata ligipääs ja andmete tervikluse, kättesaadavuse või konfidentsiaalsuse rikkumine.

Riskianalüüs on põhineb autori hinnangul, ajaloolistel andmetel, IT trendidel ja teadaolevatest nõrkustest süsteemides. Töö autor põhineb suuresti oma tööstaažile ja kogemusele

käesolevas ettevõttes, et olla pädev hindamaks riske, mis on seotud identiteedi- ja ligipääsuhaldusega.

Riskianalüüsis kasutatud mõisted:

1. Tõenäosus
    - Kõrge - Juhtumise tõenäoses üle 50%
    - Keskmine - Juhtumise tõenäoses 10% ja 50% vahel
    - Madal - Juhtumise tõenäoses alla 10%
2. Mõju
    - Suur - Suur mõju ärile. Hulgalised probleemid äriprotsessides, käideldavuses, tervikluses, konfidentsiaalsuses, ja mainekahju. Rahaline kahju üle 100000EUR.
    - Keskmine - Keskmine mõju ärile. Mitmed probleemid äriprotsessides, käideldavuses, tervikluses, konfidentsiaalsuses, ja mainekahju. Rahaline kahju kuni 100000EUR.
    - Väike - Minimaalne mõju ärile. Probleem äriprotsessides, käideldavuses, tervikluses või konfidentsiaalsuses. Rahaline kahju alla 10000EUR.

Järgnevalt on esitatud kvalitatiivne riskianalüüs illustreerimaks hetke olukorda identiteedi- ja ligipääsuhalduses:

1. Risk: Autoriseerimata ligipääs IT ressurssidele
    - Tõenäosus: Kõrge
    - Mõju: Suur
    - Maandamine:
        - Kasutajate ligipääsude ajakohasuse tagamise protsessi juurutamine
        - Kasutaja andmete ajakohasuse tagamise protsessi juurutamine
2. Risk: Kasutaja kompromiteerimine
    - Tõenäosus: Kõrge
    - Mõju: Suur
    - Maandamine:
        - Ajakohane ja tugev paroolipoliitika
        - Mitmeastmeline autentimine
        - Seadistatud ligipääsu poliitika (asukoht, seadme tüüp, võrk)
        - Kasutaja ligipääsude ajakohasuse tagamise protsessi juurutamine
3. Risk: Lahkuva töötaja kasutaja ja, või ligipääs(ud) ei ole suletud
    - Tõenäosus: Keskmine
    - Mõju: Keskmine

    - Maandamine:
        - Kasutaja ligipääsude ajakohasuse tagamise protsessi juurutamine
        - Kasutaja automaatse staatuse seadmise personalihaldussüsteemist protsessi juurutamine
4. Risk: Positsiooni muutva töötaja kasutajale jäävad vana positsiooni ligipääs(ud)
    - Tõenäosus: Kõrge
    - Mõju: Suur
    - Maandamine:
        - Kasutaja ligipääsude ajakohasuse tagamise protsessi juurutamine
        - Kasutaja automaatse staatuse seadmise personalihaldussüsteemist protsessi juurutamine
        - Kasutaja andmete ajakohasuse tagamise protsessi juurutamine
5. Risk: Positsiooni muutva töötaja kasutajal ei ole uue positsiooni ligipääsu(sid)
    - Tõenäosus: Kõrge
    - Mõju: Väike
    - Maandamine:
        - Kasutaja ligipääsude ajakohasuse tagamise protsessi juurutamine
        - Kasutaja automaatse staatuse seadmise personalihaldussüsteemist protsessi juurutamine
        - Kasutaja andmete ajakohasuse tagamise protsessi juurutamine
6. Risk: Kasutajal on käsitsi eemaldatud ligipääs(ud)
    - Tõenäosus: Väike
    - Mõju: Väike
    - Maandamine:
        - Kasutaja ligipääsude ajakohasuse tagamise protsessi juurutamine
7. Risk: Kasutajal on käsitsi lisatud ligipääs(ud)
    - Tõenäosus: Kõrge
    - Mõju: Suur
    - Maandamine:
        - Kasutaja ligipääsude ajakohasuse tagamise protsessi juurutamine

Riskianalüüsis leitud riskid, võivad omakorda moodustada komposiitriske, ehk mitu riski realiseeruvad korraga ühe kasutaja kontekstis. Sellisel juhul võib mõju akumuleeruda, aga ei ületa taset kõrge.

4.1.2 Probleemide ja lahenduste kaardistus

Riskianalüüsist leidub, et peamised riskid kasutajate, identiteedi- ja ligipääsuhaldusega on seotud sellega, et töötajatel on liiga palju ligipääse ja lahkunud töötajate kasutajaid ei ole

kinni pandud. Liiga paljude ligipääsude puhul seisneb probleem käsitsi tegevustes, millel on äärmiselt kõrge vea oht, ning ligipääse kas antakse liiga palju ja ei kontrollita, et mingid ligipääsu päriselt vaja oleks. Selliste riskide maandamiseks sobib väga hästi automaatne lahendus, mis suudaks otsustada, mis ligipääse töötajal vaja on ning neid vastavalt muuta.

Ülejäänud leitud riskide maandamiseks sobib samuti automaatne lahendus, mis suudaks töötaja andmeid ja staatust sättida personalihaldussüsteemi andmete põhjal. Uuendatud töötaja andmete põhjal on võimalik automaatikal teha täpsemaid ja ajakohasemaid otsuseid seoses kasutajate staatuse ja ligipääsudega. Seega tuleks käsitleda kogu lahendust ühe tervikuna, kuna selle erinevad põhifunktsioonid toetavad üksteist ühiste eesmärkide saavutamisel.

