Mervi Kaijanen

Tehtävänimikkeisiin perustuvien pääsyoikeusprofiilien käyttöönotto

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

6.1.2024

Tiivistelmä

Tekijä:	Mervi Kaijanen
Otsikko:	Tehtävänimikkeisiin perustuvien käyttöoikeusprofiilien käyttöönotto
Sivumäärä:	24 sivua
Aika:	6.1.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ohjaaja:	TkL Kari Järvi

Yrityksessä havaittiin ongelma, joka liittyi uusien työntekijöiden tunnusten ja pääsyoikeuksien määrittelyyn sekä nykyisten työntekijöiden työnkuvan muuttuessa. Tämän seurauksena käynnistettiin projekti, jonka tavoitteena oli parantaa pääsyoikeuksien hallintaa.

Projektissa yrityksen käyttäjien pääsyoikeudet ja käyttäjätunnukset listattiin. Tämän tiedon perusteella määriteltiin kullekin kustannuspaikalle henkilöiden tehtävänimikkeisiin perustuvat pääsyoikeusprofiilit. Määritykset tehtiin yhteistyössä kunkin kustannuspaikan esihenkilöiden kanssa. Tämä mahdollisti pääsyoikeuksien määrittelyn tarkemmin ja joustavammin, mikä paransi tietoturvaa ja tehosti työprosesseja.

Uudet käyttöoikeusprofiilit otettiin käyttöön uusille yrityksen työntekijöille sekä tilanteissa, joissa henkilöiden työnkuva muuttui. Tämä varmisti, että jokaisella työntekijällä oli oikeat pääsyoikeudet heidän tehtäviensä mukaan, ja että pääsyoikeudet päivitettiin aina, kun työntekijän rooli yrityksessä muuttui.

Lisäksi yrityksen ServiceDeskille, joka hallinnoi käyttäjätunnuksia ja pääsyoikeuksia, laadittiin Excel-pohjainen työkalu. Tämä työkalu helpotti oikeuksien lisäämistä käyttäjälle, mikä teki pääsyoikeuksien hallinnasta tehokkaampaa ja vähensi virheitä.

Kaiken kaikkiaan tämä projekti paransi merkittävästi yrityksen kykyä hallita käyttäjätunnuksia ja pääsyoikeuksia, mikä tehosti toimintaa ja paransi tietoturvaa. Se myös osoitti, kuinka tärkeää on jatkuva pääsyoikeuksien hallinta ja päivitys yrityksen IT-infrastruktuurissa.

Avainsanat: Käyttäjähallinta, käyttöoikeus, profiili, tehtävänimike

Abstract

Author:	Mervi Kaijanen
Title:	Enabling security access profiles based on job titles
Number of Pages:	24 pages
Date:	6 January 2024
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Instructor:	Kari Järvi, Lic. Sc.

The company encountered a problem related to the definition of necessary credentials and access rights when new employees started and when the job description of existing employees changed. As a result, a project was initiated with the aim of improving access rights management.

In the project, the access rights and user IDs of the company's users were listed. Based on this information, access right profiles based on the job titles of individuals were defined for each cost center. These definitions were made in collaboration with the supervisors of each cost center. This allowed for more precise and flexible definition of access rights, which improved security and streamlined work processes.

The new access right profiles were implemented for new employees of the company as well as in situations where the job description of individuals changed. This ensured that each employee had the correct access rights according to their tasks, and that access rights were always updated when an employee's role in the company changed.

In addition, an Excel-based tool was created for the company's ServiceDesk, which manages user IDs and access rights. This tool facilitated the addition of rights to the user, making access rights management more efficient and reducing errors.

Overall, this project significantly improved the company's ability to manage user IDs and access rights, streamlining operations and improving security. It also demonstrated the importance of continuous access rights management and updates in the company's IT infrastructure.

Keywords: User management, access rights, user profile, job title

Lyhenteet ja käsitteet

AccessRegister:
Yritykselle kehitetty sovellus yrityksen palveluita käyttävien henkilöiden pääsyoikeuksien tallentamiseen. Otettu käyttöön GDPR-asetuksen käyttöönoton myötä vuonna 2018.

Active Directory (AD):
Aktiivihakemisto, Microsoftin kehittämä Windows-verkoissa käytettävä hakemistopalvelu. AD:n päätehtävä on todentaa ja valtuuttaa Windows-verkon käyttäjät ja tietokoneet sekä määrittää ja valvoa turvallisuuskäytäntöjä.

