Lauri Teittinen

ROOLIPOHJAISTEN KÄYTTÄJÄTUNNUSTEN HALLINTAPROSESSIN ANALYSOIMINEN JA KEHITTÄMINEN

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Kyberturvallisuus

2024

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Lauri Teittinen
Työn nimi	Roolipohjaisen käyttäjätunnusten hallintaprosessin analysoiminen ja kehittäminen
Toimeksiantaja	Oy Mapvision Ltd
Vuosi	2024
Sivut	59 sivua, liitteitä 7 sivua
Työn ohjaajat	Pia-Maritta Puruskainen, Kimmo Kääriäinen

TIIVISTELMÄ

Toimeksiantajan yrityksessä Mapvision Oy, ollaan luomassa TISAX-pohjaista tietoturvajärjestelmää. Tähän liittyen yrityksessä on kehitetty roolipohjaista ja tietoturvallista sekä automatisoitua käyttäjätunnusten hallintaprosessia. Kehittämisprosessi on ollut odotettua haasteellisempi, ja lopputuloksesta on tullut odotettua monimutkaisempi.

Tämän opinnäytetyön tavoitteena oli tarkastella käyttäjänhallintaprosessin nykytilaa ja verrata sitä olemassa oleviin ratkaisuihin ja käytäntöihin. TISAX-sertifikaatin vaatimuksia verrattiin nykyiseen prosessiin ja tuotettiin arvioita sertifiointi auditoinnin läpäisystä. Vertailun ja prosessin kuvauksen avulla voitiin tunnistaa nykyisen prosessin riskejä ja laatia niistä kehityslista. Kehityskohteista osa implementoitiin testien avulla yrityksen prosessiin.

Opinnäytetyö tehtiin tutkimuskehitystyönä. Tutkimusaineistoa kerättiin sertifikaateista, henkilöhaastatteluista sekä tieteisjulkaisuista. Näiden lisäksi aineistoa kerättiin kenttäpöytäkirjaan tutkimuksen aikana. Aineiston analysointia suoritettiin vertailemalla nykyistä prosessia sertifiointivaatimuksiin sekä kenttäpöytäkirjan havainnointeihin.

Tutkimus onnistui antamaan toimeksiantajalle merkityksellisiä kehitysehdotuksia liittyen heidän käyttäjänhallintaprosessiinsa. Työn avulla toimeksiantajalle tehtiin neljä eri testiä käyttäjänhallinnan prosessin tietoturvallisuuden parantamiselle. Työtä voidaan käyttää yrityksessä nykyisen prosessin tunnistamiseen sekä tulevaisuuden käyttäjänhallinnan kehitykselle.

Asiasanat: roolipohjainen käyttäjänhallinta, TISAX, Entra ID, Azure AD, PowerAutomate, PowerApps

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author	Lauri Teittinen
Thesis title	Analysis and development of role-based user management process
Commissioned by	Oy Mapvision Ltd
Time	2024
Pages	59 pages, 7 pages of appendices
Supervisors	Pia-Maritta Puruskainen, Kimmo Kääriäinen

ABSTRACT

The commissioner Mapvision Oy is in the process of creating a TISAX-based information security system. In connection with this, they have developed a role-based and secure user account management process that has also been automated. The development process has been more challenging than expected, and the result has proven to be more complex than anticipated.

The objective of this thesis was to inspect the status of the user access rights process and compare it with the existing theoretical knowledge and technical solutions.

The thesis was conducted as design-based study. The basis of the TISAX evaluation was in a significant role in analyzing and comparing process results and identifying the risks in the current process. These results were used to prepare development lists for the company and implement some of the development targets in the current process.

The study was successful in giving out meaningful recommendations for the commissioner. Some of the recommendations were carried out as tests to prove their implementation in the future. The study can be used by the commissioner to identify the different phases in the process and develop them in the future.

Keywords: role-based access control, TISAX, Entra ID, Azure AD, PowerAutomate, PowerApps

SISÄLLYS

1 JOHDANTO

Autoteollisuuden jatkuvan kehityksen myötä yhä useammat autoteollisuuden toimittajat edellyttävät yhteistyökumppaneiltaan tietoturvallisuuden sertifikaatteja.

Toimeksiantajana toimii Mapvision Oy, joka toimii autoteollisuuden alalla fotogrammetrisen laadunvalvonnan asiantuntijana. Mapvision tarjoaa asiakkailleen tehdaslinjastoon laadunvalvontajärjestelmiä monimutkaisille komponenteille reaaliaikaisella nopeudella luotettavasti ja komponenttikohtaisesti. (Mapvision Oy 2023.)

Oy Mapvision Ltd on pääkaupunkiseudulla toimiva yritys ja sillä on Suomessa noin 90 työntekijää. Pääkonttori sijaitsee Helsingissä, mutta Mapvision toimii kansainvälisesti ja sillä on työntekijöitä myös muissa maissa, esimerkiksi Saksassa ja Yhdysvalloissa. Oy Mapvision Ltd:n liikevaihto vuonna 2022 oli noin 12 miljoonaa euroa (Kauppalehti 2023).

Toimeksiantajan yrityksessä ollaan pyrkimässä autoteollisuuden TISAX-sertifiointipohjan mukaiseen tietoturvajärjestelmään. Trusted Information Security Assessment eXchangessa, eli TISAX-sertifioinnissa, on yhdistettynä Saksan autoteollisuuden liiton (VDA) ja ISO/IEC 27001 -tietoturvasäännöt (DNV AS 2023). Tähän liittyen yrityksessä on kehitetty roolipohjaista ja tietoturvallista sekä automatisoitua käyttäjätunnusten hallintaprosessia. Kehittämisprosessi on ollut odotettua haasteellisempi ja lopputuloksesta on tullut odotettua monimutkaisempi.

Opinnäytetyö käsittelee toimeksiantajan valmiin roolipohjaisen automatisoidun käyttäjätunnusten hallintaprosessin tutkimista, tunnistamista ja kehittämistä. Toimeksiantaja Mapvision Oy tulee hyödyntämään opinnäytetyön tuloksia vaaditussa tietoturvajärjestelmässä, joka perustuu TISAX-viitekehykseen, sekä yrityksen käyttäjähallinnan jatkokehityksessä.

2 TUTKIMUSASETELMA

2.1 Tutkimusongelma

Lähtöpisteenä on se, että nykyinen käyttäjänhallintajärjestelmä ei ole tarpeeksi hyvin hallittu. Käyttäjänhallintaa on alun perin lähdetty suunnittelemaan yrityksessä silloin, kuin henkilömäärä oli suhteellisen vähäinen, minkä seurauksena ei käyttäjähallinnan menetelmissä päädytty valmiisiin kaupallisiin ratkaisuihin kustannuksien takia. Suunnittelu johti siihen, että käyttäjänhallinnan menetelmissä käytettiin yksinkertaisempia ratkaisuja ja itsejärjesteltyjä käyttäjän oikeuksien lisäämis- ja poistamisratkaisuja.

Käyttäjänhallintajärjestelmäprosessia on myös kehittänyt useampi henkilö niin, että aikaisempi kehittäjä on ehtinyt jo poistumaan organisaatiosta, kun seuraava on aloittanut prosessin tutkimisen ja muokkaamisen. Tällöin sisäinen hiljainen tieto ei ole kulkeutunut prosessia luovalta ja muokkaavalta tekijältä toiselle, mikä aiheuttaa ylimääräistä prosessin optimoimisen hankaloittamista.

2.2 Tutkimuskysymykset

Tutkimuksen ongelmien esittämisellä pyritään hahmottamaan sekä rajaamaan tutkimuksessa ratkaistavia tapauksia. Ongelman asettelussa, eli tutkimuskysymyksien laadinnassa, on tärkeää rajata, millaista tietoa halutaan tutkimuskohteesta saada. Tutkimuskysymykset voidaan jakaa pienempiin tutkimusongelmiin tutkimuksen edetessä. (Jyväskylän yliopisto Koppa 2021.)

Tutkimusongelmasta päästään seuraaviin tutkimuskysymyksiin:

- Millainen on käyttäjänhallintaprosessin nykytila?
- Millaisia kokonaisratkaisuja käyttäjänhallintaan on tarjolla?
    - Ovatko valmiit palvelut tarpeeksi kattavia?
- Miten nykytilannetta tulee kehittää, jotta TISAX-sertifioinnin vaatimukset täyttyvät?

Näihin tutkimuskysymyksiin opinnäytetyön aikana pyritään vastaamaan. Työn aikana keskitytään myös yleisesti prosessien tietoturvallisuuteen sekä käyttäjänhallinnan prosessin sujuvoittamiseen.

2.3 Valinta tutkimusotteesta

Tämä työ tehdään interventionistisenä kehittämistutkimuksena. Interventionistinen lähestymistapa ratkaisee käytännön ongelmia ja tavoitteena on tutkimuksellinen kehittäminen. Muutoksen kohde kehittämistutkimuksessa vaatii tutkimuksellista otetta ollakseen kehittämistutkimus. Työllä pyritään saamaan muutos toimeksiantajan prosessissa. (Kananen 2017, 10.)

Interventionistiseen kehittämistutkimukseen edellytetään konkreettista ongelmaa, joka vaatii ratkaisua. Tämä ratkaisu voi käsittää toimivan lähestymistavan parantamisen, ja toteutuksessa voivat toimia erilaiset käytännöt, työkalut ja prosessit. (Kananen 2017, 33).

Interventionistinen kehittämistutkimus sopii tähän opinnäytetyöhön, sillä se vaatii tutkimusten tuloksena saatujen ratkaisujen implementointia ja verifiointia. Ratkaisut vaativat myös usein pilotointia, eli testaamista ja varmistamista saatujen tutkimusratkaisujen kanssa. Varmistaminen voi vaatia myös useamman syklin. Interventionistinen kehittämistutkimus vaatii myös syvällistä ja pitkäkestoista yhteistyötä organisaatiolta, jolle tutkimus tehdään. (Kananen 2017, 37).

Interventionistisen tutkimuksen prosessi mukailee konstruktiivista tutkimusprosessia ja sisältää seuraavat kolme päävaihetta (Kananen 2017, 33):

1. Valmisteluvaihe
   - Käytännön ongelma
   - Teoriaan perehtyminen
   - Ongelman syiden löytäminen
2. Kenttävaihe
   - Ratkaisun tuottaminen
   - Toimivuuden varmistaminen
   - Käyttöönotto
3. Teoretisointi
   - Ratkaisun yleistäminen teoriaan

Tutkimuksen ongelman perusteellista selvittämistä ja kehittämistä varten on aluksi tärkeää tutustua jo olemassa oleviin ratkaisuihin roolipohjaisesta käyttäjänhallinnasta sekä valmiisiin yleisesti saatavilla oleviin prosesseihin. Yleisesti

saatavilla oleviin valmiisiin prosesseihin otetaan kantaa karkeasti myös hinnoittelumallien kannalta.

Kun yleisiin prosesseihin on perehdytty, täytyy selvittää toimeksiantajan tämänhetkinen ratkaisumalli roolipohjaisesta käyttäjänhallinnasta. Tutustumisen aikana on tärkeää sisäistää kaikki eri linkitetyt prosessit, jotka ovat käytössä toimeksiantajan käyttäjänhallinnan aikana. Selvityksen aikana otetaan myös kantaa siihen, miten toimeksiantajan tämänhetkinen käytäntö vertautuu valmiisiin ratkaisuihin kustannuksien ja ominaisuuksien osalta.

TISAX-sertifikaattiin perehtymisen aikana otetaan huomioon, miten nykyinen tilanne on linjassa TISAX-sertifikaatin kanssa, sekä vertaillaan ja analysoidaan kehittämiskohteita, joita nousee esille tutkimuksen edetessä.

Kehittämistutkimuksen päämääränä on saada aikaan muutos, jolloin selvitystyön lopuksi ehdotetaan tarvittavia muokkauksia tai uuden roolipohjaisen käyttäjänhallintajärjestelmän implementointia. Yksittäisiä kehitettyjä parannuksia tai uusia prosesseja implementoidaan organisaatiolle ja otetaan testikäyttöön sisäisesti hallittuun demoympäristöön. Testausta voidaan myös toteuttaa käyttäjäkeskeisillä testeillä, joissa toimeksiantajan valitsemat henkilöt testaavat kehitettyjä ratkaisuja. Tutkimuksen aikana tehtyjä havaintoja kirjataan ylös ja pohditaan lopuksi verraten niitä aikaisempiin sekä valmiisiin prosessiratkaisuihin.

2.4 Aineiston keruu ja analyysi

Kanasen (2017, 90) mukaan tieteellisen tutkimuksen laadukkaaseen toteutukseen kuuluu olennaisesti se, että tutkimuksessa noudatetaan tieteellisen tutkimuksen kriteereitä ja eettisesti kestäviä tutkimusmenetelmiä. Interventionistisen kehittämistutkimuksen aineistonkeruumenetelminä toimivat tilastot, kyselyt, teemahaastattelut, havainnoinnit ja dokumentit (Kananen, 23).

Tässä tutkimustyössä aineistoa saadaan pääsääntöisesti verkkolähteiden ja kirjojen avulla. Tietoa kerätään myös organisaation sisällä olevista lähteistä, kuten sisäisistä ohjeista ja yrityksen asiantuntijatehtävissä työskentelevien

henkilöiden kanssa käydyistä keskusteluista. Verkkolähteistä saatujen aineistojen oikeellisuutta on huomioitava työn aikana tarkasti.

Tutkimustyössä käytettävä TISAX-sertifioinnin sekä muiden mahdollisten direktiivien tai standardien lähdetieto tulee kerätä vain virallisilta sertifikaatteja, direktiivejä tai standardeja ylläpitäviltä organisaatioilta. Sertifikaatin tietojen keruuseen voidaan myös käyttää luotettujen sertifiointikumppaneiden ja auditoijien lähteitä.

Työssä suoritetaan sisällön analysointia ja havainnointia. Havainnot dokumentoidaan kenttäpäiväkirjamaisesti myöhempää tarkastelua varten. Aineiston analyysissä keskitytään erityisesti nykyisen toimintamallin vertailuun TISAX-kriteereihin, jotka on saatu virallisilta organisaatioilta sertifiointia varten. Eroavaisuudet ja poikkeamat identifioidaan ja dokumentoidaan kehitysehdotuksien muodostamista varten. Samoin valmiiden ratkaisujen ominaisuuksia vertaillaan nykyiseen toimintamalliin, jotta voidaan muodostaa asianmukainen kuva nykyisen toimintamallin puutteista, eroavaisuuksista tai hyödyistä.

3 KÄYTTÄJÄN JA KÄYTTÄJÄOIKEUKSIEN HALLINTA

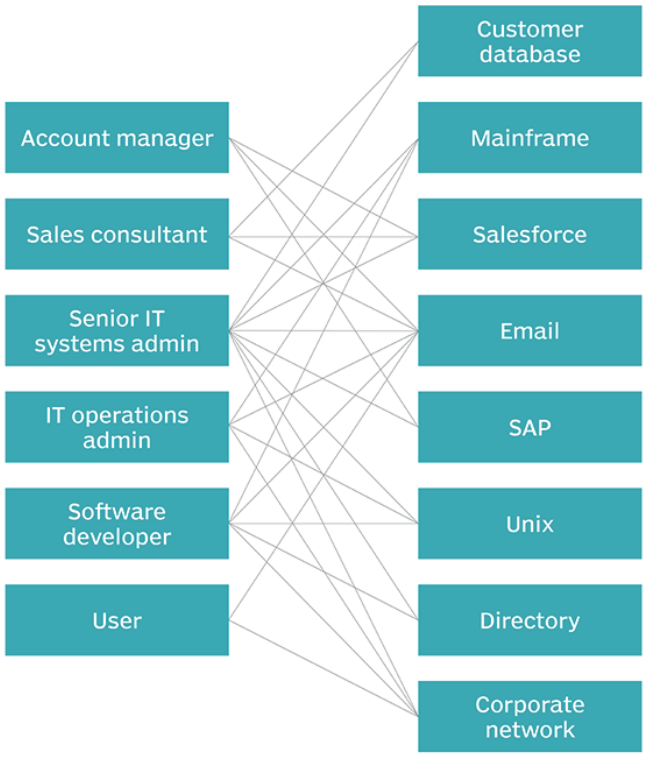
Kuten monet organisaatiot kasvaessaan, myös toimeksiantaja tavoittelee sertifikaatteja, jotka vahvistavat organisaation luotettavuutta. Sertifikaatti voi tuoda organisaatiolle kilpailuetua, markkinakasvua, kasvanutta tuottavuutta, lisääntynyttä mainetta kilpailijoihin nähden, tehostunutta sisäistä prosessia, riskienhallintaa ja parempaa tietoturvaa. Sertifikaattien hallinta voi olla myös asiakkaan vaatimus sekä vastaus lainsäädännön vaatimuksiin. (Standards & economic growth 2021.)

Toimeksiantaja on päättänyt hankkia TISAX-sertifikaatin niin asiakkaiden kuin oman organisaationsa näkyvyyden, luetettavuuden ja muiden hyötyjen takia. Lisäksi toimeksiantajan henkilöstömäärä on kasvanut huomattavasti, minkä seurauksena käyttäjänhallinnan tärkeys ja merkitys organisaatiossa on myös kasvanut. Tämä kaikki on johtanut siihen, että käyttäjänhallintaa on lähdetty automatisoimaan sekä tavoittelemaan TISAX-sertifikaatin vaatimuksien täyttämistä. Tämä liittyy luonnollisesti myös tietoturvaan käyttäjänhallinnan parissa.

3.1 Roolipohjainen käyttäjänhallinta

Roolipohjainen käyttäjänhallinta, eli Role Based Access Control (RBAC) on hallintamenetelmä, joka perustuu käyttäjän rooliin organisaatiossa. Roolin perusteella käyttäjän oikeuksia hallinnoidaan ja rajoitetaan tarpeen mukaan. RBAC:n avulla turvataan organisaation sensitiivistä dataa sekä mahdollistetaan käyttäjän pääsy vain niihin toimintoihin, jonka hänen roolinsa mahdollistaa. (NIST 2016.)

Seuraavassa kuvassa havainnollistetaan, miten roolipohjaisessa käyttäjänhallinnassa tietylle ryhmälle myönnetään ainoastaan tarpeelliset oikeudet. Tämä lähestymistapa mahdollistaa tarkemman kontrollin ja hallinnan siitä, mitä kukin käyttäjä voi tehdä organisaation tietojärjestelmässä.



Kuva 1. Käyttäjänhallinnan myönnetyt oikeudet (TechTarget2023)

Rooliryhmien sisällä tapahtuva oikeuksien jakaminen on jaettu kolmeen eri ryhmään: Access (Pääsyoikeus), Reading (Lukuoikeus) ja Writing (Muokkausoikeus).

Access viittaa käyttäjän oikeuteen päästä tiettyihin kansioihin, tietoihin, ohjelmistoihin tai datoihin. Tämä tarkoittaa käyttäjän valtuutusta saavuttaa ja käyttää tietyn resurssin tai alueen sisältöä. (Okta 2023.)

Reading määrittelee sen, kuka voi avata ja tarkastella dataa ilman, että tekee niihin muutoksia. Tämä oikeus antaa käyttäjälle mahdollisuuden nähdä ja lukea tietoja, mutta ei myönnä oikeutta muuttaa niitä millään tavalla. (Okta 2023.)

Writing, eli muokkausoikeus viittaa siihen, kuka voi muokata dataa. Tämä oikeus antaa käyttäjälle valtuudet tehdä muutoksia tietoihin ja samalla voidaan harkita, tarvitaanko muutosten hyväksyntää ennen niiden voimaantuloa. (Okta 2023.)

RBAC:n käytön hyötyjä ovat

- Helppo ja yksinkertainen käyttäjäoikeuksien auditointi
- Nopea käyttäjäoikeuksien hallinnointi
- Kolmannen osapuolen käyttäjien integrointi järjestelmään
- Tehokkaampi sertifikaattien vaatimuksien seuraaminen

3.2 Pääsynvalvontatapoja

Discretionary Access Control, eli DAC, on harkinnanvaraista pääsynvalvontaa. DAC:ssa käyttäjänoikeuksien hallinta on sen omistajan tai henkilön hallinnassa, jolle se on tiettyä resurssia vastaan myönnetty. Resurssin omistaja voi hallita kenelle oikeuksia myönnetään tai keneltä niitä poistetaan. DAC antaa mahdollisuuden joustavampaan käyttäjäoikeuksien pääsynhallintaan. DAC aiheuttaa kuitenkin myös suuremman tietoturvallisuusriskin, koska oikeuksia hallitsevia omistajia on paljon enemmän. (NIST 1992.)

Mandatory Access Control, eli MAC, on käyttäjäoikeuksien hallintaa niin, että jokin keskitetty yksilö tai ryhmä hallitsee käyttöoikeuksia usean turvaluokan yli. MAC-hallinta on selvästi DAC-hallintaa tiukempi käyttäjänhallintatyyli. MAC:ia käytetään yleisimmin organisaatioissa, joissa on useita kerroksia datan suojaamiseen, kuten viranomaisjärjestelmät. (Imperva 2023.)

Zero Trust Policy, eli nollaluottamuspolitiikka perustuu oletukseen, että kaikki toiminnat ovat potentiaalisesti turvallisuusuhkia. Lähestymistapa korostaa jatkuvan luottamuksen arviointia sen sijaan, että luottamus annettaisiin oletuksena perinteiseen tyyliin. Zero Trust -politiikka pyrkii kattamaan kaikki resurssit kuten identiteetin, pääsynhallinnan, toimintojen, päätelaitteiden ja verkkoinfrastruktuurin. Lähestymistapana on rajoittaa resursseja vain niille, joilla on siihen tarve, jolloin myönnetään käyttäjille vain vähimmäisoikeudet tarvittavan tehtävän suorittamiseksi. Myös käyttäjien laitteiden pääsy tarvittaviin resursseihin perustuu vain tarpeeseen, jolloin käyttöoikeus voidaan myöntää. Zero Trust -politiikassa keskeisimpiä jatkuvan luottamuksen arviointiin on autentikointi ja varmennus. (NIST 2020a.)