4.1.3 Identiteedi- ja ligipääsuhalduse lahenduse nõuete kaardistus

Automaatse lahenduse valiku seisukohast on tähtis kaardistada nõuded lahendusele, et oleks võimalik valida käesoleva olukorra jaoks kõige parem lahendus. Nõuded on esitatud kahes osas, üldnõuded lahendusele ja toetatud protseduurid.

Lahenduse üldnõuded:

1. Ühilduvus Active Directory'ga kasutaja loomise sihtpunktina
2. Ühilduvus personalihaldussüsteemiga autoriteedina andmete pärimiseks üle API ühenduse
3. Lahenduse ja mistahes sõltuva süsteemi soetamise, loomise ja, või käitlemise kulu on minimaalne
4. Active Directory andmete ja ligipääsude ajakohasuse kontroll ja, või uuendamine mitte harvemini kui iga 30 minuti tagant
5. Iseseisev toimimine põhifunktsioonide ulatuses

Lahendus peab suutma teostada järgnevaid tegevusi:

1. Uuele töötajale kasutaja loomine
2. Lahkuva töötaja kasutaja sulgemine
3. Kasutaja andmete uuendamine personalihaldussüsteemist
4. Kasutaja ligipääsude ajakohasena hoidmine
5. Ligipääsude lisamine kasutajale rollipõhiselt
6. Ligipääsude sulgemine kasutajalt rollipõhiselt
7. Muutvate tegevuste logimine
8. Veateadete logimine

9. E-posti teavituste saatmine

4.1.4 Lahenduse valiku põhjendus

Soovitud lahenduse realiseerimiseks otsustati luua kogumik Python 3 skripte. Lahenduse valimisel lähtuti eespool kirjeldatud nõuetest ning leiti, et Python 3 põhine lahendus tagaks parima ühtivuse nõuetega. Python 3 lahenduse ilmselge eelis on, et seda saab kõige hõlpsamalt ja kindlamalt ühitada olemasolevatesse protsessidesse, mis teeb selle juurutamise suhteliselt valutuks.

Python 3 lahendusel esineb miinuseid, mis raskendavad selle käitlemist. Iseloodud lahendustega luuakse ettevõtte IT osakonnale lisa ülesandeid lahenduse käitlemiseks, tehniliseks toeks, vigade paranduseks ja edasisteks arendusteks. Lisaks eeldab sellise lahenduse käitlemine, et lahendus on hästi dokumenteeritud ja hallatav, et erinevad IT osakonna töötajad suudaksid lahenduse haldust üle võtta vajadusel.

Python 3 lahendus katab ära kõik nõudmised ning sellel on lisaks eelised nagu suur hulk teeke, mis võimaldavad keelt laiendada vastavalt kasutusjuhule, suhteliselt lihtne programmeerimiskeele süntaks ja platvormi agnostilisus. Python 3 suudab ühenduda personalihaldussüsteemi API külge sisseehitatud teekidega "requests"ja "json", LDAP suhtluseks on võimalik kasutada teeki "ldap3".

Peale Python 3 lahenduse kaaluti ka teisi lahendusi. Personalihaldussüsteem pakub automatiseerimise teenust kasutajate loomiseks, aga see töötab ainult Azure Active Directoryga, seega ei sobi käesoleva lahenduseks. Suur hulk identiteedi- ja ligipääsuhaldussüsteeme jäid valikust välja, kuna nende kasutus on ühel või teisel moel tasuline, mis ei ole kooskõlas esitatud nõuetega. Tasulised lahendused olid näiteks OpenIAM, ForgeRock ja SailPoint IdentityIQ.

Eelnevatele lahendustele lisaks, oli valikus ja identiteeti- ja ligipääsuhaldussüsteem Midpoint. Midpoint esmapilgu on täpselt õige lahendus käesolevatele nõuetele, kuid lähemal vaatlusel esines selle funktsionaalsuse osas piisavalt palju teadmatust, et see jäi valikust välja. Nimelt ei suudetud tuvastada, kas Midpoint suudab suhelda personalihaldussüsteemi APIga korrektselt, missugused võimalused on kasutajate automaatseks loomiseks ning kas kõik soovitud tegevused oleks realiseeritud. Midpointi käideldamise ja juurutamisega seotud kulud, eriti ajaline, ei olnud ette ennustatavad.

4.2 Automaatse identiteedi- ja ligipääsuhalduse lahendus

Lahendus seisneb inimliidese ehk personali protsessides IT osakonna käsitsi tegevuste asendamises automatiseeritud tegevustega. Lahendus tegutseb iga 30 minuti tagant ajastatud tegevusena, mille käigus kontrollitakse üle personalihaldussüsteemi andmed, võrreldakse Active Directory andmetega ja sünkroniseeritakse muudatused, käesoleva sünkronisatsiooni protsessis on personalihaldussüsteem autoriteet. Sünkronisatsioon veendub, et kõik vajalikud andmeväljad oleks olemas ning andmed oleks uusimad.

Automaatne identiteedi- ja ligipääsuhaldus lahendus on realiseeritud Python 3 programmeerimiskeeles. Python 3 lahendust käivitatakse automaatselt kasutades croni. Lahendus on ülesseatud operatsioonisüsteemil Ubuntu Server 22.04 LTS, mis on kergesti hallatav ja kuluefektiivne käesoleva lahenduse jaoks.