Citrix:
Citrix tarjoaa erilaisia virtuaalisointi- ja pilvipalveluratkaisuja yrityksille. Citrixin avulla voidaan monipuolisesti hallita, virtualisoida ja toimittaa sovelluksia ja tietoja.

Excel:
Taulukkolaskentaohjelma, joka on osa Microsoft Office -tuotesarjaa.

Extranet:
Organisaation hallinnoima osa tietoverkkoa, joka mahdollistaa organisaation turvallisen palveluiden käytön esim. kumppaneille ja määrätyille asiakkaille.

General Data Protection Regulation (GDPR):
EU:n tietosuoja-asetus, joka tuli voimaan toukokuussa 2018. Asetuksella määritellään, miten henkilötietoja saadaan kerätä ja käsitellä. [5.]

Human Resources (HR):
Yrityksessä henkilöasioita käsittelevä yksikkö.

Identity Access Management (IAM):
Henkilötunnistus- ja pääsynhallintajärjestelmä, jonka avulla varmistetaan, että oikeat henkilöt pääsevät oikeisiin resursseihin oikeaan aikaan.

Intranet:
Organisaation sisäinen tietoverkko, johon pääsy on vain tietyillä henkilöillä.

Kustannuspaikka:
Yrityksen sisäinen toiminnallinen yksikkö. Kustannuspaikkojen avulla yrityksessä voidaan tarkastella erilaisten resurssien käyttöä ja esim. kustannusrakenteita.

Organization Unit (OU):
Organisaatioyksikkö, Active Directoryn osa, jota käytetään eri kohteiden (käyttäjät sekä tietokoneet) ryhmittelyyn ja luokitteluun.

Pdf:
Portable Document Format, Adoben kehittämä tiedostomuoto, jota käytetään yleisesti asiakirjojen tallennusmuotona, jota voidaan tarkastella useilla laitealustoilla.

Pääsyoikeusprofiili:
Tämän yrityksen tapauksessa kullekin tiimille nykyisten käyttäjien pääsyoikeuksista laaditut määrittelyt siitä, millaisia käyttäjätunnuksia ja pääsyoikeuksia uusille vastaavalla tehtävänimikkeellä tuleville henkilöille luodaan.

Security group:
Tietoturvaryhmä, Active Directoryn sisällä oleva ryhmä. Ryhmälle voidaan luvittaa esim. sovellukseen kirjautumisoikeuksia. Ryhmään voi kuulua käyttäjiä, tietokoneita tai toisia ryhmiä.

ServiceDesk:
Palvelupiste, yrityksen sisäinen tiimi, joka hallinnoi käyttäjätunnuksia sekä pääsyoikeuksia. Lisäksi tiimi vastaa yrityksen työasematuesta ja käyttäjätuesta.

SharePoint:
Microsoftin kehittämä ja ylläpitämä yhteistyö- ja sisällönhallintajärjestelmä, joka mahdollistaa organisaation jäsenten yhteistyön, tiedonjakamisen ja dokumenttien hallinnan.

Single-Sign-On (SSO):
Yhteiskirjautuminen, sovellukselle määritelty kirjautumistapa. SSO:n käytössä ollessa ei sovellukselle luoda erillistä käyttäjätunnusta, vaan tunnistautumiseen käytetään esim. Windowsin käyttäjätunnusta.

Teams:
Viestintä- ja yhteistyöalusta, joka mahdollistaa organisaation jäsenten välisen tiimityöskentelyn, keskustelun, tiedonjaon ja projektinhallinnan reaaliaikaisesti verkossa.

Ticket:
Tiketti, palvelupyyntö tai häiriöilmoitus, joka on tallennettu ServiceDeskin seurantajärjestelmään.

Tiimi:
Ryhmä yksilöitä, jotka työskentelevät yhdessä tavoitteen tai tehtävän saavuttamiseksi.

Web-lomake:
Verkkolomake, digitaalinen lomake, joka täytetään ja lähetetään verkon kautta.