Multi-Factor Authentication, eli monivaiheinen tunnistautuminen, sekä Two-Factor Authentication, eli kaksivaiheinen tunnistautuminen, ovat pääsynhallinnassa käytettäviä tunnistautumistapoja. Näistä käytetään lyhenteitä MFA sekä 2FA. Kummassakin tapauksessa tunnistautumista vaaditaan useammasta kuin yhdestä lähteestä käyttäjän autentikoimiseen. Esimerkiksi käyttäjän kirjautuessa palveluun tulee käyttäjän esittää salasana tunnukselleen sekä jokin muu tunnistautumistapa. Yleisesti monivaiheisissa tai kaksivaiheisissa tunnistautumistapahtumissa käyttäjän tarjoaa oman salasanan sekä henkilökohtaiseen puhelinnumeroon lähetettyyn numerokoodiin. Kuitenkin tunnistautumisessa voidaan käyttää hyvinkin paljon eri tapoja kuten salasanoja, sertifikaatteja, NFC-kortteja, sormenjälkiä, kasvontunnistusta sekä muita ominaisuuksia. Nämä muut ominaisuudet onkin jaettu viiteen eri kategoriaan: jotain mitä tiedät, jotain mitä sinulla on, jotain mitä olet, jossain missä olet ja jotain mitä teet. Yleisesti kuitenkin käytetään eniten tunnistautumistapoja ensimmäisistä kolmesta tavasta. MFA:n sekä 2FA:n selvä etu on käyttäjätunnukselle tunnistautumisen suurentunut turvallisuus hyökkääviä tahoja vastaan. Haittana voidaan pitää lisääntynyttä kompleksisuutta käyttäjälle sekä järjestelmälle. (OWASP 2024.)

3.3 Entra ID

Entra ID on identiteetin ja pääsynhallinnan hallinnoimispalvelu Microsoft-tuoteperheessä. Palvelu toimii täysin pilvessä ja mahdollistaa organisaatioiden käyttäjien kirjautumisen, sekä käyttöoikeuksien hallinnan useaan eri Microsoft-

tuoteperheen pilvipalveluun. Käyttäjänhallinnointipalvelu koostuu käyttäjäorganisaatioista, jotka esittävät yrityksen organisaatiota. Käyttäjäorganisaatioita voidaan lisätä Entra ID -järjestelmään useita ja jokaiselle käyttäjäorganisaatiolle on oma domain-nimi, esimerkiksi “@mapvision.fi”. Käyttäjäorganisaatiolla on myös yksi tai useampi palvelutilaus, mutta palvelutilauksilla vain yksi käyttäjäorganisaatio. Käyttäjäorganisaatioiden alla on hakemisto, jossa voi olla käyttäjiä, ryhmiä sekä laitteita. Ryhmiin voidaan lisätä käyttäjiä, laitteita sekä oikeuksia, jotta käyttäjät, jotka ovat ryhmässä mukana, saavat kyseisen ryhmän oikeudet käyttöönsä. (Microsoft 365 2024.)

Entra ID -käyttäjänhallintaa on kehitetty hyvin paljon Microsoftin puolesta vuosien aikana. Entra ID -palvelu onkin edelliseltä nimeltään Azure Active Directory, joka on kuulunut Azure-pilvipalvelualustan alaisuuteen. Azure AD päätettiin kuitenkin eriyttää omakseen erinäisistä syistä vuoden 2023 loppupuolella. Koska tämä työ tehtiin tämän vaihdoksen aikaan, on tärkeää tiedostaa, että Azure AD -palvelun uudelleen nimeäminen Entra ID -palveluksi ei muuttanut mitään konfiguraatioita tai integraatioita eikä yrityksen tarvinnut tehdä mitään toimintoja prosessien jatkumiseksi samana. (Microsoft Entra 2024.)

Entra ID -käyttäjänhallinnan avulla järjestelmän hallitsijoilla on mahdollisuus määritellä lisättyjen käyttäjien jäsenyyksiä dynaamisiin ryhmiin perustuen käyttäjien tietoihin. Myös laitteita voidaan määritellä ryhmiin perustuen dynaamisiin ominaisuuksiin, mutta käyttäjiä ja laitteita ei voida yhdistää samaan ryhmään. Nämä dynaamiset ryhmät poistavat tarpeen manuaaliselle käyttäjien lisäämiselle haluttuihin ryhmiin perustuen käyttäjien rooleihin. Automatisoidulla lähestymistavalla varmistetaan, että käyttäjät sekä laitteet ovat oikeissa ryhmissään aina kun tiedot muuttuvat. Tämä selkeyttää hallinnollista prosessia, kun käyttäjän tietoja muutetaan, sekä lisää organisaation joustavuutta pääsynhallinnan järjestelmän ylläpitämisessä. Dynaaminen käyttäjänhallinta Entra ID:n kanssa on myös pilvipalveluna toimiva palvelu, jolloin nykyajan kehittyvässä yritysmaailmassa on helppo integroitua ja adaptoitua muutoksiin, joita teknologian kehittyessä tulee vastaan. (Microsoft Entra 2023.)

Dynaamisissa ryhmissä on tärkeää muistaa, että käyttäjiä voidaan lisätä ryhmään vain laadittujen syntaksisääntöjen mukaan, jolloin manuaalisesti käyttä-

jän lisääminen ryhmään on mahdotonta. Tämä kuitenkin korostaa ryhmän jäsenyyssääntöjen tarkkuuden tärkeyttä, jolloin vain halutut käyttäjät liittyvät ryhmään, kun heidän attribuuttinsa muuttuvat sopiviksi. Käyttäjä myös poistuu ryhmästä automaattisesti, kun käyttäjän attribuutit tai ominaisuudet vaihtuvat niin, ettei ryhmän syntaksi enää toteudu. (Microsoft Entra 2023.)

3.4 TISAX-sertifiointi

TISAX on Saksan autoteollisuuden liiton (VDA) kehittämä sertifiointikehys, joka on suunnattu erityisesti autoteollisuudelle. TISAX-sertifikaatti keskittyy erityisesti autoteollisuuden toimijoille tietoturvan ja tietosuojan parissa. TISAX-sertifikaatti vaatii yleensä organisaatiolta tietoturvastrategian, käytäntöjen menettelyn ja noudattamisen, käyttäjähallinnan tehokkuuden ja auditoitavuuden. TISAX ei ole osa tietoturvastandardia ISO 27001, mutta on vahvasti liitoksissa siihen. (DNV AS 2023.)

TISAX-sertifiointiin vaaditaan sertifiointitarkastus, jossa tarkastusyritykset auditoivat ja tarkastavat organisaation. Sertifiointitarkastuksessa arvioidaan organisaation tietoturvaprosesseja, käytäntöjä ja järjestelmiä TISAX-vaatimuksiin vertaillen. Sertifiointitarkastuksen jälkeen organisaatio vastaanottaa TISAX-raportin, jossa osoitetaan auditoinnin tulokset ja havaitut puutteet sekä suositellut korjaustoimenpiteet. Virallisen TISAX-sertifikaatin organisaatio voi saada vasta osoitettuaan korjanneensa mahdolliset havaitut puutteet. (ENX Association 2023.)

TISAX-sertifioinnilla voidaan osoittaa asiakaskumppaneille organisaation sitoutuneisuuden tietoturvallisuuteen ja täyttävänsä tietoturvavaatimuksen autoteollisuuden alalla. TISAX-standardi on suunniteltu auttamaan autoteollisuuden yrityksiä arvioimaan ja valvomaan kumppaniverkostojen tietoturvaa. TISAX-sertifiointiprosessiin ryhdytäänkin usein asiakkaan pyynnöstä täyttää heidän vaatimukseensa tiettyyn tietoturvallisuustasoon. (ENX Association 2023.)

Käyttäjänhallinta TISAX-sertifikaatissa ilmenee sertifiointitarkastuksessa vaadittuina kohtina, joissa tarkastellaan identiteetin ja käyttöoikeuksien hallintaa

organisaatiossa. Vaatimustaulukon sertifikaattia hakeva organisaatio saa ylläpitävältä ENX-järjestöltä. ENX-järjestö ylläpitää kriteerejä ja arviointivaatimuksia TISAX-standardiin, sekä hyväksyy ja monitoroi auditointiorganisaatioita. (ENX TISAX 2023.)

TISAX-sertifikaatin vaatimustaulukosta löydetään käyttöoikeuksien hallinnoimisen kohdasta seuraavan taulukon (taulukko 1) mukaiset asiat.

Taulukko 1. (TISAX käyttäjänhallinnan kriteerit (ENX 2023)

Identity and Access Management	
Control question	**Objective**
To what extent is the use of identification means managed?	To check the authorization for both physical access and electronic access, means of identification such as keys, visual IDs or cryptographic tokens are often used. The security features are only reliable if the use of such identification means is handled adequately.
To what extent is the user access to network services, IT systems and IT applications secured?	Only securely identified (authenticated) users are to gain access to IT systems. For this purpose, the identity of a user is securely determined by suitable procedures.
To what extent are user accounts and login information securely managed and applied?	Access to information and IT systems is provided via validated user accounts assigned to a person. It is important to protect login information and to ensure the traceability of transactions and accesses.
To what extent are access rights assigned and managed?	The management of access rights ensures that only authorized users have access to information and IT applications. For this purpose, access rights are assigned to user accounts.

TISAX on myös antanut tälle kohdalle vaatimukset seuraavilla tasoilla: vaatimus (minimi), vaatimus (pitäisi tehdä), lisävaatimus korkean tason suojaukselle, lisävaatimus erittäin korkean tason suojaukselle. Kuten tasonimestä huomataan, jotta TISAX-sertifioinnin voi saavuttaa, tarvitsee vain alimman tason vaatimuksen kriteerien täyttyä. Seuraavassa taulukossa 2 vaatimuskriteerejä yhdestä käyttäjänhallintakohteesta:

Taulukko 2. TISAX vaatimuksien tasot (ENX 2023)

Control question	**To what extent are access rights assigned and managed?**
Objective	The management of access rights ensures that only authorized users have access to information and IT applications. For this purpose, access rights are assigned to user accounts.
Requirements (must)	+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Application the minimum ("need-to-know") principle. + The access rights granted for normal and privileged user accounts and technical accounts are verified at regular intervals also within IT systems of customers.
Requirements (should)	+ Strategies for authorizing access to information are prepared. + Authorization roles are used. + Rights are allocated on a need-to-use basis and according to the role and/or area of responsibility. + Normal user accounts are not granted privileged access rights. + The access rights of a user account are adapted after the user has changed (e.g. to another field of responsibility).
Additional requirements for high protection need	+ The access rights are approved by the responsible internal Information Officer. (C, I, A)
Additional requirements for very high protection need	+ Prevention of unauthorized persons gaining access and information (privileged users): (C) - Information is stored in encrypted form at content level (e.g. file level). - Where encryption is not feasible, information shall be protected by similarly effective measures. + Existing access rights are regularly reviewed at shorter intervals (e.g. quarterly) (C)

Näitä taulukkotietoja yritys voi ennen auditointitapahtumaa käyttää hyödykseen esimerkiksi identiteetin ja pääsynhallinnan prosessien kehittämiseksi. Auditointia varten yrityksen täytyy täyttää myös taulukkoon määrittelyt siitä, miten kysymyksissä olevia kohtia on yrityksen prosessissa toteutettu.

4 PROSESSISSA KÄYTETYT SOVELLUKSET

Seuraavaksi käydään läpi organisaation sisällä käytettyjen prosessien sovellutuksia sekä menetelmiä, joilla nykyinen käyttäjän oikeuksien hallinta on järjestelty. Nämä prosessit ja menetelmät perustuvat pääosin Microsoftin sovelluksiin, sillä organisaatiolla on käytössään Microsoft Entra ID P1 –lisenssi. Vaikka lisenssi ei sisällä seuraavia sovelluksia, yrityksen käytössä oleva Microsoft 365 –lisenssi sisältää ne.

Lisäksi yritys käyttää IT-palveluiden osittaisessa hallinnoimisessaan Netox-yritystä. Netox on IT-palveluita tarjoava yritys, joka keskittyy asiakasyrityksiensä pilvipalveluiden, tietoturvan, verkkoratkaisujen ja tietoliikenteen hallintaan ja kehittämiseen (Netox 2024). Netox on aikaisemmin hallinnut yrityksen käyttäjänhallintaratkaisuja, mutta usean eri syyn seurauksena käyttäjänhallintaa tehdään nyt myös yrityksen omien resurssien kautta.

4.1 Microsoft Power Apps

Microsoft Power Apps on monipuolinen mukautettujen sovellusten luontiin tarkoitettu työkalupaketti. Power Appsin kanssa pystytään muuttamaan manuaalisia liiketoimintaprosesseja automatisoiduiksi prosesseiksi muiden Microsoftin työkalujen linkittämisen avulla. Yhteyksiä voidaan luoda Microsoft Dataverse -tietoalustoihin, erilaisiin verkkolähteisiin tai paikallisiin tallennettuihin lähteisiin. Power Appsin suuri etu on, ettei sovelluksien luontiin tarvitse syvällistä ohjelmointitaitoa. (Microsoft PowerApps 2023.)

Power Apps -työkalu on nimensä mukaisesti ”app” eli sovellutus. Se perustoimintaa voidaankin miettiä samankaltaisena kuin muidenkin mobiilisovellutuksien toimintaa käyttäjän näkökulmasta. Power Appsin avulla yrityksessä luodaan uusia käyttäjiä, muokataan käyttäjien oikeuksia sekä poistetaan tarvittaessa käyttäjiä. (Microsoft PowerApps 2023.)

4.2 Microsoft Lists

Microsoft Lists on Microsoftin tarjoama sovellus, joka sisältyy Microsoft 365 -tuoteperheeseen. Sen avulla voidaan luoda ja hallita erilaisia listoja organisaatiossa. Microsoft Lists on eräänlainen tietojen kokoelma, johon voi implementoida monia eri ominaisuuksia kuten automatisointia, sääntöjä ja tärkeimpänä integraatioita muihin Microsoft-tuoteperheen sovelluksiin. (Microsoft Lists 2023.)

4.3 Microsoft Power BI

Microsoft Power BI on datan visualisointityökalu, joka auttaa organisaatiota hallitsemaan, visualisoimaan ja analysoimaan liiketoiminnan dataa. Power BI

mahdollistaa eri datalähteiden integroinnin omaan haluttuun muotoon visuaalisesti ja selkokielisesti. (Microsoft Power BI 2023.)

4.4 Microsoft Power Automate

Microsoft Power Automate on pilvitaustainen palvelu, jolla voidaan luoda automatisoituja työnkulkuja ja prosesseja organisaation tarpeisiin niiden haluamallaan tavalla. Automatisointiin on mahdollista yhdistää monia eri Microsoft 365 -palveluita, jolloin organisaation toistuvia tehtäviä ja toimintoja voidaan tehostaa ja sujuvoittaa. (Nanonets 2024.)

4.5 Microsoft Entra ID

Microsoft Entra ID on pilvipohjainen identiteetin hallinta- ja tunnistautumispalvelu, jolla voi hallita oikeuksia tiettyihin organisaation palveluihin. Entra ID on suunnattu erityisesti pilvipalvelualustojen tarpeisiin. Entra ID:n keskeisimpiä työkaluja ovat SSO (Single Sign On), roolipohjainen pääsyhallinta, turvallisuusryhmät ja identiteetin hallinta. (Microsoft Entra ID 2023.)

Työn aikana Microsoft Azure AD muuttui nimelle Microsoft Entra ID. Muutoksen myötä Microsoft on tiedottanut, ettei ylimääräisiä toimenpiteitä tarvita Azure AD:n pääkäyttäjiltä. (Microsoft Azure 2023.)

4.6 Microsoft SharePoint

Microsoft SharePoint on yhteistyöalusta, jota käytetään integroituna Microsoft Office -palveluiden kanssa. SharePoint toimii verkkoselainpohjaisesti. SharePointin keskeisin toiminta on tallentaa, järjestellä, jakaa ja hyödyntää tietoa organisaatiolle. SharePoint tarjoaa ominaisuuksia kuten projektinhallinta, versiohallinta, pääsynhallinta, organisaation sisäiset verkkosivustot ja asiakirjahallinta. Nämä ominaisuudet lisäävät tiimityöskentelyn ja organisaation sisäisen kommunikaation tehokkuutta. Power Automate on ennen toiminut SharePointiin integroituna. (Sharepoint Maven 2024.)

4.7 Microsoft 365 Groups

Microsoft 365 automatiikan taustalla on Microsoft 365 Groups. Groups on jäsenyysryhmiä Microsoft 365 sisällä, ja on keskeisin palvelu, joka ohjaa ryhmätyöskentelyä kaikkien Microsoft 365 sovellusten välillä. Jäsenyysryhmissä ohjataan käyttöoikeuksia ja resursseja. Microsoft Groups on lista eri ryhmiä, joissa jokaiselle on määritelty omat tietyt oikeudet eri sovellutuksiin tai oikeuksiin. Kun näihin ryhmiin lisätään käyttäjiä, käyttäjä perii suoraan ryhmässä määritellyt käyttöoikeudet. Eri ryhmätyypit auttavat organisaatiota organisoimaan ja hallitsemaan useiden käyttäjien käyttöoikeuksia Entra ID -ympäristössä. Esimerkiksi jos käyttäjä luo Teams-ryhmän, taustalla luodaan myös Microsoft 365 Group, johon juuri luotu Teams-ryhmä ja kaikki siihen yhdistetyt palvelut liitetään. Oikeudet ja asetukset, joita Groupin sisällä muutetaan, muuttuvat myös kaikissa M365 Groupiin liittyvissä palveluissa. (Microsoft Groups 2023.)

4.8 Security groups

Security groups, eli turvallisuusryhmät, ovat ryhmiä, joita käytetään käyttäjän pääsyn myöntämiseen Microsoft 365 -resursseihin. Turvallisuusryhmä on yksinkertaisesti looginen ryhmä objekteja. Turvallisuusryhmät voivat sisältää käyttäjiä, sovelluksia, ryhmiä ja laitteita. Laitteiden hallinta turvallisuusryhmien kanssa auttaa hallintaa esimerkiksi yrityksen työsuhdepuhelimien hallinnan kanssa. Turvallisuusryhmät konfiguroidaan Microsoft Entra ID:n kanssa. Ryhmä voidaan luoda myös dynaamiseksi, jolloin ryhmän käyttäjät määrittyvät automaattisesti käyttäjän tiedoissa olevien attribuuttien mukaisesti. Turvallisuusryhmät eivät automaattisesti luo Teams-ryhmää, kuten Microsoft 365 -ryhmät loisivat. (Microsoft Group types 2024.)

4.9 Distribution groups

Distribution groups, eli jakeluryhmät, ovat ryhmiä, joita käytetään ilmoitusten lähettämiseen sähköpostijakelun kautta. Jakeluryhmiä voidaan lisätä ryhmään Microsoft Teamsiin, mutta vain ryhmän jäsenet lisätään jakeluryhmään, ei itse Teams-ryhmää. (Microsoft Group types 2024.)

4.10 Dynamic distribution groups

Dynamic distribution groups eli dynaamiset jakeluryhmät ovat sähköposti-enabloituja ryhmiä, joille voidaan lähettää sähköpostia ryhmän tiettyjen attribuuttien perusteella. Esimerkiksi sähköposteja voidaan lähettää vain ihmisille, joilla on sijaintina Helsingin toimipiste. Nämä spesifit tiedot eivät ole Entra ID:n kautta määriteltyjä. Eroten normaalista jakeluryhmästä, dynaamisessa jakeluryhmässä viestin vastaanottajat määrittyvät viestin lähetyshetkellä valittujen attribuuttimääritelmien kanssa. (Microsoft Group types 2024.)

5 NYKYINEN TOIMINTAMALLI

Nykyinen roolipohjainen käyttäjähallinta on rakennettu toimeksiantajaorganisaatiossa aikaisemmassa luvussa kerrottujen teknologioiden avulla. Nykyistä toimintamallia on kehitetty useaan otteeseen ja kahden eri tekijän toimesta, jotka eivät ole pystyneet työskentelemään samanaikaisesti pääsynhallinnan kehittämisen kanssa. Seuraavaksi kuvailen heidän luomansa ratkaisun.

Yritys käyttää Entra ID -palvelua, jossa yrityksen työntekijöille on luotu käyttäjätili sekä mahdolliset ulkopuoliset vierailijatunnukset. Käyttäjät on pääosin lisätty Entra ID -palvelussa ”assigned” eli manuaaliseen nimettyyn kategoriaan. Myös roolipohjaisia ryhmiä on lisätty pääosin nimettyyn kategoriaan. Uuden käyttäjän lisääminen sekä oikeuksien lisääminen ja poistaminen tapahtuu yrityksen itse kehittämän sovelluksen avulla. Omatekoinen työkalu toimii aikaisemmin esitettyjen sovelluksien kanssa. Käyttäjänhallintaa kuvataan seuraavaksi alkaen tilanteesta, jolloin uusi työntekijä lisätään organisaatioon, minkä jälkeen käydään tilanteet, kun käyttäjä siirretään tai poistuu organisaatiosta.