4.2.1 Lahenduse moodulid

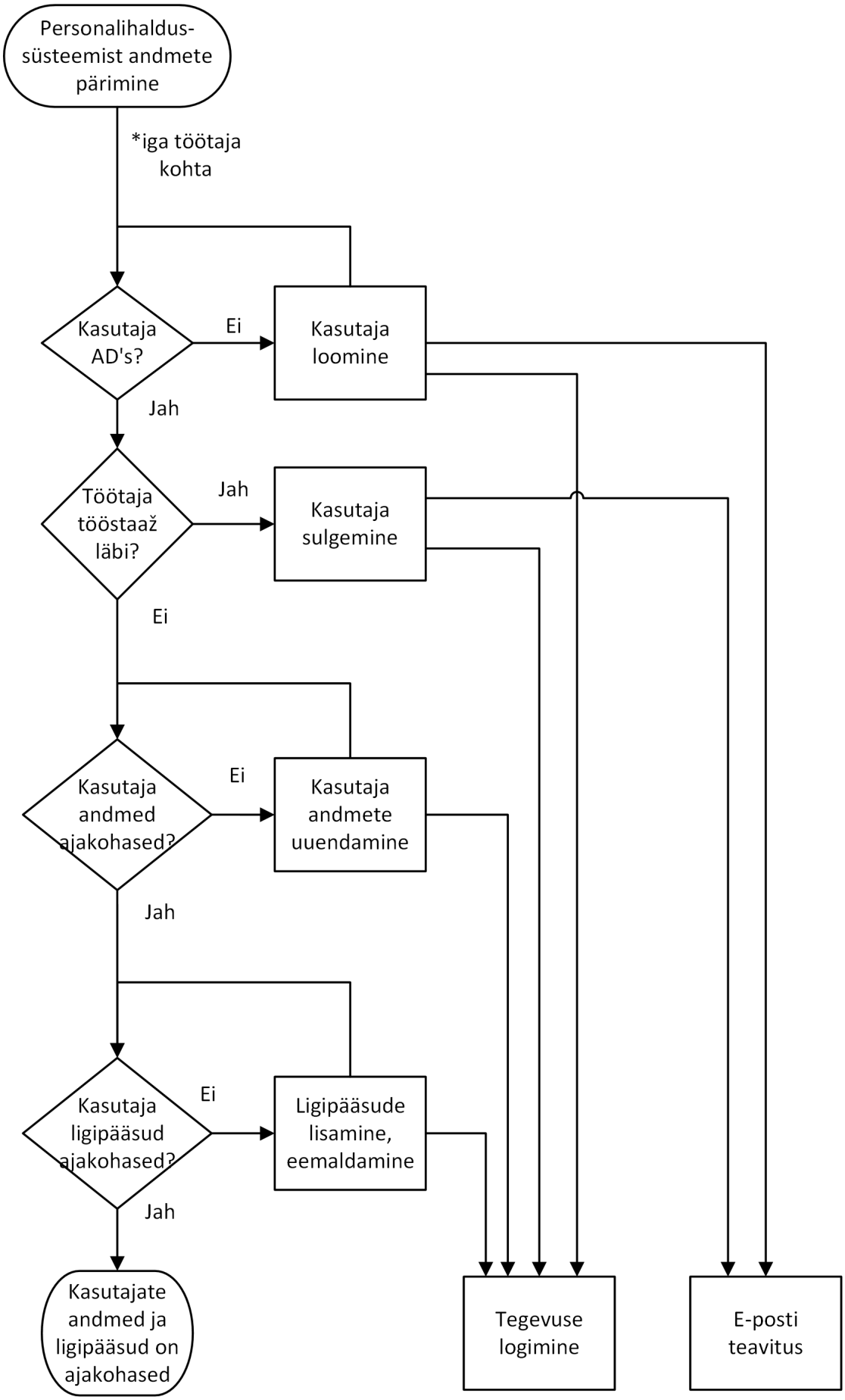
Põhimoodul ehk kasutajahaldus

Lahenduse põhimoodulis on kõik kasutajahaldusega seotud tegevused, milleks on uusimate andmete pärimine personalihaldussüsteemist, äriloogika ja LDAP operatsioonid. LDAP operatsioonidest on realiseeritud kasutajaobjektide loomine, liigutamine, muutmine ning turvarühmade kasutajatehaldus.

Põhimoodul peale andmete pärimist personalihaldussüsteemist loob iga töötaja kohta objekti. Töötaja objekt tagab hõlpsama ja tõhusama andmete kättesaamise.

Põhimoodul kasutab teisi alammooduleid erinevate toetavate tegevuste teostamiseks. Alammoodulid on loodud e-posti teavitusteks, teadete logimiseks ja ligipääsuhalduseks. Alammoodulite sisendiks on töötaja objekt.