Sisällys

1 Johdanto

Tämän projektin tavoitteena oli yhtenäistää kunkin yksikön sisällä samaa tehtävää tekevien henkilöiden pääsyoikeudet ja ottaa käyttöön työnimikkeisiin perustuvat käyttöoikeusprofiilit. Lisäksi haluttiin helpottaa esihenkilöiden työtä, kun yksikköön tulee uusia henkilöitä joko uusina työntekijöinä tai siirtyy talon sisällä. Kun käytössä ovat työnimikkeisiin perustuvat pääsyprofiilit, kaikilla on tieto millaisia oikeuksia missäkin tehtävässä pitäisi olla. Esihenkilön ei tarvitse määritellä muuta kuin käytettävä profiili, ja käyttäjätunnuksia sekä pääsyoikeuksia hallinnoiva sisäinen ServiceDesk tietää ko. yksikön dokumentaation perusteella, mitä käyttäjätunnuksia käyttäjätunnukselle luodaan sekä millaisia pääsyoikeuksia tunnuksiin luvitetaan.

1.1 Yritys

Yritys toimii tukkukaupan alalla erittäin tiukasti säännellyllä ja valvotulla alalla. Tietoturvasyistä yritystä ei nimetä tarkemmin, vaan käytetään geneeristä nimitystä Yritys. Myös toimialaa ei tässä tarkenneta sen pidemmälle.

Yritys on osa eurooppalaista konsernia. Konserniin kuuluu toimintoja 29 maassa (joulukuu 2023). Suomessa Yrityksellä on kaksi toimipistettä; pääkonttoritoiminnot ja varastotoimintaa Vantaalla ja pääosin keskusvarastotoimintoja, mutta myös toimistohenkilöstöä sekä asiakaspalvelu Tampereella. Kaikkiaan Yrityksellä on n. 500 työntekijää, joista noin puolet toimisto/esihenkilötehtävissä ja puolet varastotehtävissä. Henkilöstöstä niin ikään puolet toimii Vantaalla ja puolet Tampereella. [6.]

2 Alkutilanne

Yrityksellä on käytössä kaikkiaan yli 120 erilaista järjestelmää, joista osaan kirjautuminen tapahtuu erillisellä käyttäjätunnuksella. Yhä kasvavaan määrään on jo määritelty Single-Sign-On (SSO), jossa käyttäjä tunnistetaan sen perusteella, millä käyttäjätunnuksella hän on kirjautunut tietokoneelle. Näihin järjestelmiin pääsyoikeudet määritellään Active Directoryyn (jatkossa AD) luotavien security-ryhmien avulla.

Käyttäjien pääsyhallinta on Yrityksessä Suomen osalta keskitetty Yrityksen sisäiseen ServiceDeskiin, jossa 6 henkilön asiantuntijatiimi luo käsin uudet käyttäjätunnukset ja pääsyoikeudet Yrityksen työntekijöille. ServiceDesk hoitaa myös tarvittavat muutokset sekä käyttäjätunnusten ja pääsyoikeuksien poistot eri järjestelmien prosessien mukaisesti. [6.]

Yrityksen käyttäjähallinta toteutetaan pääosin koko konsernin kattavan Windows AD:n kautta. Kaikille konsernin maille ja niiden eri toimipisteille on luotu omat Organization Unitit (OU), joiden avulla pääsyoikeuksia ja niiden hallintaa voidaan rajoittaa sekä pääsyoikeuksien että myös ylläpidon osalta. Ns. extranet-sovellusten osalta käytetään tähän dedikoitua AD-ympäristöä. Tässä ympäristössä hallinnoidaan myös Yrityksen asiakkaiden ja kumppaneiden pääsyoikeuksia Yrityksen tarjoamiin palveluihin. [1, 6.]

Suomen osalta eri käyttäjien pääsyoikeuksista pidetään manuaalista kirjanpitoa ko. tarkoitusta varten luodussa AccessRegister -sovelluksessa mm. GDPR-säännösten edellyttämänä. GDPR tulee sanoista General Data Protection Regulation (yleinen tietosuoja-asetus). Se on henkilötietojen käsittelyä sääntelevä laki, jota alettiin soveltaa kaikissa EU-maissa keväällä 2018. Asetuksen myötä rekisteröidyllä on oikeus mm. tarkistaa hänestä tallennetut tiedot. Organisaatiolla puolestaan on velvollisuus poistaa rekisteröidyn tiedot, mikäli organisaatiolla ei ole laillisia perusteita käsitellä niitä. Laillinen peruste voi olla esimerkiksi rekisteröidyn suostumus, sopimus tai lakisääteinen velvoite. [4, 6.]