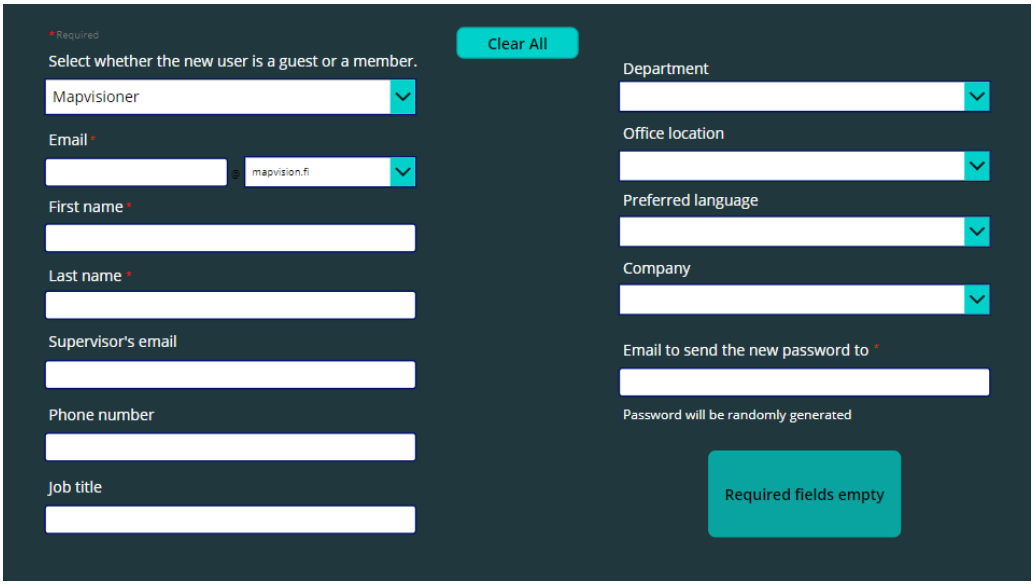
Nykyistä toimintamallia on analysoitu ja havainnoitu pääsääntöisesti tutkimalla PowerAutomaten ohjelmointilogiikkaa sekä sen kulkua sovelluksen omien työnkulun analysointityökalujen kanssa. Nykyisestä ohjelmoinnista vastannutta sekä alkuperäisen toimintalogiikan visioinutta yrityksen henkilöstöä on myös haastateltu toiminnan ja prosessin selvitystyötä varten. Näiden pohjalta sekä PowerAutomaten toimintalogiikkojen perusteiden selvittämisen jälkeen tehtiin tarkka selvitystyö nykyisestä prosessinkulusta.

5.1 Uuden käyttäjän lisääminen organisaation käyttäjänhallintaratkaisuun

Kun uuden käyttäjän perustiedot ovat hankittuna, voidaan aloittaa käyttäjän lisääminen järjestelmään. Ensimmäiseksi organisaation vastuuhenkilö täyttää uuden käyttäjän tiedot PowerAppsillä toimivaan lomakkeeseen. Tämä PowerApps-lomake on organisaation sisäisesti kehittämä (Kuva 2).

Uuden käyttäjän lisäämiseen tarvitaan seuraavat tiedot:

- Organisaation työntekijä vai vieras
- Tuleva sähköpostiosoite
- Etunimi
- Sukunimi
- Esihenkilön sähköpostiosoite
- Puhelinnumero
- Työnimike
- Osasto
- Päätoiminen työsijainti
- Kieli
- Yhtiö
- Sähköpostiosoite, johon käyttäjän salasana lähetetään

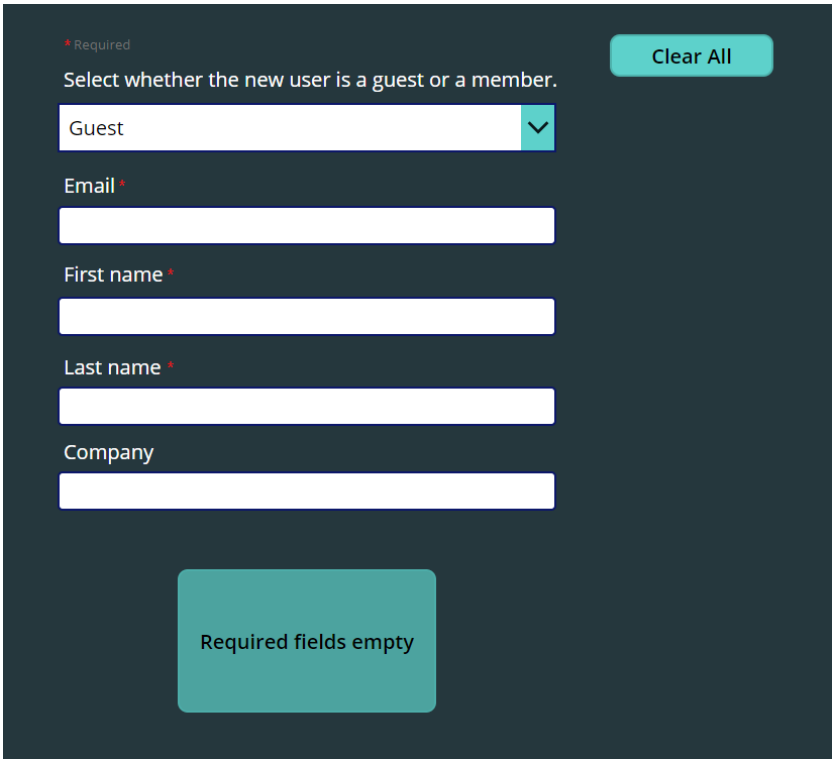


Kuva 2. Uuden käyttäjän luonti (Mapvision Oy 2024)

Vieraskäyttäjän luonti tapahtuu samantapaisesti kuin peruskäyttäjänkin. Samasta PowerApps-sovelluksesta löytyy vaihtoehto ”Guest”, jonka valitsemisen jälkeen täytettävät ja tarvittavat tiedot muuttuvat vieraskäyttäjän lisäämiseen vaadittaviksi. Vieraskäyttäjän lisäämisen lomake esitetään kuvassa 3.

Uuden vierastilin lisäämiseen tarvitaan seuraavat tiedot:

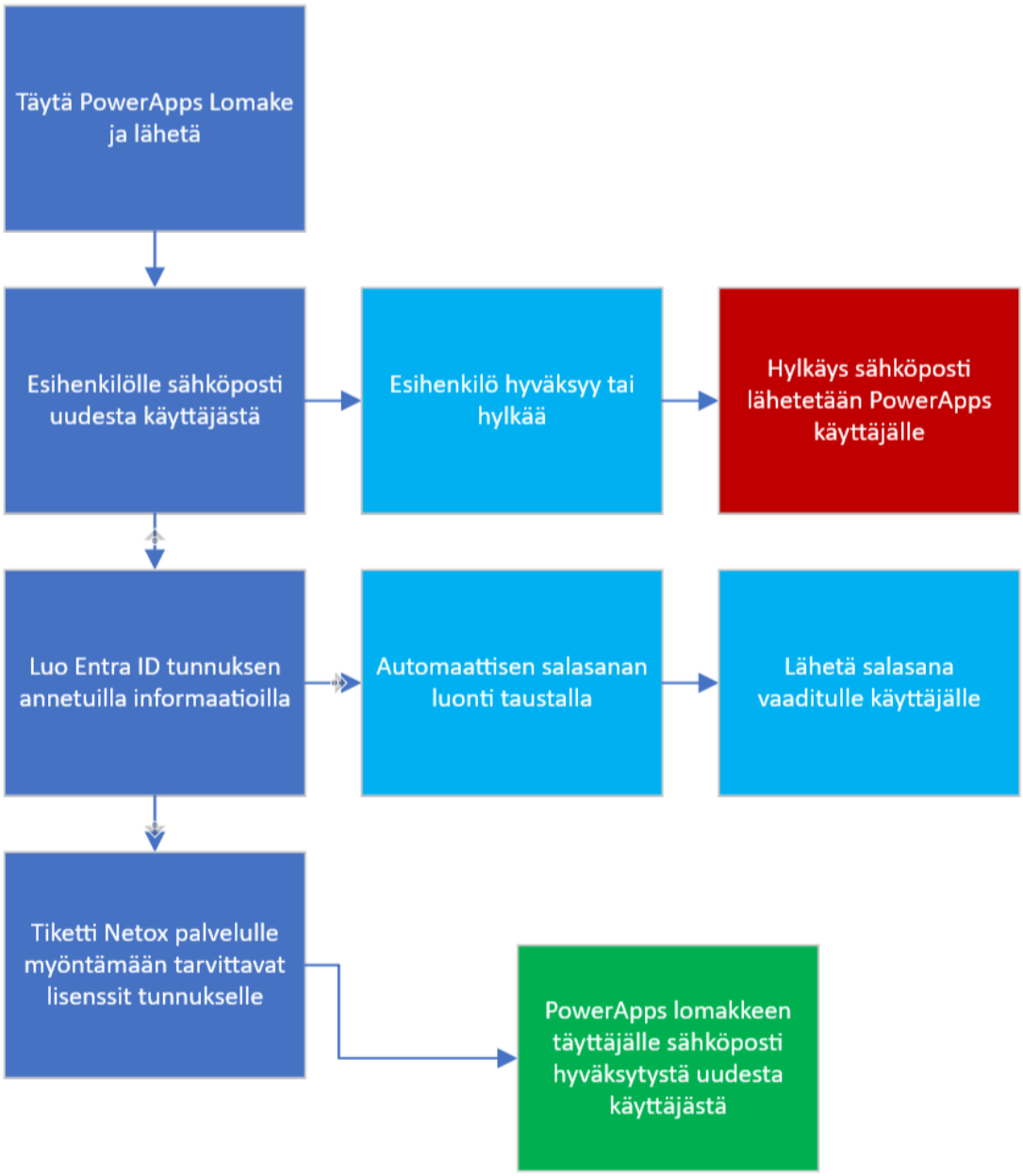
- Sähköposti
- Etunimi
- Sukunimi
- Yritys



Kuva 3. Uuden vieraskäyttäjän luonti (Mapvision Oy 2024)

Kun PowerApps-lomake on täytetty ja lähetetty eteenpäin, käynnistyy taustalla prosessi uuden käyttäjän tunnuksia varten.

1. Lomakkeen täyttäjän esihenkilölle lähtee viesti uuden käyttäjätunnuksen luomisesta
2. Järjestelmä luo automaattisesti Entra ID -tunnukset
3. Tiketti organisaation käyttämälle kolmannen osapuolen IT-palveluntarjoajalle (Netox)
    a. Netox myöntää Microsoft Business Premium -lisenssin aikaisemmin luodulle Entra ID -tunnukselle



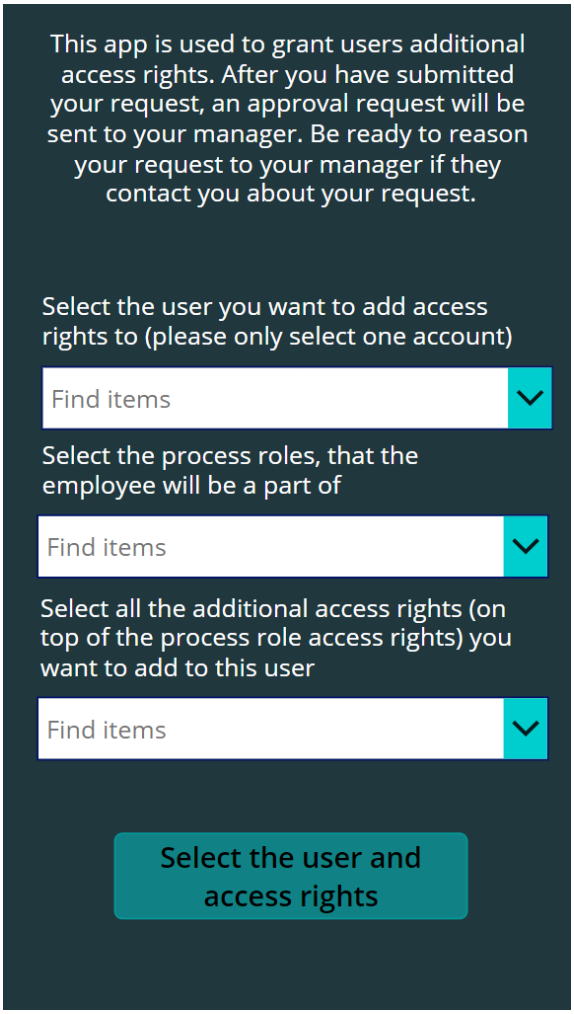
Kuva 4. Uuden tunnuksen luomisen prosessi

Näiden kohtien jälkeen uusi käyttäjä on lisätty organisaation käyttäjien piiriin. Tässä kohtaa käyttäjällä ei ole vielä mitään roolipohjaisia oikeuksia. Ainoa asia käyttäjällä tässä kohtaa on Microsoft-tunnukset Entra ID -järjestelmässä. Käyttäjän tarkan ja yksityiskohtaisen lisäysprosessin näkee liitteestä 2 ja selvennetyn yleistetyn prosessikaavion näkee kuvasta 4.

5.2 Käyttäjälle roolipohjaisten oikeuksien lisääminen

Seuraavaksi käyttäjälle on lisättävä oikeuksia, jotta tämä pystyy suoriutumaan päivittäisistä työtehtävistään organisaation kanssa. Oikeuksia lisätään roolipohjaisesti PowerApps-lomakkeiden avulla. Sovellus vaatii vain käyttäjän, jolle

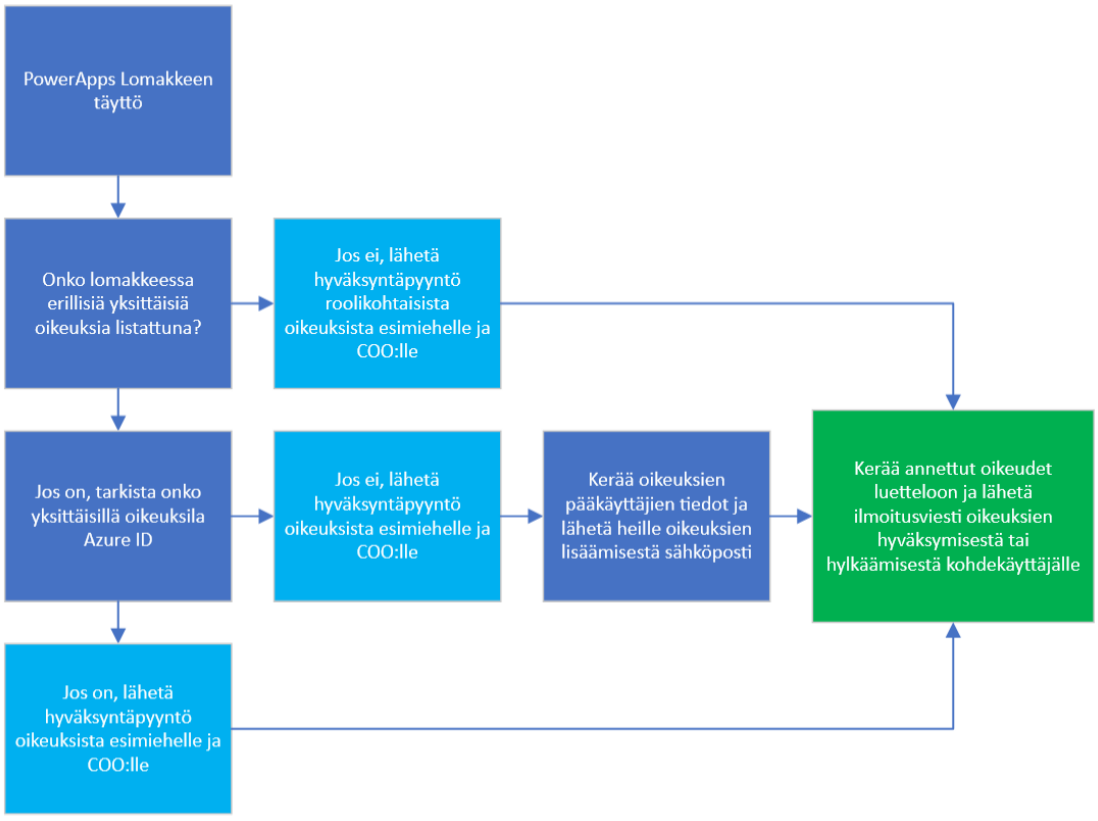
oikeuksia lisätään sekä rooliryhmät, joiden oikeuksia käyttäjä saa. Lisävalintana käyttäjälle voidaan lisätä yksittäisiä oikeuksia. Rooliryhmät tulevat linkitettynä Microsoft Lists -sovelluksesta ”Role based access rights” -listasta, johon kaikki organisaation roolit on koottu. Yksittäiset lisäoikeudet linkittyvät myös samaan Lists-sovellukseen. Tämäkin PowerApps-lomake on organisaation sisäisesti kehittämä. Kuvasta 5 nähdään oikeuksien lisäämisen lomake.



Kuva 5. Oikeuksien lisääminen käyttäjälle. (Mapvision Oy 2024.)

Kun lomake on täytetty, käynnistyy taustalla seuraavanlainen automaatio:

1. Taustalla toimiva PowerAutomate käy läpi kaikki rooliryhmät, jotka lomakkeeseen on listattu.
2. Oikeuksien hyväksyntäkutsu COO:lle sekä lomakkeen täyttäjän esihenkilölle.
3. Kaikki rooliryhmille annetut oikeudet käydään läpi järjestyksessä
    a. Jos oikeudella on Azure AD id, käyttäjä lisätään automaattisesti kyseiseen Azure-oikeuteen.
        i. Azure id löytää siihen liittyvät oikeudet erillisestä listasta
    b. Käyttöoikeuspyynnöt ryhmiin ja järjestelmiin, joihin Netox liittää henkilöitä manuaalisesti, kerätään yhteen viestiin
    c. Jos oikeudelle on pääkäyttäjä, lähetetään pääkäyttäjälle sähköposti oikeuksien luomisesta
        i. Samalla lähtee annettavalle käyttäjälle sähköposti oikeuksien saamisesta
4. Kun kaikki oikeudet on lisätty käyttäjälle, PowerAutomate lähettää käyttäjälle viestin siitä, mitä oikeuksia tälle on annettu



Kuva 6. Käyttäjälle oikeuksien lisäämisen prosessi

Käyttäjäoikeuksien lisäämisessä on yritetty panostaa prosessin hyväksyntöihin esihenkilöiltä, jotta oikeuksien lisääminen ei altistuisi väärinkäytölle. Käyttäjälle oikeuksien lisäämisen yksinkertaistetun prosessikaavion näkee kuvasta 6 ja yksityiskohtaisen prosessin kaavio on nähtävissä liitteestä 3.

5.3 Käyttäjäoikeuksien poistaminen

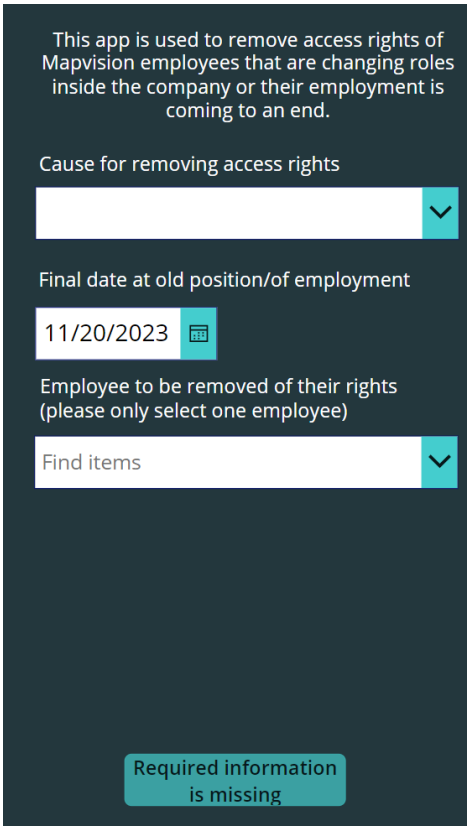
Kun käyttäjä siirtyy organisaation sisällä eri tehtäviin, tai käyttäjän toiminta organisaation kanssa loppuu, on oikeuksien mitätöimiselle myös luotu oma PowerApps-applikaatio. Lomakkeessa on kaksi eri vaihtoehtopolkua: työsuhteen päättäminen tai roolin vaihtuminen.