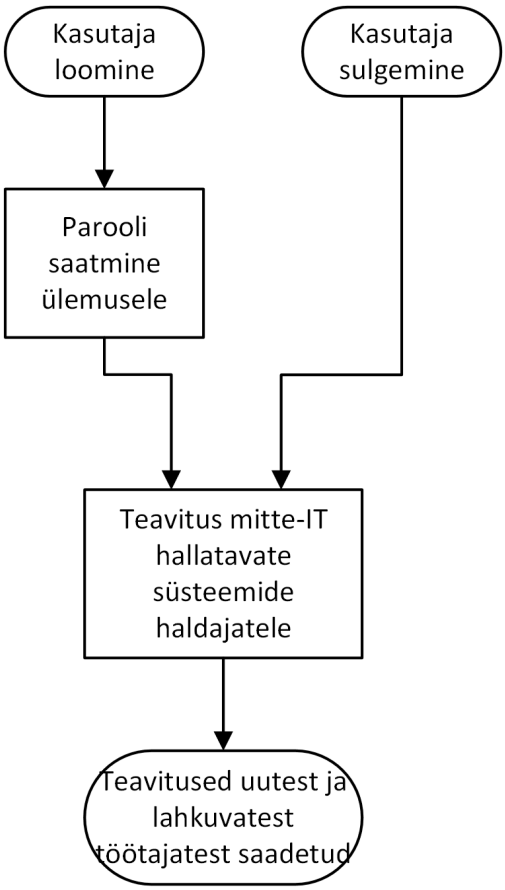
Active Directory kasutajate otsimine tugineb töötaja koodi võrdlusele. Igal töötajal ja kasutajal on unikaalne töötaja kood, mis võimaldab töötajat identifitseerida süsteemide üleselt.



Joonis 2. *Identiteedi- ja ligipääsuhalduse põhimooduli toimimine.*

Joonisel 2 on märgitud eraldi tegevustena tegevuste logimine ja e-posti teavitused. E-posti teavituste protsess on kirjeldatud joonisel 3.

E-posti teavitused



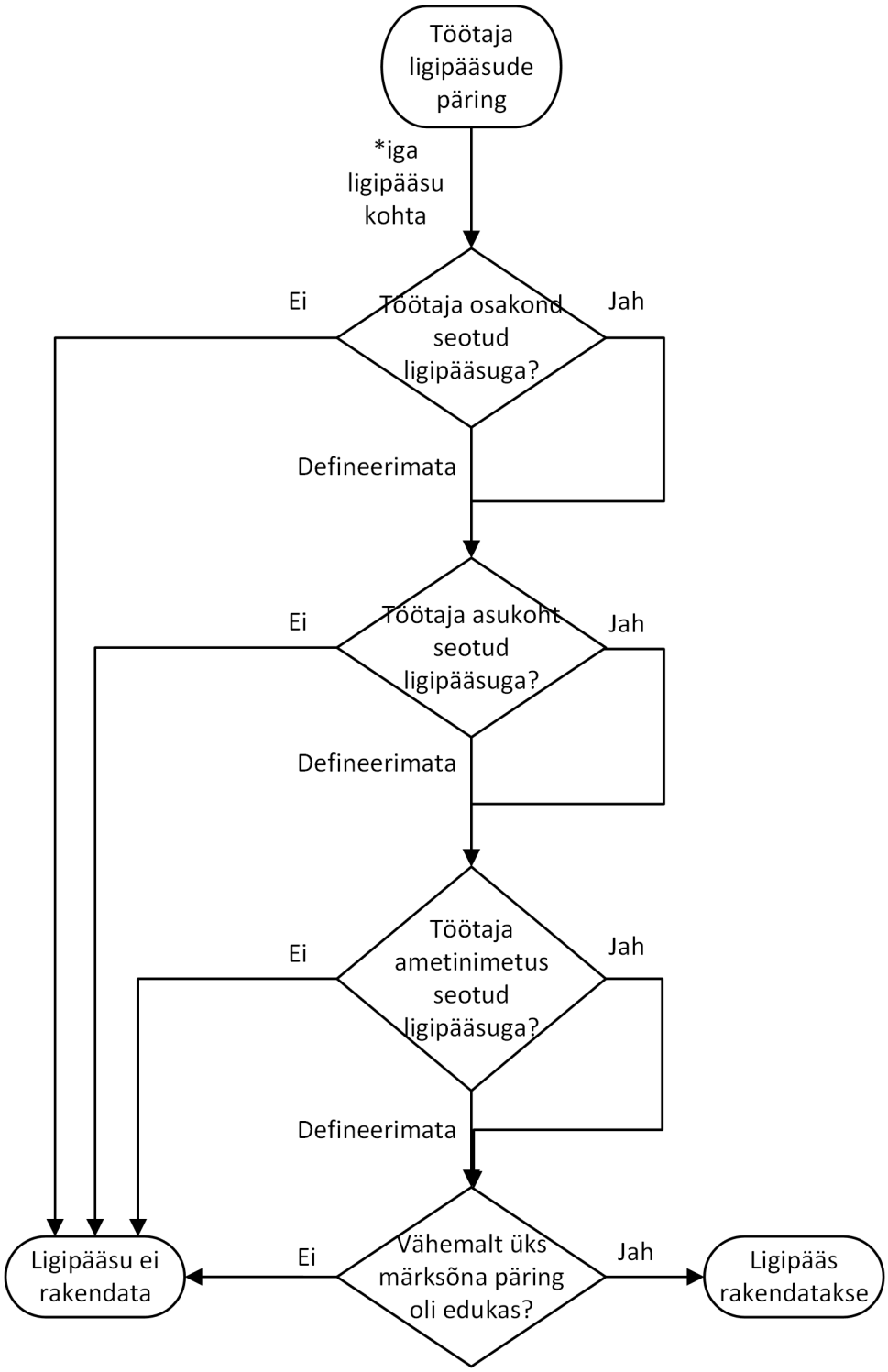
Joonis 3. *E-posti teavituste saatmine.*

Ligipääsuhaldus

Ligipääsuhaldus tegeleb töötajate ligipääsude kontrollimise, pärimise ja haldamisega. Ligipääsuhalduse alammoodul rakendab eelgenereeritud andmebaasi, kus on informatsioon kõikidest ligipääsudest ja nende rakendamisest. Loodud ligipääsuhalduse loogika tagab ligipääsude ajakohasuse ning pakub IT osakonnale vahendid ligipääse ja nende rakendumist kontrollida ja hallata.