Työsuhteen päättyessä valitaan ”Termination of employment”, jolloin PowerAutomaten avulla henkilön kaikki oikeudet poistetaan. Oikeuksien poiston voi ajoittaa tiettyyn päivään, jona PowerAutomate käynnistyy. Käyttäjän tunnuksia ei kuitenkaan virallisesti poisteta kokonaan organisaation listoilta, vaan tunnus asetetaan ”disabled”-tilaan. Tällöin jos käyttäjätunnusta vielä tarvitaan tulevaisuudessa, voidaan aktivoida vanha tunnus ilman uuden luomista. Tämä ominaisuus on myös oletuksena päällä Entra ID -palvelussa. Poistetut käyttäjät kuitenkin poistuvat lopullisesti tietyn ajanjakson jälkeen. Käyttäjän poistamisen aikana käynnistyy taustalla seuraavanlainen työnkulku:

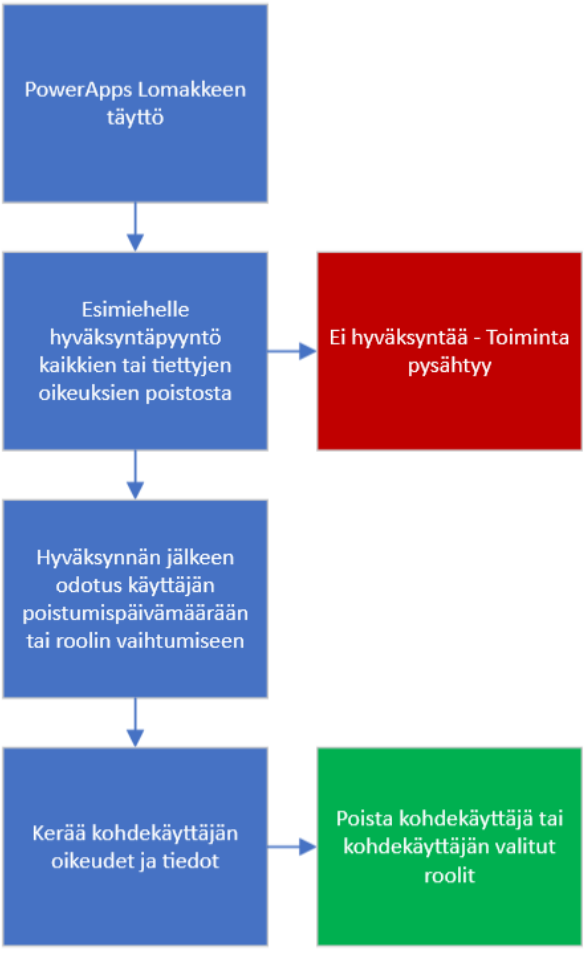
1. Sovelluksen käyttäjä antaa tiedot PowerApps-sovellukselle
2. Esihenkilölle lähetetään hyväksymissähköposti kohdekäyttäjän kaikkien oikeuksien poistamisesta
3. Odota ilmoitettuun irtisanomispäivään
4. Kerää kohdekäyttäjän tiedot oikeuksista
5. Poistetaan henkilö Entra ID -palvelusta

Kun käyttäjän rooli vaihtuu, valitaan ”Role change inside the company”, jolloin järjestelmä etsii käyttäjän kaikki nykyiset annetut oikeudet. Tämän listan avulla voidaan poistaa kaikki tarpeettomaksi jääneet oikeudet. Käyttäjälle uuden roolin vaatimat oikeudet lisätään oikeuksien lisäämiseen tarkoitetulla työkalulla. Roolinvaihdossa käynnistyy seuraavanlainen työnkulku:

1. Sovelluksen käyttäjä antaa tiedot PowerApps-sovellukselle
2. Esihenkilölle lähetetään hyväksymissähköposti kohdekäyttäjän roolin vaihtumisesta ja tiettyjen oikeuksien poistamisesta
3. Odotetaan roolinvaihtumispäivämäärään saakka
4. Kerätään kohdekäyttäjän tiedot oikeuksista ja poista niistä lomakkeelle valitut roolit



Kuva 7. Käyttäjän poistoon luotu työkalu (Mapvision Oy 2024.)



Kuva 8. Käyttäjän roolinvaihtumisen tai poistamisen prosessi

Käyttäjän oikeuksien poistamisen PowerApps-työkalun näkymä ja prosessin vaiheet nähdään kuvista 7 ja 8. Kuten prosessista huomataan myös tilanteessa, jossa esihenkilö ei hyväksy poistoprosessia, mitään ei tapahdu. Poistoprosessi jää siis kesken ja käyttäjän oikeuden pysyvät voimassa.

6 TISAX-VAATIMUKSIEN TÄYTTYMINEN NYKYISELLÄ RATKAISULLA

Osa tutkimustyön kokonaisuutta on vertailla TISAX-käyttäjänhallinnalle asetettujen vaatimuksien täyttymistä organisaation nykyisen käyttäjänhallinnan toimintamalleja vastaan. TISAX-vaatimuksien tarkastelulla saadaan tietoa siitä, riittävätkö organisaation käyttäjänhallintaoikeuksien prosessit auditoinnista, jolloin havaittuja puutteita voidaan käyttää työn kehityskohteina.

TISAX-käyttäjänhallinnalle asetetut vaatimukset löytyvät ENX-järjestöltä vapaasti ladattavana Excel-tiedostona. Tätä hyödyksi käyttäen voidaan vertailla ja arvioida nykyistä organisaation toimintaa taulukkoa vasten. Taulukossa olevat kysymykset ja niitä vastaavat organisaation toimintamallit on selvitetty niitä vastaavista henkilöiltä yrityksestä. Henkilöitä on joko haastateltu yksittäisiin kohtiin tai näitä kysymyksiä on käyty läpi jo valmiiksi yrityksen valmistauduttua TISAX-auditointia varten. Samalla on tehty arviointia mahdollisesta saavutettavasta vaatimustasosta perustuen jo aiempaan roolipohjaisen käyttäjähallinnan selvitystöihin sekä organisaation henkilöstön tietoihin.

TISAX on kokonaisvaltainen tietoturvaviitekehys, jonka yksi osa on käyttäjänhallinta. Tämän työn aikana tarkastellaan vain käyttäjän hallitsemisen vaatimuksia. Alla olevista taulukoista 3, 4, 5 ja 6 nähdään TISAX-käyttäjänhallinnan vaatimukset ja miten ne on nykyisellään toteutettu organisaatiossa.

Taulukko 3. Käyttäjänhallinta aihe vaatimus 1 (ENX 2023)

	To what extent is the use of identification means managed?
Objective	To check the authorization for both physical access and electronic access, means of identification such as keys, visual IDs or cryptographic tokens are often used. The security features are only reliable if the use of such identification means is handled adequately.
Requirements (must)	+ The requirements for the handling of identification means over the entire lifecycle are determined and fulfilled. The following aspects are considered: - Creation, handover, return and destruction, - Validity periods, - Traceability, - Handling of loss.
Requirements (should)	+ Identification means can be produced under controlled conditions only.
Additional requirements for high protection need	+ The validity of identification means is limited to an appropriate period. (C, I, A) + A strategy of blocking or invalidation of identification means in case of loss is prepared and implemented as far as possible. (C, I, A)
Additional requirements for very high protection need	None

Organisaation elektronisiin laitteisiin on käytössä Microsoft Entra ID -tunnukset, joissa on Single Sign On sekä MultiFactor Authentication vaadittuna. Fyysinen identifiointi on hoidettu elektronisilla avaimilla kiinteistön omistajayrityksen kautta. Näiden tietojen ja aikaisemmin työssä selvitettyjen prosessien avulla voidaan todeta, että ainakin kohta ”Requirements (should)” toteutuu.

Taulukko 4.Käyttäjänhallinta aihe vaatimus 2 (ENX 2023)

	To what extent is the user access to network services, IT systems and IT applications secured?
Objective	Only securely identified (authenticated) users are to gain access to IT systems. For this purpose, the identity of a user is securely determined by suitable procedures.
Requirements (must)	+ The procedures for user authentication have been selected based on a risk assessment. Possible attack scenarios have been considered (e.g. direct accessibility via the internet). + The procedures applied for user authentication comply with the current state of the art.
Requirements (should)	+ The user authentication procedures are defined and implemented based on the business-related and security-relevant requirements: - Users are authenticated at least by means of strong passwords according to the state of the art. + Superior procedures are used for the authentication of privileged user accounts (e.g. Privileged Access Management, two-factor authentication).
Additional requirements for high protection need	+ Depending on the risk assessment, authentication procedure and access control have been enhanced by supplementary measures (e.g. permanent access monitoring with respect to irregularities or use of strong authentication, automatic logout or disabling in case of inactivity). (C, I, A)
Additional requirements for very high protection need	+ Before gaining access to data of very high protection needs, users are authenticated by means of strong authentication (e.g. two-factor authentication) according to the state of the art. (C, I)

Organisaatiolla on käytössään Microsoft Entra SSO, eli Single Sign On -järjestelmä, jolloin kaikki pääsy tietoverkkopalveluihin on järjestetty Microsoft Entran kautta. Organisaation tavoitteena on käyttää kaikissa verkkopalveluissa Entra SSO -integrointia. Myös MultiFactor Authentication, eli monivaiheinen tunnistautuminen, on Microsoft Entran hallinta-asetuksista kytketty päälle. Tällöin jos Entra SSO ei ole mahdollinen vaihtoehto pääsynhallinaksi verkkojärjestelmiin, voidaan käyttää monivaiheista tunnistautumista sekä VPN-yhteyksiä. Riskinarviointia on suoritettu sisäisesti ja dokumentoitu IT-dokumenttirekisteriin, jota johtava porras tarkastelee.

Näiden organisaation järjestelmien pohjalta, sekä aikaisemmin työssä selvitettyjen prosessien kanssa voidaan todeta, että minimivaatimukset täyttyvät. Voidaan myös arvioida, että TISAX-auditoinnissa saadaan vaatimuslistalta täytettyä kohta ”Additional requirements for high protection need”.

Seuraavassa taulukossa 5 käsitellään käyttäjien tunnuksien tietojen sekä kirjautumistunnuksien hallintaa. Tämä aihe on neljästä kohteesta vähiten liittyvä roolipohjaiseen käyttäjänhallintaan, koska se käsittelee lähinnä tietoturvan tärkeydestä käyttäjätunnuksien autentikoinnissa. Vertailukohde on kuitenkin tärkeä auditoinnissa, joten sitä tulee tutkia yhtä tarkasti kuin muitakin kohteita.

Taulukko 5. Käyttäjänhallinta aihe vaatimus 3 (ENX 2023)

	To what extent are user accounts and login information securely managed and applied?
Objective	Access to information and IT systems is provided via validated user accounts assigned to a person. It is important to protect login information and to ensure the traceability of transactions and accesses.
Requirements (must)	+ The creating, changing and deleting of user accounts is conducted. + Unique and personalized user accounts are used. + The use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable). + User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract). + User accounts are regularly reviewed. + The login information is provided to the user in a secure manner. + A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used). + The login information (e.g. passwords) of a personalized user account must be known to the assigned user only.
Requirements (should)	+ A basic user account with minimum access rights and functionalities is existent and used. + Default accounts and passwords pre-configured by manufacturers are disabled (e.g. by blocking or changing of password). + User accounts are created or authorized by the responsible body. + Creating user accounts is subject to an approval process (four-eyes principle). + User accounts of service providers are disabled upon completion of their task. + Deadlines for disabling and deleting user accounts are defined. + The use of default passwords is technically prevented. + Where strong authentication is applied, the use of the medium (e.g. ownership factor) is secure. + User accounts are reviewed at regular intervals. This also includes user accounts in customers' IT systems.
Additional requirements for high protection need	None
Additional requirements for very high protection need	None

Organisaatio käyttää pääsääntöisesti henkilökohtaisia käyttäjätilejä. Poikkeustapauksia, joissa käytetään jaettuja käyttäjätilejä, on hyvin vähän. Näissä tapauksissa on arvioitu käyttäjätilien jakamista riskinarvioilla. Ensimmäisen ker-

ran käyttäjätunnuksen salasanan toimittaminen käyttäjälle järjestetään eri informaatiokanavia pitkin, kuin käyttäjän vastaanottavien tilien kautta. Usein käyttäjälle luovutetaan salasana henkilökohtaisesti paperisena. Käyttäjän tulee vaihtaa käyttäjätunnuksiensa salasana ensimmäisellä kirjautumiskerrallaan. IT-järjestelmien pääkäyttäjien tulee valvoa ja hallita järjestelmiensä käyttäjätilejä säännöllisesti auditointi- ja valvontaohjeiden mukaisesti. Tätä säännöllistä tarkastelua hallitsee myös Business Excellence -tiimijärjestelmä.

Näiden tietojen pohjalta, sekä aikaisemmin työssä selvitettyjen käyttäjätunnusten hallintaprosessien kanssa, arvioidaan TISAX-auditoinnista saatavan taso ”Requirements (should)”. Tällöin minivaatimukset täyttyvät.

Taulukko 6. Käyttäjänhallinta aihe vaatimus 4 (ENX 2023)

	To what extent are access rights assigned and managed?
Objective	The management of access rights ensures that only authorized users have access to information and IT applications. For this purpose, access rights are assigned to user accounts.
Requirements (must)	+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification and approval, - Application the minimum (“need-to-know”) principle. + The access rights granted for normal and privileged user accounts and technical accounts are verified at regular intervals also within IT systems of customers.
Requirements (should)	+ Strategies for authorizing access to information are prepared. + Authorization roles are used. + Rights are allocated on a need-to-use basis and according to the role and/or area of responsibility. + Normal user accounts are not granted privileged access rights. + The access rights of a user account are adapted after the user has changed (e.g. to another field of responsibility).
Additional requirements for high protection need	+ The access rights are approved by the responsible internal Information Officer. (C, I, A)
Additional requirements for very high protection need	+ Prevention of unauthorized persons gaining access and information (privileged users): (C) - Information is stored in encrypted form at content level (e.g. file level). - Where encryption is not feasible, information shall be protected by similarly effective measures. + Existing access rights are regularly reviewed at shorter intervals (e.g. quarterly) (C)

Aikaisemmin työn aikana selvitetyn käyttäjätunnusten oikeuksien hallinnan prosessia voidaan verrata tähän TISAX-vaatimustaulukkoon. Prosessin perusteella voidaan arvioida auditoinnin aikana saavutettavan vaatimustaso ”Additional requirements for high protection need”.

Näiden läpikäytyjen TISAX-tarkastuslistojen avulla voidaan todeta, että organisaatiolle tehdyn tarkastusauditoinnin arvioidaan menevän läpi. Arviointi perustuu näiden kohtien vähimmäisvaatimuksien saavuttamiseen. Muita TISAX-auditoinnin aikana käytyjä tarkastuskohteita ei otettu huomioon.

7 ENTRA ID -PALVELUIDEN VERTAILU

Kuten nykyisen toimintamallin selvityksestä huomataan, Entra ID on jo käytössä yrityksen käyttäjänhallinnan prosessissa. Yrityksen Entra ID- sekä Azure Active Directory Premium P1 -palvelut ovat sisältyneet yrityksen olemassa olevaan Office business -lisenssiin. Työn kehityksen kannalta on tärkeää selvittää mitä hyötyjä ja eroja nykyisen Premium P1- ja Premium P2 -version välillä on. Tärkeimmät erot käyttäjätietojen hallinnasta sekä identiteetin turvaamisesta näemme seuraavista taulukoista 7 ja 8.

Taulukko 7. Hinnoittelu käyttäjätietojen hallinnasta (Microsoft Security 2024)

Käyttäjätietojen hallinta	Microsoft Entra ID, maksuton	Azure Active Directory Premium P1	Azure Active Directory Premium P2	Microsoft Entra ID Governance
Käyttäjienn automatisoitu valmistelu SaaS-sovelluksia varten	x	x	x	x
Käyttäjien automatisoitu käyttöönotto paikallisiin sovelluksiin		x	x	x
Ryhmien automatisoitu valmistelu sovelluksia varten		x	x	x
HR-lähtöinen valmistelu		x	x	x
Käyttöehtojen vahvistaminen		x	x	x
Käyttöoikeuksien perusvarmistukset ja tarkistukset			x	x
Koneoppimisen avustama käyttöoikeuksien myöntäminen ja tarkistukset				x
Oikeuksien perushallinta			x	x
Oikeuksien hallinta – tehtävien erottaminen			x	x
Oikeuksien hallinta varmennettujen tunnusten avulla				x
Elinkaaren työnkulut				x
Käyttäjätietojen hallinnan koontinäyttö				x
Käyttäjätietojen erityisoikeuksien hallinta (PIM)			x	x

Kuten taulukosta 7 huomaamme, yrityksen käyttämässä P1 -paketissa ei ole käyttäjätietojen hallintaan tärkeitä ominaisuuksia, jotka P2 Premium -paketissa on. Näistä tärkein on käyttäjätietojen erityisoikeuksien hallinta (PIM). Yrityksen käyttämä ulkopuolinen IT-palveluorganisaatio Netox on ehdottanut ja jopa vaatii uusilta kumppaneiltaan Active Directory Premium P2 -palvelupaketin käyttöä. Päällimmäisenä syynä on PIM-hallinta, eli käyttäjätietojen erityisoikeuksien hallinta.

Privileged Identity Management eli PIM mahdollistaa keskitetyn hallinnan käyttäjätietojen erityisoikeuksien hallintaa roolipohjaisille tai yksittäisille käyttöoikeuksille Microsoft Groupsissa, Azuressa ja Entra -rooleissa. PIM:n tarkoituksena on antaa käyttäjälle oikeus hallita ylläpitäjän valitsemia erillisiä oikeuksia. Oikeudet voidaan myöntää käyttäjille "just-in-time" eli juuri oikeaan aikaan, aikaperusteisesti tai pysyvästi. Käyttäjä voi käydä aktivoimassa oikeudet itselleen hallintapaneelista ylläpitäjän määrittelemällä tavalla. PIM:n tarkoitus on vähentää riskiä liiallisen, tarpeettoman tai väärinkäytetyn roolituksen suhteen. (Microsoft PIM 2024.)

Taulukko 8. Hinnoittelu käyttäjätietojen suojauksessa (Microsoft Security 2024)

Käyttäjätietojen suojaus	Microsoft Entra ID, maksuton	Azure Active Directory Premium P1	Azure Active Directory Premium P2	Microsoft Entra ID Governance
Riskipohjaiset ehdolliset käyttöoikeudet (kirjautumisriski, käyttäjien riski)			x	
Todentamiskonteksti (siirtymistodentaminen)			x	
Laite- ja sovellussuodattimet ehdollisia käyttöoikeuksia varten			x	
Tunnusten suojaus			x	
Haavoittuvuudet ja riskialttiit tilit			x	
Riskitapahtuman tutkinta		x	x	

Taulukosta 8 havaitaan, että vain yksi ominaisuus on käytettävissä P1-palvelupaketissa verrattuna P2-palvelupakettiin. Käyttäjätietojen suojauksessa palvelupaketti P2 on siis huomattavasti laajemmalla tasolla kuin P1. Kaikki puuttuvat ominaisuudet ovat tärkeitä omalla osa-alueellaan, mutta tärkeimpänä ominaisuutena organisaatiolle on Laite- ja sovellussuodattimet ehdollisia käyttöoikeuksia varten, joka P1 -paketista puuttuu. Laite- ja sovellussuodattimet toimivat hyvin samankaltaisesti kuin dynaamiset ryhmät. Tällöin pystytään hallitsemaan pääsyoikeuksia suodattamalla laitteita niiden attribuuttien kanssa.

Silloin organisaation omistamiin palveluihin voidaan sallia vain halutut laitteet. Esimerkiksi yrityksen SharePoint-verkkosivuille päästetään vain yrityksen hallinnassa olevia laitteita.

Tässä vertailussa otettiin huomioon palvelupaketeista vain käyttäjätietojen hallinnan ja suojauksen ominaisuudet. Vertailun tuloksina havaitaan, että P2-palvelupaketti tarjoaa laajemmin ja monipuolisemmin ominaisuuksia kuin P1. Tietoturvan näkökulmasta on selvää, että yrityksen tulisi siirtyä P2-palvelupakettiin, jotta kaikki mahdolliset ominaisuudet käyttäjänhallintaan ja identiteetin suojaukseen varmistuvat. Ratkaisuja ei kuitenkaan tehdä ihannetilanteiden perusteella, vaan realistisella näkökulmalla huomioiden myös, ettei yrityksellä välttämättä ole kustannussyistä mahdollisuuksia hankkia laajempaa pakettia ilman syvempää vertailua. Azure Active Directory Premium P2 -paketti tarjoaa monipuolisemmin käyttäjänhallinnan ratkaisuja tulevaisuuden näkökulmalta, ja vaikka yritys ei tällä hetkellä välttämättä tarvitse pakettia, on syytä varautua suurentuneen henkilöstömäärän takia selvittämään, onko kustannuksellisesti järkevää siirtyä P2-palvelupakettiin.

8 KEHITYSEHDOTUKSET

Tutkimuksen herättämien havaintojen sekä analyysien perusteella voidaan esittää organisaatiolle ehdotuksia, miten roolipohjaisia käyttäjähallinnanprosesseja voidaan kehittää. Ehdotukset perustuvat aiemmin esitettyihin teorioihin ja käytäntöihin, sekä yleisiin tietoturvallisiin käytäntöihin. Tutkimuksen kehitysehdotuksissa on myös huomioitu TISAX-vaatimukset käyttäjänhallinnan osuudelta, mikä takaa organisaation TISAX-sertifiointiprosessin huomioonoton.

Kehitysehdotuksissa on myös huomioita, joita havaittiin tämän opinnäytetyön teon aikana. Näitä ehdotuksia kerättiin suurimmaksi osaksi yrityksen henkilöstön antamien havaintojen ja palautteiden kautta. Nämä ehdotukset kerättiin myös omien havainnontien kanssa kenttäpöytäkirjaan, jota ylläpidettiin läpi opinnäytetyön. Kenttäpöytäkirjan voi kokonaisuudessaan havaita liitteestä 1.

8.1 Rooliryhmät ja ryhmälistat

Yrityksen nykyisen käyttäjänhallintaprosessin ratkaisemisen aikana huomioitiin suuri määrä ryhmiä ja roolilistoja, kuten kenttäpöytäkirjan 14.11.2023 kohdassa esitetään. Kenttäpöytäkirjahuomion mukaan rooliryhmiä on 325. Näitä listoja läpikäydessä huomattiin myös, että organisaatio ei ole perillä kaikista listoilla olevista ryhmistään. Näiden ryhmien mukana oli myös ryhmiä, joissa ei ollut yhtäkään jäsentä. Tämä ei välttämättä ole huono indikaatio, sillä ryhmä voi olla tarpeellinen, jos sinne tulee lisättyä käyttäjiä väliaikaisesti saamaan roolipohjaisia oikeuksia.

Tietoturvan kannalta tärkeää on kuitenkin minimoida mahdolliset riskipinnat, eli tyhjät sekä hallitsemattomat ryhmät tulee poistaa. Yleisimmin hyökkäykseen altistuvia riskipintoja ovat salasanat, avonaiset portit, sähköpostiturvallisuus tai sovellusten päivittämättömyys, mutta riskipinnoiksi voidaan myös luokitella kaikki mahdolliset digitaaliset sekä fyysiset organisaation hallussa olevat järjestelmät ja alueet. Riskipintojen ehkäisyksi on järkevää vähentää kompleksisuutta sekä implementoida Zero Trust -mallia järjestelmiin. (Fortinet 2024.)