Iga ligipääsu kohta on märgitud märksõnad ja nende kombinatsioonid, kui seda ligipääsu peaks rakendatama. Iga ligipääsu ja märksõna kombinatsiooni kohta on lisaks veel informatsioon ligipääsu rakendamisest, ligipääs saab olla kohustuslik, vabatahtlik ja keelatud. Kohustuslikke ligipääse rakendatakse kõikidele kasutajatele iga kord kui kasutaja suunal tehakse päring kas tema ligipääsud on ajakohased. Vabatahtlikud ligipääsud rakendatakse ainult kasutaja loomisel ning neid ligipääse saab soovi korral eemaldada. Keelatud ligipääsud toimivad sarnaselt kohustuslikule, et nende olemasolu kontrollitakse iga päringuga,

kuid kui kasutajale on ligipääs antud, siis see võetakse maha. Vastavalt ettevõtte äriprotsessidele ja vajadustele, on ligipääsuhalduseks kasutatavad märksõnad töötaja osakond, ametinimetus ja asukoht.



Joonis 4. *Ligipääsude pärimise protsess.*

Logimine

Lahenduses on realiseeritud tegevuste logimine. Logimine toimib vastavalt esitatud nõuetele, et kõikide muutvate operatsioonide kohta on logiteade. Logid on kuvatud lahenduse käivitamisel konsoolis kui ka kirjutatud logifaili. Logifailid asuvad logi kaustas, mis omakorda asub lahenduse kaustas.

Logifailide terviklus on kaitstud läbi lugemis- ja kirjutusõiguse lubamise ainult kasutajakontole, mille alt lahendus jookseb. Faili õigusi saab muuta ainult süsteemiadministraator.

Mooduli ülesehitus on lihtsakoeline, moodulisse on võimalik programselt saata andmeid ja sõnumeid ning tekitada logikirjeid. Moodulis on määratud, millistesse kohtadesse logikirjeid luuakse. Vaikimisi on logikirjed näidatud konsoolis ja salvestatud tekstifaili. Uute logide sihtkohtade ja tehnoloogiate lisamine on triviaalse keerukusega.

4.2.2 Lahenduse tööprotsessid

Kasutaja loomine

Kasutaja loomisel luuakse kataloogiteenuses Active Director uus kasutajaobjekt. Kasutaja luuakse põhinedes personalihaldussüsteemi andmetele. Kasutaja loomisel on tähtis töötaja kood, millega on võimalik viia kokku töötajat ja tema kasutuses olevat kasutajat. Kasutaja loomisel päritakse töötaja andmetega ligipääsuhalduse alammoodulit, et tuvastada vajalikud ligipääsud ning lisada need kasutajale. Kasutaja loomine tekitab logikirjeid ja lisaks saadetakse e-posti teavitus asjaosalistele.

Kasutaja sulgemine

Kasutaja sulgemine toimub automaatselt põhinedes andmetele personalihaldussüsteemis. Personalihaldussüsteemis on võimalik märkida töötajale viimane tööpäev ning peale selle kuupäeva möödumist muutub töötaja inaktiivseks. Lisaks on personali osakonnal võimalik töötaja märkida koheselt inaktiivseks, sellisel juhul läheb kasutaja sulgemiseni kuni 30 minutit, mis tuleneb lahenduse käivitamise intervallist. Kasutajate sulgemised logitakse.

Kõik inaktiivsed töötajad kontrollitakse üle, et nende nimel ei oleks aktiivset kasutajat. Inaktiivse töötaja aktiivsed kasutajad suletakse. Sulgemine on paroolivahetamine, kasutajaobjekti sulgemine, kasutaja liigutamine suletud kasutajate talletamiseks mõeldud kausta ja ligipääsude eemaldamine.

Kasutaja andmete ajakohasuse tagamine

Kasutajate andmete ajakohasuse tagamine on realiseeritud andmete võrdlustena personalihaldussüsteemi ja Active Directory vahel. Kui töötajaid läbi itereerides avastatakse, et mingid andmeväljad ei ole võrdsed, siis asendatakse andmed Active Directory's sellega, mis on personalihaldussüsteemis. Personalihaldussüsteem on alati autoriteet andmete ajakohasuse osas.

Kasutaja andmete ajakohasuse kontroll ja uuendamine katab järgnevaid andmevälju:

1. Eesnimi
2. Perenimi
3. Töötaja kood
4. Asukoht
5. Osakond
6. Ametinimetus
7. Ülemus

Lahenduse käivitamine 30-minutilise intervalliga tagab, et kasutaja andmed on ajakohased. Kõik muudatused kasutaja andmetele logitakse vastavalt sätetele, mis on määratud logimise alammoodulis.