Unohtuneet ryhmät, joihin on jäänyt käyttöoikeuksia, voivat luoda riskin yksittäisen käyttäjän oikeuksien väärinkäyttöön. Listat ja ryhmät luovat siis ylimääräisen riskipinnan ja niitä tulisi tarkastella, onko niitä mahdollista poistaa. Listojen siivoamisen aikana on hyvä huomioida, että jokainen luotu Teams -kanava näkyy listattuna, joten on pidettävä erityistä huolta valittaessa poistettavia ryhmiä.

Näillä jokaisella rooliryhmällä on myös oletetusti joku käyttäjä, joka hallitsee ryhmää. Ryhmillä on myös suurimmaksi osaksi vain yksi omistajakäyttäjä. Tällöin törmätään ongelmatilanteeseen, jossa ryhmän omistaja poistuu organisaatiosta, tai muuten estyy käyttämästä tunnuksia. Ratkaisuksi tähän yrityksen tulisi pitää vähintään kahta henkilöä omistajana jokaisessa ryhmässä. Tällöin vältytään turhilta ja ylimääräisiltä mahdollisilta katkoksilta ryhmään vaikuttavissa asioissa, vähennetään riskiä yksilöllisestä vikaantumispisteestä, vähennetään omistusoikeuden väärinkäyttöä ja vahvistetaan vastuullisuutta.

8.2 Entra ID

Merkittävä havainto tehtiin kenttäpöytäkirjaan 17.1.2024 liittyen Entra ID -järjestelmän ominaisuuksien vähäiseen hyödyntämiseen. Erityisesti dynaamisten ryhmien havaittiin olevan lähes olemattomat. Kenttäpöytäkirjahuomiossa yhteensä vain 23 ryhmää oli havaittu olevan dynaamisena ryhmätyyppinä. Entra ID -palvelussa roolipohjaisten käyttäjänhallinnan ominaisuudet ovat hyvinkin laajat. Nykyisellään yrityksen käyttäjänhallinnan automatisoitu prosessi toimii hyvinkin paljon itserakennetun PowerApps PowerAutomate -sovelluksen päällä. Ryhmät ja roolit on alun perin luotu Entra ID -palveluun normaaleina ”assigned” ryhminä. Tällä hetkellä prosessi ei siis käytä hyödykseen Entra ID:n tarjoamia sisäisiä työkaluja käyttäjänhallintaan, jolloin prosessin yksinkertaistaminen ja automatisoiminen on paljon monimutkaisemmin ratkaistu – tässä tapauksessa erillisellä omalla työkalulla. Kehitysehdotuksena yrityksen tulisi muokata olemassa olevia oikeudellisia ryhmiä, joihin lisätään dynaamisiksi ryhmiksi käyttäjiä perustuen heidän yleisiin attribuutteihinsa. Tällöin käyttäjien ryhmiin lisäämisen monimutkaisuus vähenee ja prosessi automatisoituu. Myös yrityksen oman käyttäjänhallintatyökalun prosessi yksinkertaistuu ja näin vältetään ylimääräisiä riskikohteita käyttäjänhallintaprosessin aikana.

Työn aikana havaittiin myös tilanteita, joissa perusoikeuksilla oleva käyttäjä pystyy navigoimaan Entra ID -palvelualustalla vapaasti ilman laajempia estoja. Käyttäjän vastuiden mukaan on hyvä olla oikeuksia Entra ID -palvelun eri osiin ja hallintakomponentteihin. On kuitenkin hyvä miettiä tässäkin Zero Trust -politiikkaa, jolloin kaikki alueet ja prosessit, joihin käyttäjällä ei ole tarvetta saada pääsyä, on tietoturvallisuuden kannalta hyvä pitää käyttäjältä estettynä. Myös muissa hallinnollisissa asioissa olisi tärkeää pitää kiinni Zero Trust -mallista, kuten on tehty myös Microsoft List -sovelluksen ”Role based access rights” -taulukossa, josta löytyy kaikki roolipohjaiset ryhmät. Entra ID -järjestelmään peruskäyttäjänä pääsy voi aiheuttaa ylimääräisiä tietovuotoriskejä, ja tulisi paikata ongelmien välttämiseksi (AdminDroid 2024).

Työn aikana myös huomattiin, että peruskäyttäjällä on oikeus luoda Entra ID -järjestelmään uusia käyttäjäorganisaatioita. Jos tavallinen käyttäjä pystyy ilman järjestelmänvalvojan oikeuksia luomaan uusia käyttäjäorganisaatioita järjestelmään, tämä tunnistetaan suureksi tietoturvariskiksi (Microsoft Azure

2024). Yrityksen tulisi kytkeä Entra ID -järjestelmänvalvojakeskuksesta tavallisilta käyttäjiltä pois päältä asetus käyttäjäorganisaatioiden luomisesta. Ilman asetuksen muuttamista käyttäjillä on täysin vapaa mahdollisuus lisätä uusia käyttäjäorganisaatioita. Käyttäjillä on myös mahdollisuus luoda security-ryhmiä omatoimisesti, jolloin organisaation protokollien ja prosessien mukainen hyväksymisprosessi ryhmien luomiseksi ja oikeuksien hallinnoimiseksi ohitetaan. Tämä valinta tulisi estää peruskäyttäjiltä Entra ID -järjestelmässä.

Vaikka ehdotuksissa todetaan, että käyttäjänhallinta olisi yrityksen kannalta parempi hoitaa muilla valmiilla palveluratkaisuilla, ei käyttäjänhallintasovellus ole kuitenkaan tarpeeton. Nykyisen prosessin ratkaisut ja työkalut ovat monin tavoin hyödyllisiä. TISAX-määrityksissä havaitaan, että käyttäjän oikeuksien lisäämisprosessin aikana tulisi olla tiettyjä turvallisuusominaisuuksia, kuten toisen osapuolen tai esimiehen hyväksyntäprosessi aina oikeuksien lisäämisen aikana. Nykyinen oikeuksien lisääminen, sekä käyttäjän luominen toimii erittäin hyvin tähän tarkoitukseen.

8.3 Käyttäjän poistoprosessi

Käyttäjän poistoprosessista kirjattiin kenttäpöytäkirjaan useita kohtia, jotka nousivat aiheeksi PowerApps -sovelluksen käytön jälkeisinä keskusteluissa, kuten esimerkiksi päiväykselle 27.10.2023 merkityssä muistiinpanosta havaitaan. Keskusteluja käytiin lähinnä sähköpostin välityksellä, mutta huomioita kirjattiin ylös, koska havaintoihin nähtiin tärkeäksi löytää ratkaisuja. Erityisesti kenttäpöytäkirjassa huomioitiin, onko mahdollista, että oikeuksia jää aktiiviseen tilaan käyttäjän poiston jälkeenkin.

Käyttäjän poistuessa yrityksestä prosessin nykyinen toiminta deaktivoi käyttäjätunnuksen mahdollista myöhempää takaisinaktivointia varten. Käyttäjätunnuksen siirryttyä passiiviseen tilaan sen kaikki oikeudet tileiltä siirtyvät myös epäaktiiviseen tilaan. Tämä kuitenkin toimii pelkästään Microsoft-kohtaisiin oikeuksiin, kuten sähköpostitiliin ja muihin Microsoft-ryhmiin. Tällöin kohdataan ongelma, jolloin oikeudet, jotka ovat erillisenä Microsoftin alaisissa palveluissa, jäävät aktiiviseen tilaan. Näitä ovat yrityksen tapauksessa erilliset pää-

käyttäjälliset palvelut, kuten esimerkiksi Siemens NX -tunnukset. Tällöin käyttäjällä on edelleen mahdollisuus käyttää erillisiä tunnuksia vaativia palveluita, vaikka käyttäjän oikeudet yrityksen sisällä ovat poistuneet.

Organisaatiolla on tärkeä olla protokollia käyttäjän tiedoille sekä oikeuksille henkilön poistuessa yrityksestä. On erittäin tärkeää poistaa kaikki oikeudet niin fyysiset kuin digitaalisetkin oikeudet sekä kerätä organisaation omistamat laitteet. Käyttäjältä tulee myös evätä pääsy kaikkiin saavutettaviin yrityksen informaatioihin, joita ei julkisesti jaeta. Poistuneiden käyttäjien oikeuksia tulisi myöhempinä ajankohtina monitoroida mahdollisen väärinkäytön kannalta sekä varmistaa, että pääsy on estetty. (NIST 2020b.)

Käyttäjätunnuksien automatisoidun poistoprosessin aikana henkilön esihenkilöille lähetetään hyväksymispyyntö. PowerAutomate-ohjelmointi nykyisen poistoprosessin aikana kuitenkin mahdollistaa prosessin jäävän seisahtuneeseen tilaan, jos hyväksyntäpyyntöön ei koskaan vastata. Poistoprosessi siis jää odottamaan vastausta hyväksyntäpyynnöltä, ennen kuin jatkaa prosessia sekä määrittelee poistettavat käyttäjät tai oikeudet ja suorittaa poiston. On siis mahdollista, että poistetuksi luultu käyttäjä säilyttääkin oikeudet, koska hyväksyntä tai hylkääminen on jäänyt tekemättä kaikilta vaadittavilta henkilöiltä. PowerAutomaten toimintaan kuuluu, että 90 päivän epäaktiivisen tilan jälkeen prosessitoiminta lakkautetaan (Power Automate 2024). Tämä tarkoittaa sitä, että unohtaessaan vastata hyväksymispyyntöön, 90 päivän jälkeen käyttäjän oikeuksien poistoprosessi tulisi muistaa aloittaa uudestaan.

Kehitysehdotuksena näihin kohtiin tarvitsee käyttäjänpoistoprosessin automatisointiin lisätä työnkulkuja. Erillisten palveluiden pääkäyttäjille ilmoitetaan, että käyttäjän tunnukset on poistettava tai sijoitettava deaktivoituun tilaan sekä poistettavien käyttäjien esihenkilöille lähetetään muistutusviesti tietyin väliajoin, kunnes hyväksymispyyntö on tehty. Pääkäyttäjät saavat tällöin käyttäjän poistosta tarpeellisen informaation, joka muuten voisi jäädä huomioimatta sekä poistettavien käyttäjien esihenkilöt muistaisivat hyväksyä tai hylätä pyynnon ajallaan. Automatisointiin olisi myös hyvä lisätä kohta, jossa pääkäyttäjältä vaaditaan vahvistus kyseessä olevien oikeuksien poiston loppuun suorittamisesta. Tällä varmistettaisiin, että yrityksestä poistuneelle käyttäjälle ei jää mitään palveluita saavutettavaksi.

8.4 Lokitietojen kerääminen

Yrityksen prosessissa ei tällä hetkellä käsitellä lokitietoja ollenkaan. Microsoft PowerAutomate tallentaa lokitietoja käynnistetyistä prosesseista, mutta säilyttää niitä vain 28 päivää GDPR-lakien mukaisesti. Nämä valmiiksi luodut lokitiedot kertovat tärkeitä tietoja, kuten aloitusajan, käyttäjän ja prosessin onnistumisen. Tarvittaessa prosessikulkuja sekä tapahtumatietoja voidaan tarkastella jälkikäteen, koska prosessissa lähetetään useita sähköposteja, joista löytyy tärkeää informaatiota käynnistetystä prosessista.

Minkäännäköistä oikeaa automatisointia lokitietojen keruuseen ei ole tehty, vaikka tämä olisi erittäin tärkeää muutoksia vaativiin prosesseihin. (Kyberturvallisuuskeskus 2024). Yrityksen tulisi lisätä vähintään PowerAutomaten automaattisten lokitietojen automatisoitu kerääminen, että lokitiedot ovat tarvittaessa saatavilla myöhemminkin. Jotta lokitietoja voitaisiin hyödyntää parhaiten, niiden keräys tulisi lisätä kuhunkin PowerAutomate-prosessiin, jolloin mahdollisimman useaa sekä tarpeellista tietoa voidaan kerätä tulevaisuuden varalle. Koska prosessissa lähetetään useita sähköposteja, joista löytyy tärkeää informaatiota käynnistetystä prosessista, voidaan lokitietoja päätellä ainakin osittain.

8.5 Prosessin dokumentointi

Kenttäpöytäkirjaan kirjatussa huomiossa tällä hetkellä nykyisen käyttäjän lisäämisen ja poistamisen ja oikeuksien lisäämisen prosesseja ei ole dokumentoitu minkäänlaisella tavalla. Tämän työn aikana tehdyt selvitykset olivat ensimmäiset selvitykset käyttäjänhallintaprosessista. Liitteistä 1 ja 2 löytyvät ainoat tulkintakaaviot, jotka yrityksellä on prosessista. Ennen opinnäytetyötä yrityksellä oli vain henkilökohtaisen tietämyksen tasolla dataa siitä, miten käyttäjänhallintaprosessia hallitaan.

Organisaation olisi myös hyvä lisätä kommentteja PowerAutomaten käyttäjänhallintaprosessin ohjelmointiin, jolloin myöhempien muutosten aikana ei tule väärinymmärryksiä jonkun muun luomasta automaatiosekvenssistä. Prosessin ohjelmoinnin dokumentointi ja kommentointi on tärkeää useastakin eri syistä.

Tällä hetkellä työskentely prosessin kanssa on ollut lähinnä yhden henkilöt toimesta, mutta tulevaisuuden varalta dokumentointi hyödyttää tiimityöskentelyä erityisen paljon. Tämä ehkäisee samalla tiedon katkeamisen, jos prosessia työstävä henkilö poistuu yrityksestä. Prosessin dokumentointi auttaa myös jatkuvan parantamisen mallin hallitsemisessa sekä vähentää riskejä väärinymmärryksille. Tällöin prosessiin muutosta vaativa taho voi varmistua siitä, että vaadittu muutos on myös toteutettu niin kuin on alun perin tarkoitettu. (Notion 2023.)

9 KEHITYSTYÖ

Konkreettiseen kehitystyöhön valittiin työn aikataulurajoitteiden takia vain muutamia aiemmin tehtyjä kehitysehdotuksia. Kehitystyön tavoitteena on toteuttaa ratkaisuja tunnistettuihin ongelmiin tai kehityskohteisiin. Kehityskohteet on valittu teknologisen kehityksen jatkuvuuden takaamiseksi, ja ne on tunnistettu organisaation sisäisesti tarpeellisiksi kohteiksi.

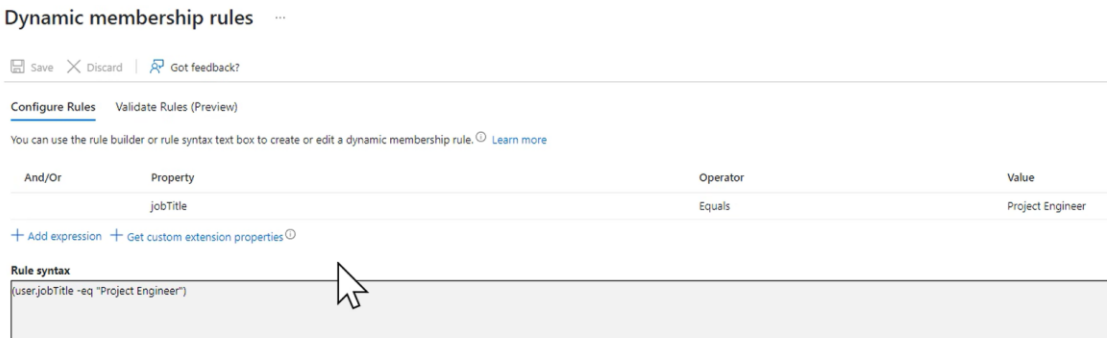
Kehitystyöt ja testit suoritetaan organisaation tileillä tällä hetkellä käytössä olevassa ympäristössä, mutta kuitenkin luoden testikappaleita vain ympäristöihin, ryhmiin tai käyttäjiin, jotka eivät ole kytköksissä organisaation käyttöversioon mitenkään. Näin vältytään tahattomilta katkoksilta tai muilta yrityksen prosessien häiriöiltä.

9.1 Kehityskohde Entra ID:n dynaamiset ryhmät

Tämä kohde valittiin otettavaksi kehitykseen työn aikana, koska se koetaan organisaatiossa suurimpana vaikuttavana tekijänä kohti parempaa riskienhallintaa, TISAX-vaatimuksia, tehokkuutta sekä jatkolaajenemiseen varautumista. Vaikka aikaisemmin totesimme TISAX-vaatimuksien täyttyvän, tämä kehityskohde on kuitenkin hyvä toteuttaa. Kokonaistoteutusta ei kuitenkaan tämän työn aikana tehdä, vaan teimme ryhmien dynaamiseksi vaihtamiseksi testejä, joiden avulla kokonaistoteutus havaitaan mahdolliseksi.

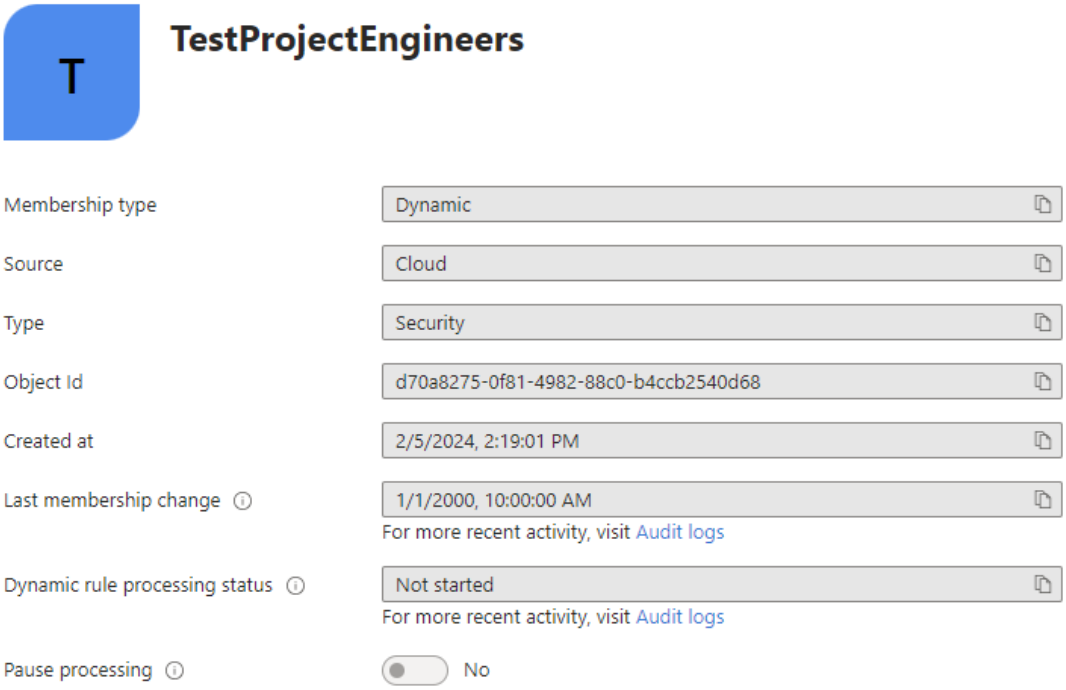
Ensimmäiseksi luotiin uusi Entra ID security -ryhmä, jolle annettiin ryhmän jäsenyystyypiksi dynaaminen. Dynaamisella jäsenyystyypillä mahdollistetaan ryhmään kuuluvien jäsenien automaattinen liittyminen ja poistuminen käyttäjän attribuuttien avulla. Jotta luotuun testiryhmään saadaan liitettyä käyttäjiä,

luotiin dynaamisia jäsenyyssääntöjä. Testiryhmään haluttiin projekti-insinöörejä, joten ensimmäiseksi säännöksi luotiin syntaksina ”jobTitle = Project Engineer”. Tämä sääntö luotiin graafisen käyttöliittymän kanssa, mutta sääntöjä on mahdollista luoda myös skripteinä tarjottuun tekstikenttään, kuten kuvasta 9 voidaan nähdä. Sääntöjä luotaessa tulee muistaa, että dynaamiseen ryhmään on mahdollista lisätä vain viisi sääntöriviä. Jos syntakseja halutaan lisätä useampia, on se tehtävä PowerShellin kautta sääntöjä yhdistellen.