Kasutaja ligipääsude ajakohasena hoidmine

Ligipääsude ajakohastamisega pöördutakse ligipääsude alammooduli poole, kust päritakse töötaja andmetega, millised ligipääsud peaksid töötajal olema ning võrreldakse töötaja hetke ligipääsudega. Kui leitakse erinevusi töötaja ligipääsudes, tehakse töötaja ligipääsud vastavaks sellele, mis ligipääsud alammoodul tagastas.

Ligipääsude päring tagastab töötaja kohta loetelu ligipääsudest. Ligipääsudega koos on informatsioon, kas ligipääs on kohustuslik, vabatahtlik või keelatud. Kohustuslikud ligipääsud surutakse kasutajale peale, veendutakse, et ligipääs on määratud. Keelatud ligipääsud võrreldakse töötaja ligipääsudega ja kui leitakse, et töötajal on mingi keelatud ligipääs, siis see ligipääs eemaldatakse.

Lahenduse käivitamine 30-minutilise intervalliga tagab, et kasutaja ligipääsud on ajakohased. Kõik muudatused kasutaja ligipääsudele logitakse vastavalt sätetele, mis on määratud logimise alammoodulis.

Rollipõhine ligipääsude pärimine

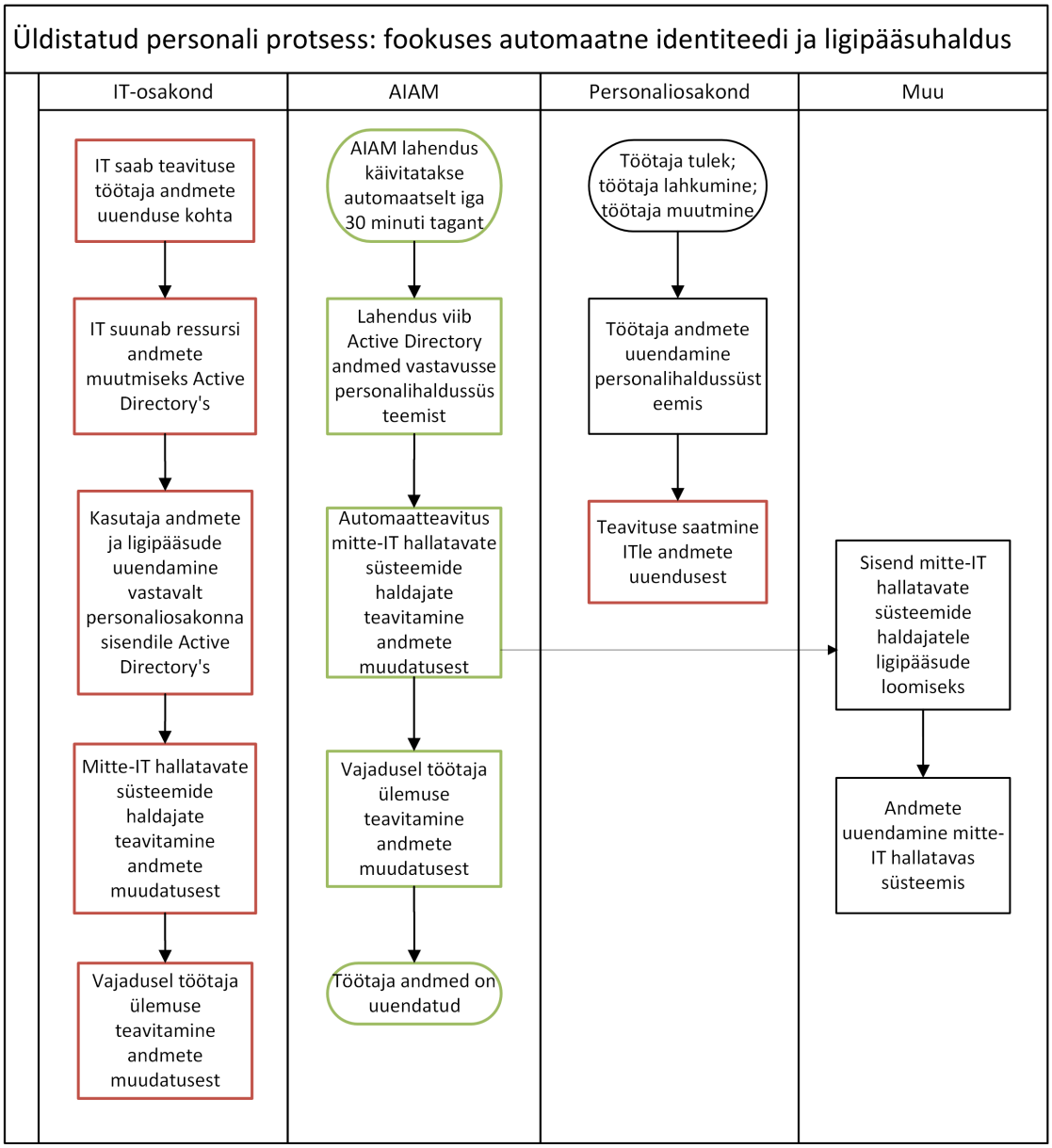
Ligipääsude alammoodulis realiseeritud märksõnadele tuginev ligipääsuhaldus, määramine ja pärimine on rollipõhine ligipääsuhaldus. Töötajale omased andmed osakond, ametinimetus ja asukoht moodustavad töötaja rolli. Iga märksõna kombinatsioon on omaette roll ning igal rollil on talle omased ligipääsud.