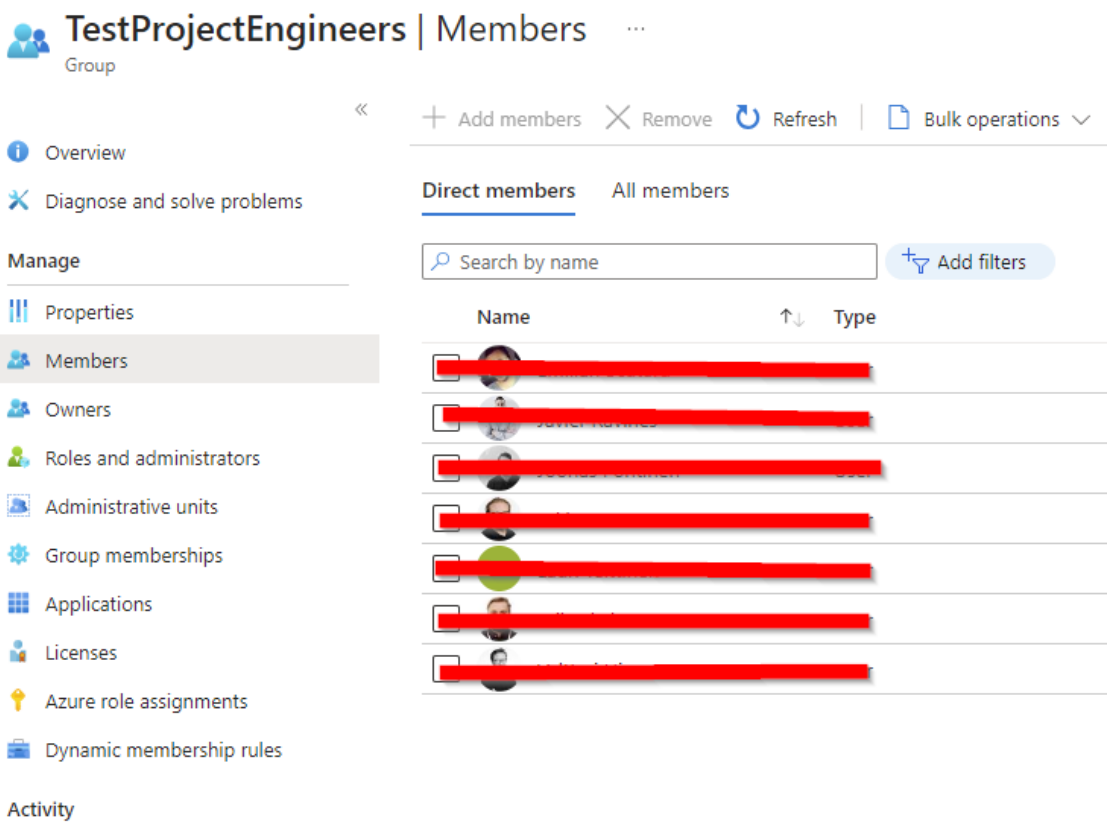
Kuva 9. Dynaamisen säännön luonti

Testien aikana huomattiin, etteivät käyttäjät päätyneet välittömästi uuden ryhmän jäseniksi. Tämän ilmiön luo Entra ID:n automatiikka, joka ei välittömästi käynnistä ryhmän syntaksien läpikäyntiä kaikilta käyttäjiltä. Uuden dynaamisen säännön luonnin jälkeen voi kestää tunteja, ennen ryhmään on automaattisesti lisääntynyt käyttäjiä sääntöjen perusteella. Tämä huomattiin myös ryhmän tiedoista, joissa kerrotaan dynaamisten sääntöjen prosessoinnin statuksesta, joka ei ollut käynnistynyt. (Kuva 10.)

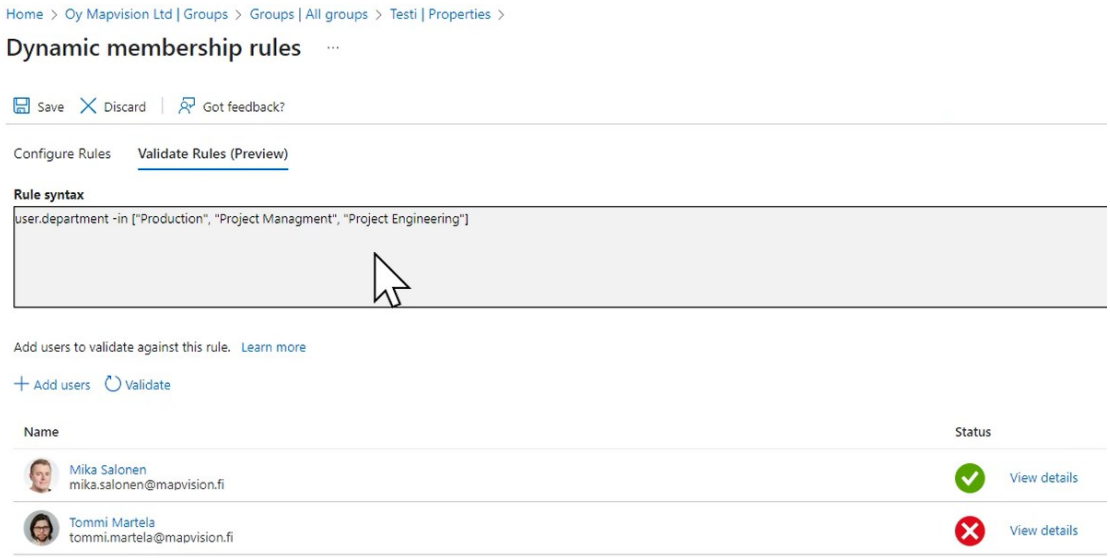


Kuva 10. Dynaamisen ryhmän informaatio välittömästi sääntöjen lisäämisen jälkeen

Syntaksin toimivuus varmistettiin tarkistamalla ryhmän jäsenet dynaamisen säännön prosessoimisen jälkeen. Huomattiin että ryhmään ovat ilmaantuneet kaikki käyttäjät, jotka vastaavat luotua sääntöä (Kuva 11). Tarkastelua voidaan myös tehdä sääntöjen luontihetkellä kohdasta ”Validate Rules (Preview)”. Täällä voidaan lisätä satunnaisia tai kohdennettuja käyttäjiä ja validoida se, olisivatko he luodun säännön perusteella ryhmän jäseniä (Kuva 12).



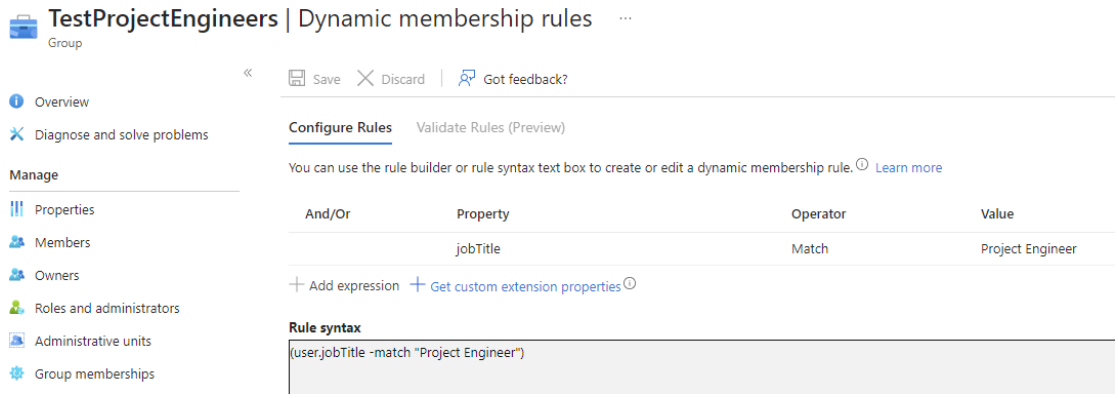
Kuva 11. Ryhmään tulleita käyttäjiä syntaksin perusteella



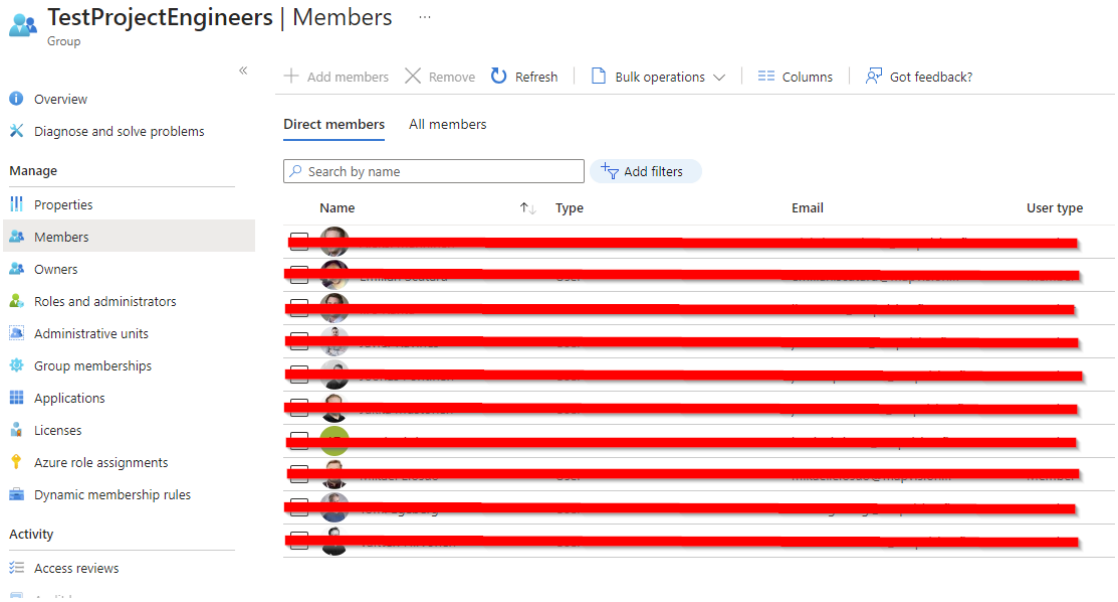
Kuva 12. Sääntöjen validointi

Seuraavaksi muutimme juuri luodun ryhmän sääntöä seuraavanlaiseksi: ”jobTitle Match Project Engineer”. Tämän syntaksin kanssa yritetään löytää kaikki sellaiset käyttäjät, joiden työnimikkeeseen sisältyy arvo ”Project Engineer” (Kuva 13). Näin pystymme testaamaan, tuleeko ryhmään käyttäjiä, joiden nimike on esimerkiksi ”Senior Project Engineer”. Kuvasta 14 huomataan, että myös tavoitellut käyttäjät, joilla on ”Project Engineer” työnimikkeessään,

olivat lisättyinä testiryhmään. Tämä todistaa, sen että ryhmän syntaksia voidaan myös muuttaa tarpeen tullen ryhmän luonnin jälkeenkin.



Kuva 13. Syntaksina "match"



Kuva 14. Uuden saapuneet käyttäjät uuden säännön myötä

Tämän kehityskohteen testit todetaan siis toimiviksi. Voidaan varmuudella todeta, että organisaation nykyisen käyttäjänhallinnan järjestelmällä voidaan luoda ja hallita dynaamisesti käyttäjiä omissa ryhmissään. Tämä avaa mahdollisuuden yksinkertaistaa huomattavasti roolipohjaisten käyttäjänhallinnan prosessia organisaation sisällä. On kuitenkin todettava, että tällä dynaamisella ryhmänhallinnalla ei voida operoida kaikkia käyttäjäoikeuksia, jolloin tarve yksittäisille manuaalisille oikeuksille on edelleen olemassa. Organisaation tulisi ottaa myös tarpeellinen huolellisuus huomioon jatkokehityksen aikana muuttaessaan olemassa olevia ryhmiä dynaamisiksi ryhmiksi, etenkin jos tätä työvaihetta yritetään automatisoida PowerShellin avulla.

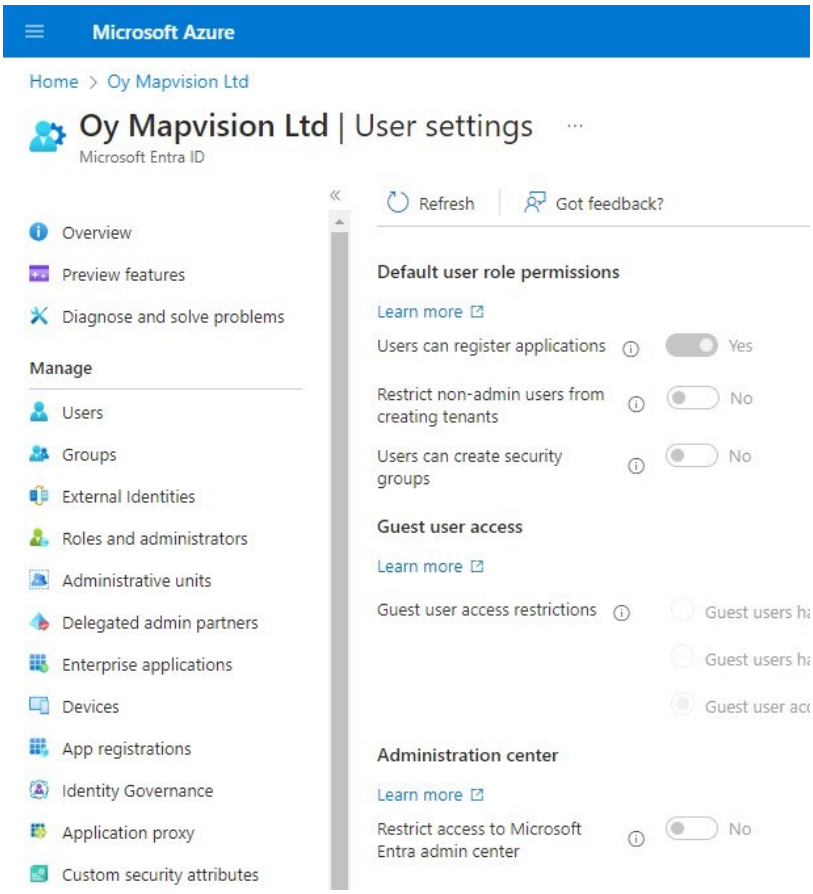
9.2 Kehityskohde Entra ID:n rajoittaminen

Tämä kehityskohde valittiin, koska tutkimuksen aikana huomattiin, että käyttäjillä on liikaa ominaisuuksia ja näkymiä tarjolla Entra ID -alustalla. Näiden rajoittaminen lisää organisaation tietoturvallisuutta, sekä vähentää väärinkäytöksen mahdollisuuksia normaaleilta käyttäjiltä. Zero Trust -politiikkaa voidaan pitää pohjana tässä kehityksen kohteessa.

Muokattavina olevat asetukset ovat:

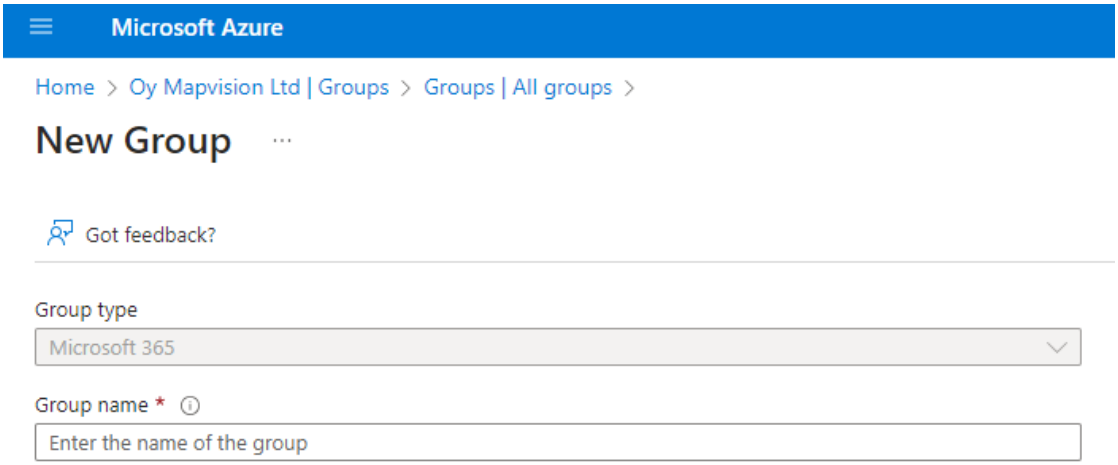
- Rajoita peruskäyttäjiä luomasta käyttäjäorganisaatioita
- Käyttäjät voivat luoda security-ryhmiä
- Rajoita pääsyä Microsoft Entra -hallintakeskukseen

Näiden kolmen kohdan asetukset löytyvät kaikki samasta käyttäjäasetusvalikosta. Kuten kuvasta 15 huomataan, organisaatiolla on nämä kaikki kolme asetusta rajoittamatta.

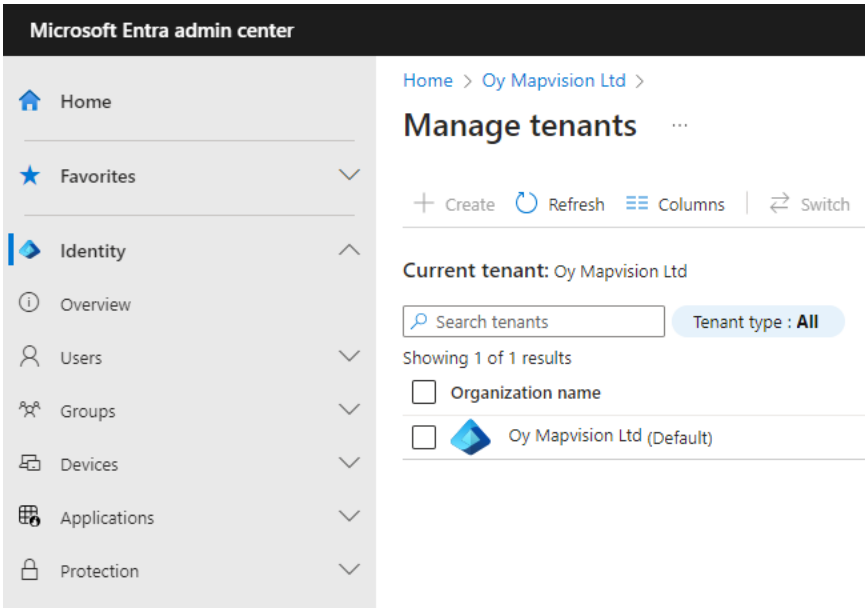


Kuva 15. Käyttäjäasetukset

Seuraavaksi muutetaan asetuksia niin, että kaksi ensimmäistä kohtaa vaiihdetaan asetukselle ”Yes”. Näin pääsemme normaalikäyttäjänä vielä testaamaan, että nämä muutokset tulivat toteen. Muutoksien jälkeen normaalikäyttäjän ei tulisi pystyä luomaan uusia käyttäjäorganisaatioita tai uusia security-ryhmiä.



Kuva 16. Uuden ryhmän luonti

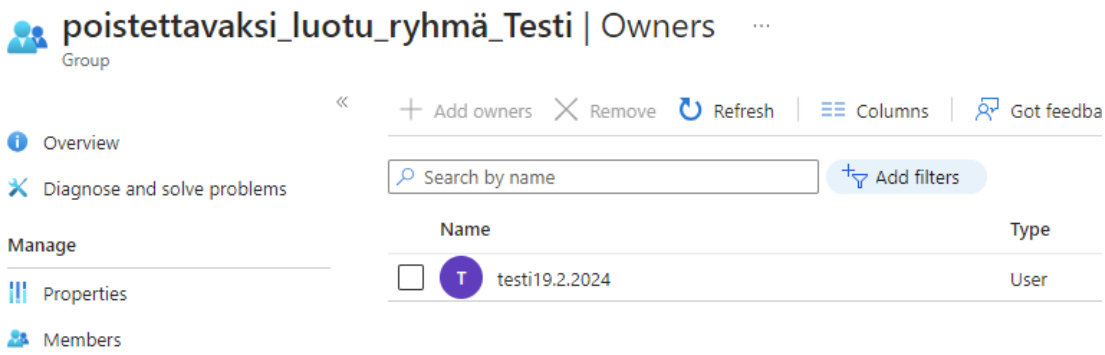


Kuva 17. Uuden käyttäjäorganisaation luonti

Kuten kuvista 16 ja 17 huomataan, uusien ryhmien lisääminen on rajattu vain Microsoft 365 -ryhmän luomiseen, ja käyttäjäorganisaatioiden luominen ei ole mahdollista asetuksien muutoksien jälkeen. Ryhmien luomisessa on järkevää pitää normaalikäyttäjällä oikeus luoda Microsoft 365 -ryhmiä, koska käyttäjät voivat tällöin edelleen vapaasti ilman lisäresursseja luoda uusia Teams -kanavia.

9.3 Kehityskohde Entra ID:n ryhmän omistajat

Tämä kehityskohde valittiin osakseen siksi, että tutkimuksen aikana huomattiin, että ryhmänomistajien käyttöoikeuksien avulla voidaan osakseen ohittaa organisaation oikeuksien lisäämisprosessin aikana tulevia hyväksyntäkierroksia. Tarkoitus on siis varmistaa testien avulla se, mitä tapahtuu, jos ryhmän käyttäjänä oleva omistaja poistetaan. Testin aikana lisätään uusi testikäyttäjä sekä uusi testiryhmä. Testikäyttäjä lisätään testiryhmän omistajaksi, ja testiryhmään käyttäjiä jäseniksi. Tämän jälkeen poistetaan testikäyttäjän tili, jotta nähdään mitä tapahtuu testiryhmän omistajuudelle. Kuvasta 18 nähdään testiryhmä, sekä testikäyttäjä omistajana.



Kuva 18. Testiryhmä, sekä testikäyttäjä

Testikäyttäjän poiston jälkeen huomattiin, ettei ryhmälle nimetä automaattisesti uutta omistajaa. Tällöin ryhmä jää ilman omistajaa sekä hallintamahdollisuutta lisätä uusia käyttäjiä tai omistajia. Peruskäyttäjille tai ryhmän käyttäjille ei siis jää oikeuksia lisätä uutta ryhmän omistajaa, tai mitään muitakaan oikeuksia. Globaalin järjestelmän ylläpitäjä tai muut ylläpitäjät voivat lisätä ryhmään lisää käyttäjiä tai omistajia. Omistajan poistuessa ryhmä ei siis jää ilman mahdollisuuksia muutoksiin.

Tämä kehityskohde todistaa sen, että ryhmän hallinta hankaloituu huomattavasti, jos ryhmän omistajakäyttäjä(t) poistetaan. Tällöin ryhmän muutosoikeus jää vain järjestelmäoikeuden hallitsijoille. Jos kuvailtu tilanne tulee vastaan, se luo ylimääräistä resurssien ja ajan käyttöä. Kuitenkin samalla huomattiin myös, että jos ryhmällä on omistaja, niin tämä omistajakäyttäjä voi lisätä uusia käyttäjiä ryhmään vapaasti ilman muiden hyväksyntää. Tämä tarkoittaa sitä, että organisaation käyttöoikeuksien lisäämisprosessissa käytetyt esihenkilöille

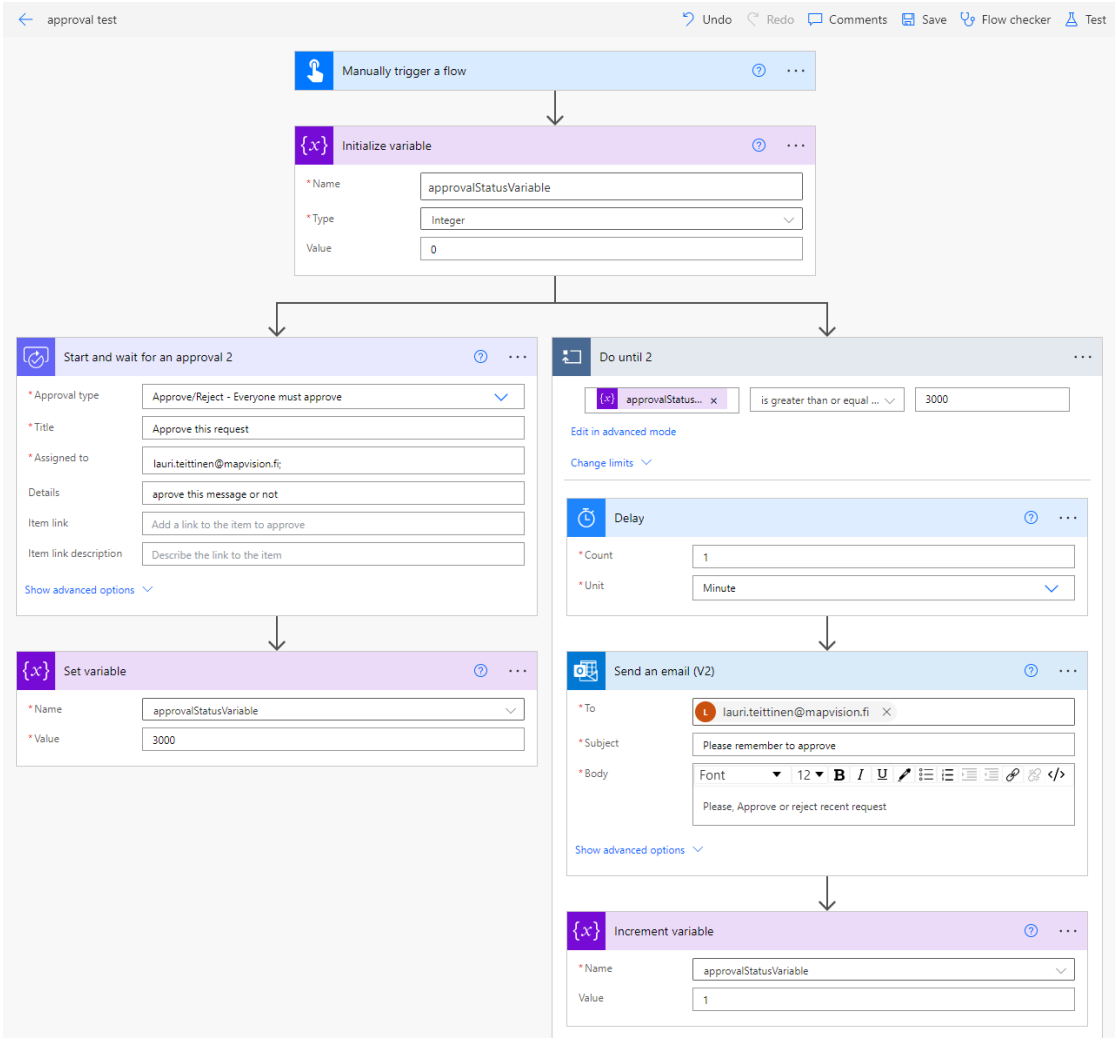
lähetettävät hyväksymispyynnöt ohitetaan kokonaan. Tämä mahdollistaa siis yksittäiselle käyttäjälle oikeuksien väärinkäytön. Yrityksen tulisikin jatkoarvioida se, tarvitseeko ryhmillä olla omistajia ollenkaan, koska omistajattomat ryhmät ovat myös mahdollisia. Toinen mahdollisuus on se, että ryhmissä itsessään rajoitetaan omistajien oikeuksia.

9.4 Kehityskohde poiston hyväksynnän vaatiminen

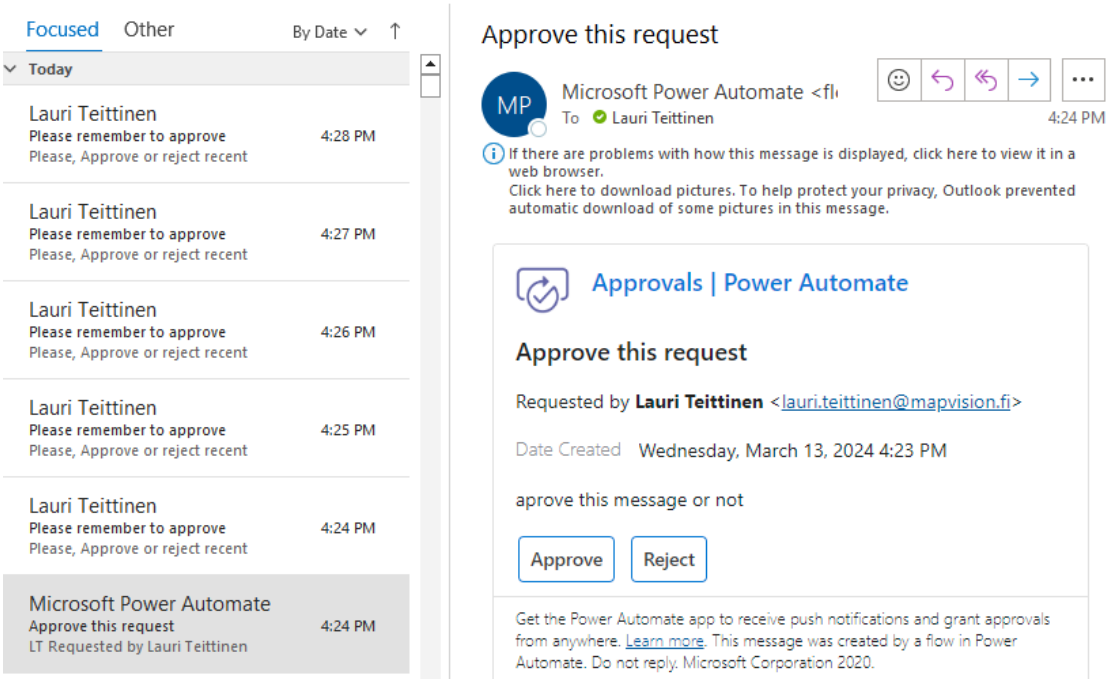
Tämä kohde valittiin kehitettäväksi, koska organisaatio tunnisti kohteen olevan tapahtumana todennäköinen sekä tietoturvan kannalta suuri riski. Käyttäjän poistoprosessin aikana on riski, että käyttäjän oikeuksien poistamisen hyväksyminen jää vastaamatta, jolloin taustalla toimiva PowerAutomate ei koskaan aja prosessia loppuun. Prosessissa käyttäjän oikeuksien poisto tapahtuu vasta hyväksyntäkierroksen jälkeen, jolloin vastaamatta jäänyt hyväksyntä jättää käyttäjäoikeudet henkilön käyttöön. Pahimmassa tapauksessa asia unohtuu kokonaan ja kommunikaatiokatkosten jälkeen yrityksen henkilöstö on väärässä uskossa, että organisaatiosta lähtevän henkilön oikeudet ovat poistettuja.

Prosessia haluttiin muuttaa niin, että PowerAutomate muistuttaisi hyväksyntäpyynnön saanutta henkilöä tietyn aikavälein sähköpostiviestillä. Testissä luotiin ensiksi PowerAutomateen uusi testiympäristö, johon voidaan ohjelmoida tarvittava muistutus käyttöoikeuksien poistamisesta. Tähän tarkoitukseen PowerAutomaten ”Do until” -toiminto sopii hyvin. Toiminnon avulla voimme lähettää sähköpostiviestejä asetetuin aikavälein halutulle käyttäjälle muistuttamaan hyväksyntäpyynnöstä.

Aluksi siis ohjelmoitiin kokonaislukumuuttuja lukuun 0. Tämä luku vaihtuisi lukuun 3000 vasta, kun hyväksyntä tai hylkäys olisi tehty. Jos hyväksyntää tai hylkäystä ei tehty, odottaisi prosessi halutun aikavälin ja lähettäisi sähköpostiviestin muistuttamaan hyväksyntäpyynnöstä. Tämän jälkeen lisätään yksi yksikkö lisää ja prosessi alkaisi jälleen alusta, kunnes vaaditut kriteerit täyttyvät. Testitapauksessa on otettu kokonaislukumuuttujaksi 3000 ja muistutuksien aikaväliksi 1 minuutti, kuten kuvasta 19 huomataan, mutta niitä voidaan halutun käytön mukaan muuttaa.

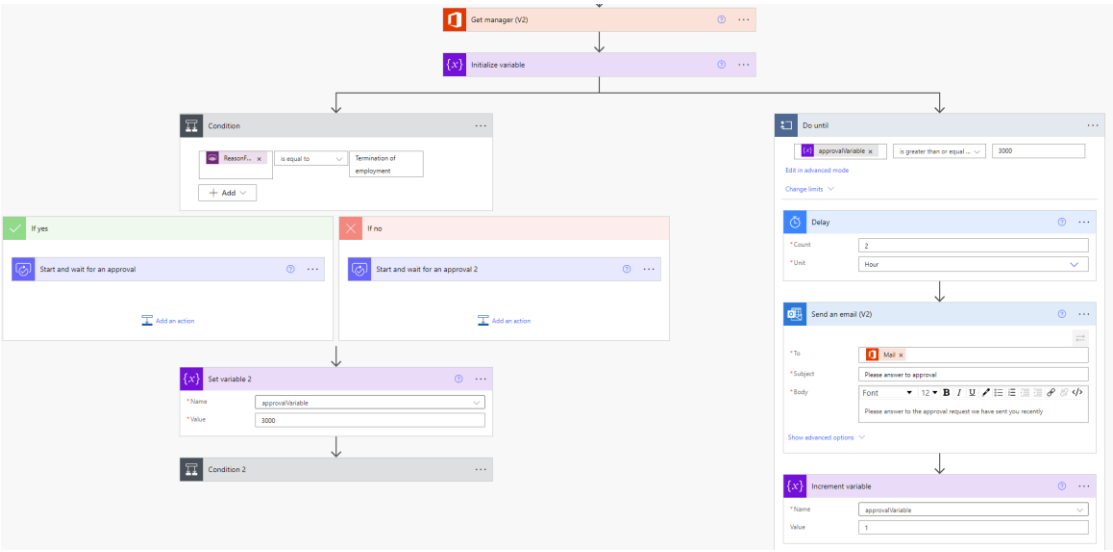


Kuva 19. Testiprosessin ohjelmointi



Kuva 20. Hyväksyntäpyyntöön vastaamisen muistutukset

PowerAutomate-testiskenaarion ajaminen tuottaa halutun ja odotetun tuloksen. Testiskenaariossa hyväksyntä lähetetään ja odotetaan vastausta, kunnes 3000 minuuttia on kulunut tai hyväksyntäpyyntöön on vastattu. Minuutin välein hyväksyjälle lähetetään sähköpostiviesti muistuttaen hyväksyntäpyynnön suorittamisesta loppuun. Kuvasta 20 huomataan, että hyväksyntäpyyntö on vastaanotettu sekä yhden minuutin välein saapuvat muistutusilmoitukset. Voidaan siis luottaa, että tämänkaltainen PowerAutomaten ohjelmointi toimii implementoituna nykyiseen järjestelmään.



Kuva 21. Hyväksyntämuistutus implementoituna nykyiseen ohjelmointiin

Kuvassa 21 testiohjelmointi on implementoituna nykyisen PowerAutomate-prosessiin. Ainoat muuttujat tässä ohjelmoinnissa on muistutusvälien aika sekä kenelle muistutus lähetetään. Aikavälinä toimii kaksi tuntia ja vastaanottaja muistuttajalle on aikaisemmin ohjelmoinnista haettu poistettavan käyttäjän esihenkilö.

Nykyiseen prosessiympäristöön lisättyä muistutusta testattiin testikäyttäjän poiston kanssa. Testauksen aikana todettiin, että muistutusviesti vastaanotettiin kuten oletettiin kahden tunnin välein ja kun alkuperäinen hyväksyntäpyyntö hyväksyttiin tai hylättiin, niin muistutusviestit loppuivat. Voidaan siis todeta, että tämä kehityskohde saatiin toimintaan myös tuotantoympäristössä.

10 TULOKSET JA YHTEENVETO

Kehittämistutkimustyön päätavoitteena oli selvittää, onko organisaation nykyisen roolipohjaisen käyttäjänhallinnan prosessi tarpeeksi hyvässä tilassa siihen, että TISAX-sertifiointiin vaadittu auditointi läpäistään hyväksytysti. Tutkimuskysymyksinä oli myös käyttäjänhallintaprosessin nykytilan selvittäminen, sekä mitä käyttäjänhallintaratkaisuja on valmiiksi tarjolla ja ovatko ne tarpeeksi kattavia. Asetetut tutkimuskysymykset tulivat tutkituiksi sekä vastatuiksi. Työn aikana selvitettyjen kehitysehdotuksien perusteella tehtiin kehitystyötä, mutta vain demotasolla. Konkreettinen kehitystyö käytössä olevaan ympäristöön jäi matalalle tasolle, mutta yrityksen prosessien ja kehityskohteiden herkkyyden vuoksi kehitystä ei ole järkevää pakottaa ilman tarpeeksi laajaa suunnitelmallisuutta.

Käyttäjänhallinnan nykytilan prosessi saatiin onnistuneesti tutkittua, dokumentoitua ja selvitettyä mahdollisien kehityskohteiden varalta. Selvitystyötä jouduttiin tekemään paljon, sillä aikaisempaa dokumentointia prosessista ei ollut. Selvitettiin myös, millaisia kokonaisratkaisuja käyttäjänhallintaan on tarjolla sekä onko niistä hyötyä yrityksen toiminnalle nykyhetkellä. Ratkaisujen kustannuksiin ei puututtu, jolloin hyötyjen vertailu jäi vain teknisen tarkastelun varaan. Tuloksina todettiin yrityksen tulevaisuuden varalta käyttäjänhallinnan lisäpalveluiden hankkimisen olevan järkevää.

Työn aikana kuitenkin havaittiin kehityskohteita ja tehtiin kehitysehdotuksia, joita yritys voi hyödyntää tulevaisuudessa tavoitellessaan entistä turvallisempaa ja sujuvampaa ratkaisua käyttäjänhallinnassaan. Työssä tehtyjen kehitystöiden pohjalta on hyvin vaivatonta parantaa yrityksen nykyistä prosessia sekä pohtia, miten muuten roolipohjaisen käyttäjänhallinnan toimintoja on mahdollista hyödyntää yrityksen tämän hetken tarpeiden ja vaatimusten mukaiseksi. Tietoturvan kannalta työn aikana annettiin kehitysehdotuksia sekä kehitettiin kohteita, jotka vähentävät mahdollisia väärinkäytöksiä puutteellisien suojauksien ja prosessien kautta.

TISAX-sertifikaatin kannalta tutkimuskehityksen aikana päädyttiin tulokseen, ettei muutoksia vaadita. TISAX-sertifikaatin käyttäjähallinnan ratkaisut täyttivät

vähimmäisvaatimukset. Tämä antaa kuvan siitä, että yrityksellä on tällä hetkellä käytössään tarpeeksi asianmukainen käyttäjänhallinnan ratkaisu. Tuloksissa päädyttiin myös toteamaan, että auditoinnin jälkeen on mahdollista saavuttaa jopa taso kaksi, eli ”requirements (should)”. Parempaan tulokseenkin on yrityksellä mahdollisuudet pienien toimintojen ja prosessien muokkaamisen jälkeen. Vaatimustasoista huolimatta on aina hyvä jatkaa kohti parempia tietoturvaratkaisuja kaikissa yrityksen aihealueissa, myös roolipohjaisessa käyttäjänhallinnassa. Opinnäytetyön loppuvaiheilla organisaatiolle suoritettiin TISAX-sertifikaatin vaatima auditointi ja tuloksena yritykselle myönnettiin TISAX-sertifikaatti. Tämä itsessään todistaa myös sen, että työn aikana arvioidut TISAX-tulokset olivat oikein.

11 POHDINTA JA JATKOEHDOTUKSET

Kehitystutkimustyön aikana kohdattiin paljon vastoinkäymisiä aikataulun kanssa. Suunnitelman mukaisesta aikataulusta jäätiin varhaisessa vaiheessa jälkeen. Alun perin asetettu aikataulutus työlle oli kuitenkin hyvin tiukka sekä vaativa, joten aikataussa pysyminen osoittautui entistä haastavammaksi. Alkuvaiheen aikatauluhaasteiden jälkeen työhön saatiin kuitenkin tarvittava panostus tahdissa pysymiseen, vaikkakin aikataulusta jäljessä. Tutkittavan prosessin analysoiminen ja ymmärtäminen alkuun vei paljon resursseja ja oli haasteellista. Selvittämistyötä hidasti myös järjestelmän laajuus ja monien eri sovelluksien toimintojen linkittyminen ja järjestäytyminen toisiinsa.

Kehityskohteiden pohdinta ja niiden toteuttaminen olivat suuri osa kehitystutkimusta. Tutkimuksessa havaittujen kehitystarpeiden valinta kehityskohteiksi osoittautui pulmalliseksi. Kehitysmuutoksien testaamiseen tuli suhtautua suurennetulla huolellisuudella, sillä kehityskohteen ympäristö oli samaan aikaan yrityksellä aktiivikäytössä. Kehitystesteihin valmistauduttiin suunnitelmilla, jotka oli laadittu tarpeellisen teorian taustatutkimusten jälkeen. Testit sujuivat odotetusti suunnitelmien mukaan sekä onnistuneesti. Testeissä ei kehitetty suuria mullistavia muutoksia, mutta todettiin kuitenkin, että teorioihin pohjautuvia kehitysehdotuksia on mahdollista käyttää tulevaisuudessa yrityksen lopullisessa käyttöympäristössä.

Työn kannalta on tärkeää pohtia, miten laadukas ja luotettava tehty tutkimus on. Tutkimukseen aineistoa kerättiin lähinnä aiheeseen liittyvien, verkossa olevien oppaiden sekä lähteiden kautta. Myös henkilöstön kautta opinnäytetyöpalavereissa sekä satunnaisten haastattelujen avulla on kerätty aineistoa. Kerättyä aineistoa kirjattiin havaintoina kenttäpöytäkirjaan. Nämä havainnot kuitenkin painottuvat opinnäytetyöpalaverien ja satunnaisten keskustelujen muistioksi. Tutkimuksessa aineiston keräyksen monimuotoisuus on siis vähäistä. Useammalla tavalla kerätty aineisto voisi syventää laatua, mutta pitää myös pohtia onko tämän tyylisessä tutkimuksessa tarpeellista laajentaa aineiston keräystä suuresti tai edes ollenkaan. Rajoituksina työssä huomattiin organisaation omat rajoitteet salassapidon kanssa.

Koska tehdyt kehitystyöt opinnäytetyön aikana olivat vain teoriakonseptien todisteita, jäi yrityksen järjestelmiin kehittämistarpeita. Tulevaisuuden kannalta organisaatiossa tulisi saattaa päätökseen työn aikana selvitettyjä kehityskohteita, mutta myös katsoa tulevaisuuden kannalta merkittäviä uusia kohteita. Yrityksen on hyvä varautua mahdollisiin henkilöstömäärän kasvuihin ja suunnitella roolipohjaista käyttäjänhallintaa laajemmalla näkökulmalla. Tällä hetkellä myös henkilöstöstä ei löydy tarpeeksi resursseja kehittämään käyttäjänhallintaa. IT-palvelut ovat yrityksessä kolmannen osapuolen hoitamia, mutta yrityksen henkilöstössä ei ole itsellään kuin yksi prosessia eteenpäin kehittävä henkilö.

Jatkotutkimusaiheena voisikin olla joitakin selvityksiä, miten laajentaa käyttäjänhallintaprosessi ja sen taustalla oleva organisointi tai henkilöstö yrityksen laajetessa moniin satoihin työntekijöihin. Myös kustannuskysymyksiä olisi hyvä tutkia, jotta yritys saisi selville mikä on taloudellisesti kannattavin ratkaisu nykyhetkellä, lähitulevaisuudessa sekä pitkän ajan tähtäimellä. Jatkoaiheina olisi myös hyvä tutkia, miten kolmansien osapuolien ratkaisut, kuten Netoxin tarjoamat palvelut voisivat mahdollisesti ulkoistaa täysin nykyisen ratkaisun, kustannukset tutkimukseen mukaan ottaen.

LÄHTEET

AdminDroid. 2024. Restrict User Access to Azure AD to Prevent Data Exposure. WWW-dokumentti. Saatavissa: https://blog.admindroid.com/restrict-user-access-to-azure-ad-to-prevent-data-exposure/ [viitattu 20.2.2024].

DNV AS. 2023. TISAX® - Autoteollisuuden tietoturva. WWW-dokumentti. Saatavissa: https://www.dnv.fi/services/tisax-r-autoteollisuuden-tietoturva-185873 [viitattu 25.9.2023].

ENX Association. 2023. TISAX Participant Handbook. PDF-dokumentti. Saatavissa: https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf [viitattu 6.2.2024].

ENX. 2023. Information security assessment. Excel-dokumentti. Saatavissa: https://portal.enx.com/isa5-en.xlsx [viitattu 01.11.2023].

ENX TISAX. 2023. About TISAX. WWW-dokumentti. Saatavissa: https://portal.enx.com/en-US/TISAX/ [viitattu 6.2.2024].

Fortinet. 2024. What Is An Attack Surface? WWW-dokumentti. Saatavissa: https://www.fortinet.com/resources/cyberglossary/attack-surface [viitattu 4.3.2024].

Imperva. 2023. Role-Based Access Control (RBAC). WWW-dokumentti. Saatavissa: https://www.imperva.com/learn/data-security/role-based-access-control-rbac/ [viitattu 01.10.2023].