Märksõnadele lisaks, on igal ligipääsul ka kaal. Väiksema kaaluga ligipääsud on prioriteetsemad kui suurema kaaluga. Kui ligipääsude operatsiooniga tekib konflikt, et mingi ligipääs on mitmekordselt ja erineva staatusega, siis võrreldakse ligipääsu kaalu ja väiksema kaaluga ligipääs ja staatus jääb peale.

4.2.3 Uuendatud personali protsessid

Automaatne identiteedi- ja ligipääsuhaldus lahendus on muutnud personali protsesse. Varasemad tegevused IT osakonna poolt, mida teostati käsitsi, on asendatud automaatikaga. Joonisel 5 on märgitud ära vana personali protsess ja uuendatud protsess, kus automaatika on asendatud IT tegevused. Jooniselt tuleb välja, et IT tegevuste hulk on minimaliseeritud ning identiteedi- ja ligipääsuhaldusega seotud tegevused on lahendus täielikult üle võtnud.

Joonisel 5 on punasega märgitud tegevused, mis pole enam aktuaalsed peale lahenduse kasutusele võttu. Rohelisega märgitud tegevused on need, mida teostab identiteedi- ja ligipääsulahendus.



Joonis 5. *Üldistatud personali protsess: fookuses automaatne identiteedi- ja ligipääsuhaldus*

4.3 Lahenduse väljundi analüüs

Automaatse identiteedi- ja ligipääsuhaldus lahenduse tulemusena muutusid töötajatega seotud protsessid sujuvamaks ja töökindlamaks, kuna eelnevalt käsitsi tegevused asendati automatiseeritud lahendusega. Automatiseeritud lahendus suutis teha sama töö ära proaktiivsemalt ja veakindlamalt.

Samuti muutusid Active Directory kasutajate andmed ajakohaseks ja uuendati andmetega personalihaldussüsteemist. Lahendus on jooksnud alates märtsist 2023. Lahendus on senini sulgenud 8 kasutajat plaaniliselt, mis on tavapärane hulk kahe kuu lõikes. Identiteedi- ja

ligipääsuhaldus lahendus leidis ja uuendas 200 kasutaja andmeid, mis illustreerib algprobleemi mastaapi.

Identiteedi- ja ligipääsuhaldus lahendus suutis tuvastada ja sulgeda 15 kasutajat, mis olid avatud, kuigi töötaja ei olnud enam aktiivne. Varem sulgemata kasutajate sulgemine tagantjärele illustreerib väga tugevalt algprobleemi olemust ning on tõenduseks lahenduse vajalikkusest.

Identiteedi- ja ligipääsuhaldus lahendus muutis ulatuslikult ligipääsude kasutust ja nendega kaasnevaid protsesse. Töötajate kasutajatel on nüüd keskselt automatiseeritult hallatavad ligipääsud, mis tagavad, et kasutajatel on alati neile kohased ligipääsud. Käesolev muudatus vähendab suuresti riskianalüüsis toodud riskide realiseerimise võimalust. Riskianalüüsis toodud riskid on maandatud ning olenevalt realiseeruvast riskist, on ära hoitud kahjud suurusjärgus 100000EUR ja mainekahju.

4.4 Tuleviku arengusuunad

Identiteedi- ja ligipääsuhaldus lahendus on hetkel prototüübi tasemel ja toimib edukalt. Küll aga on hulgaliselt arengusuundi käesoleva lahendusega, et muuta seda töökindlamaks, kasutajasõbralikumaks ja laiendada funktsionaalsust.

Lahenduse logimist saaks parandada, kui võtta kasutusele standardne formaat, mis võimaldab logide tõhusamat analüüsi. Logide alamoodulile saaks arendada syslog toe, et oleks võimalik saata logisid kesksesse logiserverisse, mis võimaldaks paremat logide analüüsi. Lisaks annaks lahendusele lisada monitooringu, et tuvastada kahtlaseid olukordi kui lahendus näiteks ei tööta.

Lahendust saaks ülesseada virtualiseeritud konteinerisse. Konteineril on mõned eelised klassikalise serveriga, näiteks suurem sõltumatus platvormist, väiksem ressursi kasutus, monitooringu võimalused ja vähem kompleksne haldus.

Lahenduse teavitusi saaks ümber teha, näiteks teatud teateid luua automaatselt kasutajatoe süsteemis pöördumisena, või olenevalt sihtgrupist, saatma Microsoft Teamsis sõnumina osasid teateid.

Hetkel on lahendus puhtalt konsooliliidesega programm ning puudub graafiline kasutajaliides. Kasutajaliidese arendus lubaks hõlpsamat haldust kogu süsteemist, muudaks süsteemi kättesaadavamaks ja maandaks lahenduse opereerimisega seotud riske maandada.

5. Kokkuvõte

Käesoleva bakalaureusetöö põhieesmärgiks oli Mangetic MRO AS ettevõttes automaatse identiteedi- ja ligipääsuhalduse juurutamine. Esimeses osas on kirjeldatud identiteedi- ja ligipääsuhaldus süsteemide tausta, põhimõtteid, valmis lahendusi turul ning kataloogiteenuseid.

Teises osas antakse ülevaade Magnetic MRO AS struktuurist, kasutusel olevatest tehnoloogiatest, identiteetidest ja ligipääsudest ettevõte kontekstis ning personali protsessidest.