Jyväskylän yliopisto Koppa. 2021. Tutkimuksen suunnittelu. WWW-dokumentti. Päivitetty 27.09.2021. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/tutkimusprosessi/tutkimuksen-suunnittelu#tutkimusongelmant-sment-minen [viitattu 27.11.2023].

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona: opas opinnäytetyön ja pro gradun kirjoittajalle. Suomen Yliopistopaino Oy – Juvenes Print. 2017 Jyväskylä: Jyväskylän Ammattikorkeakoulu.

Kauppalehti yrityshaku Oy Mapvision Ltd. 2023. WWW-dokumentti. Saatavissa: https://www.kauppalehti.fi/yritykset/yritys/oy+mapvision+ltd/0662033-1 [viitattu 30.11.2023].

Kyberturvallisuuskeskus. 2024. Collecting and using log data. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/collecting-and-using-log-data [viitattu 20.2.2024].

Mapvision Oy. 2023. Introduction to Mapvision. PDF-dokumentti. Intranet.

Mapvision Oy. 2024. PowerApps. PDF-dokumentti. Intranet.

Microsoft 365. 2024. Introduction to Microsoft Entra tenants. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/microsoft-365/education/deploy/intro-azure-active-directory [viitattu 19.2.2024].

Microsoft Azure. 2023. Azure AD is becoming Microsoft Entra ID. WWW-dokumentti. Saatavissa: https://azure.microsoft.com/en-us/updates/azure-ad-is-becoming-microsoft-entra-id/ [viitattu 01.10.2023].

Microsoft Azure. 2024. Review tenant creation permission in Azure Active Directory B2C. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/azure/active-directory-b2c/tenant-management-check-tenant-creation-permission [viitattu 19.2.2024].

Microsoft Entra. 2023. Dynamic Membership rules for groups in Microsoft Entra ID. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership [viitattu 16.1.2024].

Microsoft Entra. 2024. New Name for Azure Active Directory. WWW-dokumenti. Saatavissa: https://learn.microsoft.com/en-us/entra/fundamentals/new-name [viitattu 15.2.2024].

Microsoft Entra ID. 2023. What is Microsoft Entra ID. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whatis [viitattu 01.10.2023].

Microsoft Group types. 2024. Compare types of groups in Microsoft 365. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide [viitattu 15.1.2024].

Microsoft Groups. 2023. Groups in Microsoft 365 and Azure, and Which is Right for You. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/microsoft-365/community/all-about-groups [viitattu 01.10.2023].

Microsoft Lists. 2023. Introduction to lists. WWW-dokumentti. Saatavissa: https://support.microsoft.com/en-us/office/introduction-to-lists-0a1c3ace-def0-44af-b225-cfa8d92c52d7 [viitattu 01.10.2023].

Microsoft PIM. 2024. Plan a Privileged Identity Management deployment. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan [viitattu 17.1.2024].

Microsoft Power BI. 2023. What is Power BI. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/power-bi/fundamentals/power-bi-overview [viitattu 01.10.2023].

Microsoft PowerApps. 2023. Power Appsin kuvaus. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/fi-fi/power-apps/powerapps-overview [viitattu 01.10.2023].

Microsoft Security. 2024. Microsoft Entran palvelupaketit ja hinnoittelu. WWW-dokumentti. Saatavissa: https://www.microsoft.com/fi-fi/security/business/microsoft-entra-pricing [viitattu 15.1.2024].

Nanonets. 2024. How to Use Microsoft Power Automate Workflows in 2024. WWW-dokumentti. Saatavissa: https://nanonets.com/blog/microsoft-power-automate-tutorial-guide/ [viitattu 10.1.2024].

Netox. 2024. Tietoa meistä. WWW-dokumentti. Saatavissa: https://netox.fi/netox/ [viitattu 13.2.2024].

NIST. 1992. Role-Based Access Controls. PDF-dokumentti. Saatavissa: https://csrc.nist.gov/pubs/conference/1992/10/13/rolebased-access-controls/final [viitattu 15.10.2023].

NIST. 2016. Role Based Access Control. WWW-dokumentti. Päivitetty 22.6.2020. Saatavissa: https://csrc.nist.gov/Projects/Role-Based-Access-Control/faqs [viitattu 01.10.2023].

NIST. 2020a. Zero Trust Architecture. PDF-dokumentti. Saatavissa: https://csrc.nist.gov/pubs/sp/800/207/final [viitattu 12.1.2024].

NIST. 2020b. Security and Privacy Controls for Information Systems and Organizations. PDF-dokumentti. Saatavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [viitattu 4.3.2024].

Notion. 2023. Shaping better software: The benefits of effective code documentation. WWW-dokumentti. Saatavissa: https://www.notion.so/blog/code-documentation [viitattu 28.2.2024].

Okta. 2023. What Is Role-Based Access Control (RBAC)? WWW-dokumentti. Saatavissa: https://www.okta.com/identity-101/what-is-role-based-access-control-rbac/ [viitattu 02.10.2023].

OWASP. 2024. Multi-Factor Authentication Cheat Sheet. WWW-dokumentti. Saatavissa: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html [viitattu 14.2.2024].

Power Automate. 2024. Limits of automated, scheduled, and instant flows. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/power-automate/limits-and-config [viitattu 14.3.2024].

Sharepoint Maven. 2024. What is SharePoint, and what is it used for? WWW-dokumentti. Saatavissa: https://sharepointmaven.com/what-is-sharepoint-and-what-is-it-used-for/ [viitattu 15.1.2024].

Standards & economic growth. 2021. International Organization for Standardization. WWW-dokumentti. Saatavissa: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100456.pdf [viitattu 20.10.2023].

TechTarget. 2023. Role-based access control (RBAC). WWW-dokumentti. Saatavissa: https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC [viitattu 01.10.2023].

Kenttäpöytäkirja – Huomiot – Muistiinpanot

15.10.2023 - Opinnäytetyöpalaveri

Entra ID ja Azure AD nimenmuutos. Työhön lisätään Entra ID taustotus ja siihen, miten se liittyy Azure AD sekä muihin Azure toimintoihin.
Onkohan nykyistä prosessia dokumentoitu mihinkään että voisi ottaa siitä koppia.

24.10.2023 – Sähköpostikeskustelu

”

Moi,
Tuli mieleen, että me sovittiin viime keväänä, että aina, kun joku lähtee talosta, laitetaan tieto myös tälle jakelulistalle, jotta järjestelmien omistajat osaavat poistaa henkilön käyttäjälistoilta (TISAX-vaatimuskin). Tämä on varmaan unohtunut (?), mutta se on myös muuttumassa. *Henkilö-x* on tätä edistänyt, mutta toimiiko se jo? Mutta kunnes uusi tapa on käytössä, käytetään tätä. Jos se on jo käytössä, niin kertokaa mullekin.
Mutta siis, meillä pitäisi olla näyttöä TISAX-auditoinnissa, että me myös huolehdimme lähtevien poistamisesta järjestelmistä.

”

27.10.2023 - Opinnäytetyöpalaveri

Onko riskiä, jos käyttäjä näkee missä ryhmissä on oikeudet. Tai onko riskiä, jos näkee mihin ei ole oikeutta?
Käyttäjän poistuessa talosta, onko minkäänlaista varmistusprosessia että henkilön oikeudet on poistettu?
Nykyistä prosessia ei ole dokumentoitu missään. Kaikki tieto on siis käytännössä Lassella päässään.

28.10.2023 - Opinnäytetyöpalaveri

Onko olemassa yksittäishallintaoikeuksia – Vain yhdellä ihmisellä oikeuksia yms
Selvitetään miten powerapps eroaa taustalla toimivasta power automatesta

30.10.2023 - Opinnäytetyöpalaveri

Lokitietojen kerääminen kuka antanut mitäkin oikeuksia ja miten.
Kannattaako kirjata kaikki tiedot ylös tai mitkä tiedot ovat tarpeellisia tai välttämättömiä? Tämä on ehkä enemmänkin oma ”tutkimuksensa” tai Study tyyppinen. Voi perehtyä myöhemmin.

10.11.2023 - Opinnäytetyöpalaveri

Kun luo Teams ryhmän niin tulee automaattisest M365 ryhmä

Esim kun tekee uuden teams ryhmän, sille pitäisi saada jotenkin linkitetty group Eli kun käyttäjälle annetaan group oikeus, pitäisi käyttäjän myös liittyä sinne Teams ryhmään automaattisesti

Azuren ratkasut käyttäjänhallintaprosessiin

Selvitys näistä?

Kustannuspolitiikat?

Prosessin dokumentointi on järkevää, mutta onko automate prosessin ohjelmointiin järkeä tehdä kommentoinita? Onko se tietoturvallista?

14.11.2023 - Opinnäytetyöpalaveri

Listaominaisuus tutkittava: se on luojansa omaisuutta, poistuuko se, jos sen luoja lähtee talosta ja tunnus disabloidaan?
Listojen suurusluokka on valtava. Valtavasti hallitsemattomia asioita sekä tietämättömiä ryhmiä. Listojen päivitettävyys Entra ID ryhmien kanssa?
Entra ID ryhmiä 325 kpl. Aika paljon verrattuna Kuinka pieni yritys on kyseessä.

13.12.2023 – Keskustelu opinnäytetyön ohjaajan kanssa

Menetelmällisesti sisällön analyysi
Zero trust - Anna ainoastaan admin rooleja niille, jotka tarvii ja anna vain niitä rooleja. (Ei Global rooleja kellekään yms)
Onko ryhmien luontia rajoitettu vain tietyille henkilöille? (tuli mieleen m365 group luennan aikana)

15.1.2024 - Opinnäytetyöpalaveri

Selvitä mikä on PIM. Mitä se hyödyttää. Miksi se pitäisi olla / miks pitäis olla Premium P2? Vertaile P1 ja P2 malleja.

Nykysin käytössä jo Premium P1 käytössä. Netox haluaisi että otettaisiin P2.
P1 ei ole identiteetti manageria mitä Netox haluaa (PIM)
Jos me otettaisi P2, mitä etua saadaan PIM prosessista.
Flowssa on samoja ominaisuuksia kuin PIMmissä.
Vaikka otettaisiin P2, niin silti jouduttaisiin täydentämään prosesseja (Own-Clowd yms)
Tutkitaan hyvät ja huonot puolet P2 lisenssistä ja mitä tarpeellisia prosesseja yritykselle sillä ei saada.
Ensiviikoksi. PIM selvitys, Mitä eroja mitä hyötyjä ja mitä sillä ei voida hoitaa meidän prosessistamme.
Pitkän ajan ajattelu. Yksinkertaistaako P2 huomattavasti prosessia.

17.1.2024 – Henkilökohtainen havainto

Onko tosiaan niin, että jokainen M365 group on assigned eikä dynamic?
Jos käytetään dynamic niin käyttäjä siirtyy automaattisesti esim project engineers grouppiin kun luodulle käyttäjälle on annettu rooli project engineer.
Vaikka on mahdollinen ongelma että pelkkä project engineer oikeudet ei riitä yhdelle PE:lle ja oikeuksia pitäisi lisätä erikseen, Tämä on silti ”erittäin?” iso kehitysaskel?
Tähän liittyy tänään käyty project engineer team day missä Aleksi Manninen kovasti puhui taktiikoista ja niiden suunnasta. Aina ensimmäisenä: ”voiko sen poistaa?”, sitten vasta optimointi/tehtävän nopeutus.

18.1.2024 - Opinnäytetyöpalaveri

Määritetäänkö käyttäjänluonnin yhteydessä mitä kaikkea tietoja tarvitaan, että Entra ID pystyy tarpeeksi hyvin lisäämään henkilön kaikkiin ryhmiin.
PIM kannattaako hankkia.
Muista sisällyttää poistoprosessin ongelma käyttäjäoikeuksista. Koska havaittiin että myös ne oikeudet mitkä ei tule automaattisesti vaan on pääkäyttäjän takana on tässä poistoprosessi ongelmassa edelleen.

19.1.2024 - Opinnäytetyöpalaveri

Pitäisikö lisätä kappale miksi on päädytty nykyratkasuun?

Esim miksi ei otettu käyttöön normaalityyliä hallita rooleja Intra ID:n sisäisten dynaamisten hallintojen avulla?

22.1.2024 - Opinnäytetyöpalaveri

Kehitystyössä voisi tehdä testiympäristössä kehityksen, ei tarvitse organisaation live ympäristöä.
Ehdotukset konkreettisia prosessien muutoksia. Myös voi ehdottaa ”ehdotan tätä asiaa jatkotutkittavaksi”
Role list on ”tuntematon” ja pitkä

29.1.2024 - Opinnäytetyöpalaveri

Kehityksen tekeminen:
Demo testit. Voisi tehdä joitakin testiryhmiä, joihin lisättäisiin uusia testikäyttäjiä. Tässä samalla voitaisiin yrittää selvittää hyväksymispolkua ja miten se toimisi Entra ID dynaamisen ryhmän kanssa (koodaaminen pitäisi onnistua suoraan dynaamiseen ryhmään?).
Miten hoitaa tilanne jos esimerkiksi projekti insinööri ryhmään lisätään käyttäjä joka ei tarvitsekkaan kaikkia niitä projekti insinööriryhmiä.
Saadaanko Sympa dynaamiseks?
Pystyykö m365 groupin sähköpostin edelleen lähettää kaikille käyttäjille joilla se jakelulista on. Ongelma että se m365 ei lähetä käyttäjille vaan sille pelkälle sähköpostille, voisiko sen edelleen lähettää mail enabled tai distribution groupille
Näkyykö yksityiset ryhmät azuressa, esim Irtisanottavat ihmiset niminen ryhmä

02.02.2024 - Opinnäytetyöpalaveri

Pitäisikö Add user rights yms automateja commentoida että näkyy kunnolla mitä tapahtuu. Vai onko tämä turvallisuusriski

Käyttäjänlisäyskohta: Tähän kehitystarve: (Tiketti organisaation) automaattinen lisenssin myöntämisprosessi, joka aikaisemmassa versiossa oli, mutta tähän ei saatu vielä toimimaan - näin Netoxia ei tarvittaisi tässä kohti ollenkaan.

Kehityskohta käyttäjälle oikeuksien lisääminen: (Kehitysidea muistiin: prosessi ei tarkista, että pyyntöjä toteutetaan eli että manuaalisesti lisättävät asiat hoidetaan)

05.02.2024 - Opinnäytetyöpalaveri

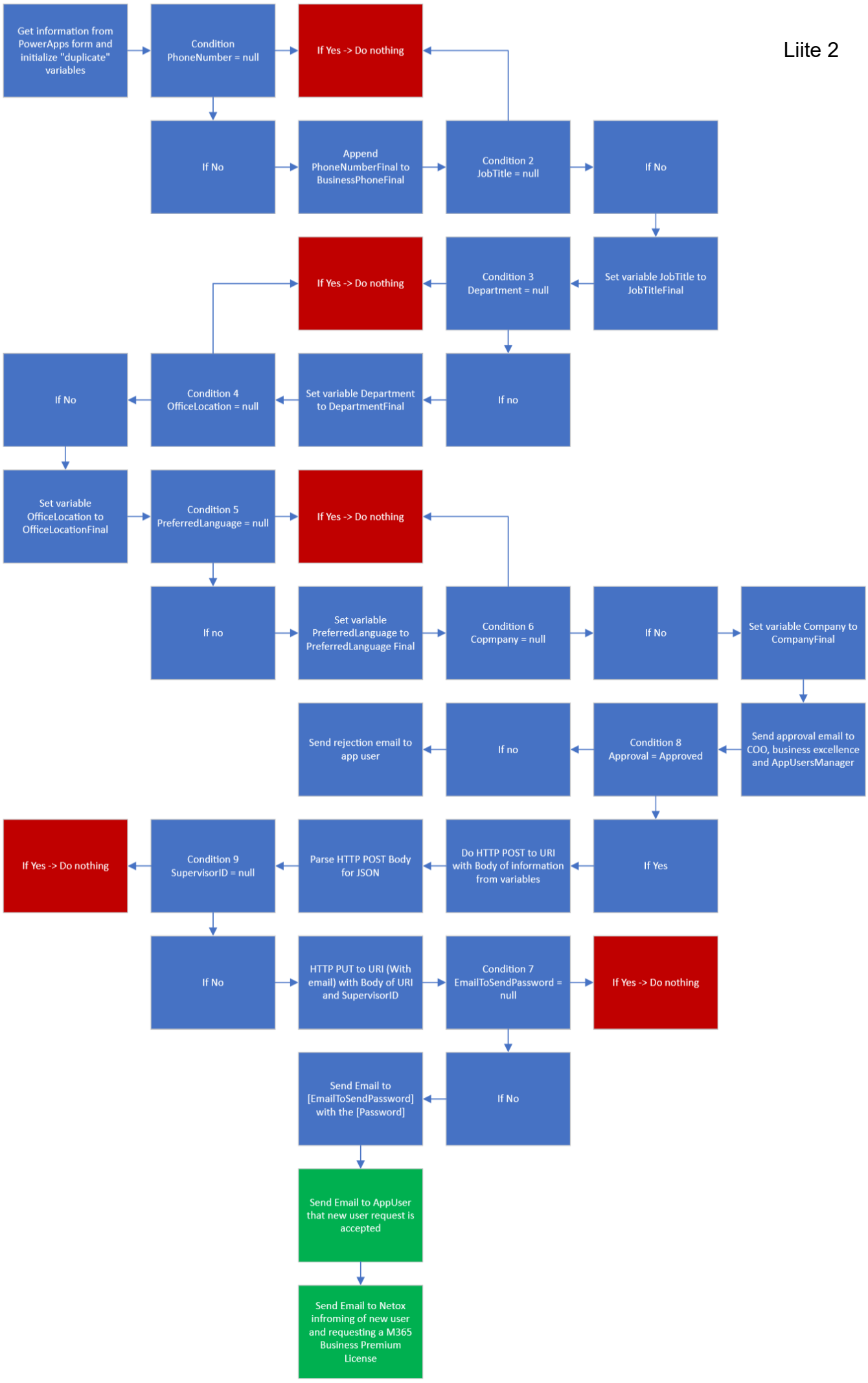
Microsoft Lists ei päivity automaattisesti muiden mukana

12.02.2024 - Opinnäytetyöpalaveri

Pitäisikö kehitystyönä olla: Ryhmien läpikäynti ja vaihdetaan siihen dynaaminen ryhmä
Olisiko hyvä että tittelin perusteella kaikki ryhmät vaihtoon.
Miten saataisiin sähköpostilistat toimimaan. Kehityskohde? Dynaaminen distribuution lista? Käyttäjäprofiili onlinen puolelle.
Jos kehitystyönä olisi listojen optimoiminen tai vähentäminen, niin jos saataisi dynaaminen sähköpostijakelulista, niin se auttaisi vähentää listoja ja sitä kautta olisi kehitystyö
Oisko kehityskohteena se, että muut ihmiset ei näkis mitään Entra ID tms
Jos on omistaja niin voi lisätä ryhmään ketävaan ja ketä omistajia vaan. Silloin ohitetaan esimieshyväksyntäinen prosessi käyttäjän lisäys

Create New User

Liite 2



Liite 3


Add Role Based Access Rights
Get information from PowerApps form
Change group names and process roles into array format (separate)
Initialize string for the new access right information
Make new array for Main Users list, Access Rights with main user list, and Access Rights per Main user list
Get app users manager info from AppUserID
Condition 6 [ProcessRoles =/= null] (There is something in the extra process roles box)
If yes
If no
Send acceptance email for manager to approve new access rights adding process
Condition 7 [AzureADgroupnames = null]
Send acceptance email for manager to approve process for requested groups and individual rights
If no
If yes
Pelkät prosessiroolit hyväksyntä manageri systmsen
First finds with group, then with single acces right inside role for next step
Condition 3 [Outcome of any = Approved]
If no -> Do nothing
If yes
Find selected process roles from SharePoint Lists
Condition 2 [If main user contains "@"] (If it is not a Azure automatic group)
If no
Check if user already is in Azure AD group with an empty function
If no -> Do nothing
If yes
Add user to Azure AD group
If Yes
For checking duplicates
If Yes -> Do nothing
Condition 12 [accessRightsMainUserList contains Title (from sharepoint)]
If Yes
Condition 8 [If mainUserList variable contains MainUserList (Sharepoint)]
If No
If No
Append to array variable [Title]
Append to array variable [accessRightsMainUserList]
Append to array variable [MainUserList]
Append to variable [Title]
If no
Condition 13 [newAccessRightsInformation contains Title (from sharepoint)
If yes -> Do nothing
Apply to each [AzureADGroupNames]
Get list items from sharepoint [Role based access rights]
Condition Above list contains "@"
If No
Check if user is in AzureAD Group
If not -> Add user to AzureAD Group
Single access right loop
If Yes
Condition 9 [MainUserList contains MainuserList(Sharepoint)]
If Yes
Condition 11 [accessRightsMainUserList variable contains Title (from sharepoint)]
If No
If No
If Yes -> Do nothing
Append Title to Array
If No
Condition 14 [newAccessRightsInformation contains Title(from sharepoint)]
Append MainUserList and Title to array
Append Title to variable
If yes -> Do nothing
Apply to each 6 [mainUserLists variable]
Apply to each 8 [accessRightsMainUserList]
Get list items from sharepoint [Role based access rights]
Apply to each 9 [Sharepoint value]
Condition 10 [MainUserList = Current item apply to each]
If No -> Do nothing
Set [accessRightsPerMainUserLists] variable to "null"
Send email to [current item apply each] requesting access for items [AccessRightsPerMainUserList]
Append Title to AccessRightsPerMainUserList
Using a loop to go through all mainusers to collect all rights and add rights to e-mail and send them to current mainuser
Send email to user that access to [newAccessRightsInformation] has been granted or will be granted