Kolmandas osas koostati riskianalüüs, seati nõuded juurutatavale identiteedi- ja ligipääsuhaldus lahendusele, valiti lahendus, mis on kõige sobivam käesoleva ettevõtte kontekstis, juurutati valitud lahendus, võrreldi personali protsesse enne ja pärast seisuga, veenduti lahenduse toimivuses lahenduse väljundi põhjal ning võrrelduna personalihaldussüsteemi sisestatud andmetega ja anti hinnang lahendusele.

Töö tulemusena valmis automaatse identiteedi- ja ligipääsuhalduse lahenduse prototüüp, mida kasutatakse Magnetic MRO AS-s käesoleva töö valmimise ajal. Autor leiab, et loodud lahendust muudaks paremaks logi mooduli ümber tegemine, teavituste süsteemi parandamine, lahenduse konteinerdamine ja auditeerimine. Kuna käesolev lahendus koormab IT osakonda uute riskide näol, on võimalik asendada loodud lahendus valmis tootega, üks selline toode oleks paljulubav lahendus Midpoint.

Kasutatud kirjandus

[1] M. Becker ja M. Drew. „Overcoming the challenges in deploying user provisioning/identity access management backbone“. *BT Technology Journal* 23 (2005), lk. 71–79.

[2] OpenLDAP Foundation. *Introduction to OpenLDAP Directory Services*. [Accessed: 24-04-2023]. URL: https://www.openldap.org/doc/admin24/intro.html.

[3] J. Sermersheim. *Lightweight Directory Access Protocol (LDAP): The Protocol*. [Accessed: 24-04-2023]. URL: https://www.rfc-editor.org/rfc/rfc4511.txt.

[4] *Active Directory Domain Services*. [Accessed: 24-04-2023]. URL: https://learn.microsoft.com/en-us/windows/win32/ad/active-directory-domain-services.

[5] *Windows Server 2003 Technical Reference*. [Accessed: 24-04-2023]. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758478(v=ws.10).

[6] *Azure Active Directory and identity management*. [Accessed: 24-04-2023]. URL: https://www.skillzcafe.com/blog/microsoft/azure/azure-active-directory-and-identity-management.

[7] *Azure AD Domain Services documentation*. [Accessed: 24-04-2023]. URL: https://learn.microsoft.com/en-us/azure/active-directory-domain-services/.

[8] *IAM Concepts*. [Accessed: 24-04-2023]. URL: https://web.archive.org/web/20170606124911/http://hitachi-id.com/resource/iam-concepts/.

[9] *Identity and Access Management (IAM)*. [Accessed: 24-04-2023]. URL: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam.

[10] Vangie Beal. *Identity and Access Management (IAM)*. [Accessed: 24-04-2023]. URL: https://www.webopedia.com/definitions/iam/.

[11] *What Is Identity and Access Management (IAM)?* [Accessed: 24-04-2023]. URL: https://www.sailpoint.com/identity-library/identity-and-access-management/.

[12] OpenIAM. *Solutions for Managing Active Directory*. [Accessed: 24-04-2023]. URL: https://www.openiam.com/solutions-for-managing-active-directory.

[13] ForgeRock. *Workforce Identity and Access Management*. [Accessed: 24-04-2023]. URL: https://www.forgerock.com/digital-identity/employee-identity-access-management.

[14] Radovan Semančík et al. *Practical Identity Management With MidPoint*. [Accessed: 24-04-2023]. URL: https://docs.evolveum.com/book/practical-identity-management-with-midpoint.html.

[15] *Python 3.11.3 documentation*. [Accessed: 24-04-2023]. URL: https://docs.python.org/3/.

[16] *The ldap3 project*. [Accessed: 24-04-2023]. URL: https://ldap3.readthedocs.io/en/latest/welcome.html.

[17] Hanan M. Shukur *et al.* „Design and Implementation of Electronic Enterprise University Human Resource Management System“. *Journal of Physics: Conference Series* 1804.1 (veebruar 2021), lk. 012058. DOI: 10.1088/1742-6596/1804/1/012058. URL: https://dx.doi.org/10.1088/1742-6596/1804/1/012058.

[18] Dianna L. Stone ja James H. Dulebohn. „Emerging issues in theory and research on electronic human resource management (eHRM)“. eng. *Human resource management review* 23.1 (2013), lk. 1–5. ISSN: 1053-4822.

[19] Magnetic MRO AS. *Ettevõttest*. [Accessed: 24-04-2023]. URL: https://magneticmro.com/ettevottest/.

[20] Magnetic MRO AS. *About us: History*. [Accessed: 24-04-2023]. URL: https://magneticmro.com/company/about-us/history/.

[21] Magnetic MRO AS. *Magnetic MRO Services*. [Accessed: 24-04-2023]. URL: https://magneticmro.com/services/.

[22] BNS. *Lennukihooldaja Magnetic MRO langes 13,6 miljoniga kahjumisse*. [Vaadatud: 24-04-2023]. URL: https://majandus.postimees.ee/7374118/lennukihooldaja-magnetic-mro-langes-13-6-miljoniga-kahjumisse.

[23] Centre for Aviation. *Aircraft fleets: Western v Eastern/Central Europe. Airbus leads orders*. [Accessed: 24-04-2023]. URL: https://centreforaviation.com/analysis/reports/aircraft-fleets-western-v-easterncentral-europe-airbus-leads-orders-410122.

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Fred Matis Teeäär

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Automaatse identiteedi- ja ligipääsuhalduse juurutamine Magnetic MRO AS näitel", mille juhendaja on Edmund Laugasson
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

16.05.2023

[1] Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.