Yrityksen prosessin mukaisesti kaikkien pääsyhallintapyyntöjen pitää tulla Yrityksen sisäisen ServiceDeskin kautta, jolloin kirjanpito on hallittua ja pyynnöt pystytään rajaamaan vain määrätyille henkilöille. Automaattista pääsynhallintajärjestelmää (IAM) ei ole käytössä. Kaikkien pääsynhallinnan pyyntöjen pitää tulla ServiceDeskille esihenkilön kautta, ja näistä tehdään palvelupyynnöt Yrityksen tikettijärjestelmään. Käyttäjät eivät voi itse pyytää itselleen pääsyoikeuksia tai oikeuksien muutoksia. Tikettijärjestelmässä palvelupyynnöt ovat dokumentoituna ja niihin voidaan auditointien yhteydessä tarvittaessa palata.

Joihinkin järjestelmiin luodaan myös erillisiä käyttäjätunnuksia suoraan järjestelmään. Myös näiden tunnusten hallinta tapahtuu ServiceDeskissä saman yrityksessä sovitun ja hyväksytyn prosessin käyttövaltuusprosessin mukaisesti kuin Windows AD-tunnustenkin ylläpito

Eri yksiköitten/kustannuspaikkojen esihenkilöt määrittelevät itsenäisesti kaikille työntekijöille tarvittavat pääsyoikeudet ja niiden laajuuden. Periaatteena on, että kullekin henkilölle tulee vain sellaiset oikeudet, joilla hän pystyy toimimaan sujuvasti hänelle määritellyissä tehtävissä. ServiceDesk toimii hyvin usein apuna tarvittavien oikeuksien määrittelyssä käyttäen apuna muiden vastaavissa tehtävissä toimivien henkilöiden oikeuksien listauksia.

Esihenkilöillä on usein hankaluuksia tietää, mihin kaikkiin järjestelmiin ja sovelluksiin pääsyoikeuksia tarvitaan esim. uuden henkilön aloittaessa tai työtehtävien muuttuessa. Hyvin yleinen tapa määritellä oikeuksia on kopioida pääsyoikeudet joltain vastaavissa tehtävissä toimivalta kollegalta.

Yrityksessä kannustetaan henkilöstöä kehittämään itseään eri tavoilla; yksi suosittu tapa on osallistua työnkiertoon. Tällöin jonkun yksikön henkilö siirtyy määräajaksi tai esim. vanhempainvapaan sijaiseksi toiseen yksikköön tutustumaan heidän työtehtäviinsä ja työtapoihin. Uusien työtehtävien myötä myös uusia pääsyoikeuksia pitää määritellä, ja usein se tehdään pyynnöllä ”lisää samat oikeudet mitä X.X.:llä, mutta älä poista vanhoja oikeuksia, kun hän tarvitsee niitäkin”. Sitten kun henkilö taas palautuu omaan yksikköönsä, ei lisättyjä oikeuksia

kuitenkaan pyydetä poistamaan. Tällöin henkilölle jää ylimääräisiä oikeuksia, joita saatetaan jopa monistaa eteenpäin.

Yrityksen henkilöstöhallinnan sovellus mahdollistaa vapaamuotoisten työnimikkeiden käytön. Tästä aiheutuu melkoisen kirjava nimeämiskäytäntö. Jopa yhden kustannuspaikan sisällä saattaa olla samaa tarkoittavia mutta hienoisilla kirjoitusasujen eroilla olevia työnimikkeitä.

Kun uusi henkilö tulee Yritykseen, joko esihenkilö tai HR-asiantuntija syöttää henkilön perustiedot sekä tiedot hänen työsuhteestaan HR-järjestelmään. Järjestelmästä lähtee automaattisesti ServiceDeskille ns. aloitusilmoitus, joka sisältää seuraavat tiedot:

- henkilön nimi
- työsuhteen alkamispäivä
- yrityksen henkilönumero
- tehtävänimike
- esihenkilö
- kustannuspaikka
- toimipaikka.

Tämän aloitusilmoituksen perusteella ServiceDesk aloittaa ns. perustunnuksen luomisen. Perustunnuksella Yrityksen käyttäjät pääsevät kirjautumaan Yrityksen lähiverkkoon, sekä saavat käyttöönsä Yrityksen palveluita, esim. sähköpostilaatikon, yleisiä verkkohakemistoja sekä tallennushakemiston henkilökohtaisille tiedostoille.

Tämän jälkeen esihenkilö tekee erillisen tunnustilauksen käyttäen Yrityksen itse suunnittelemaa web-lomaketta. Lomakkeella määritellään mihin eri järjestelmiin ja tarvittaessa minkä tasoisia oikeuksia henkilölle halutaan, millainen puhelinliittymä hänelle avataan ja mitä tiimikohtaisia kansio- ja sähköpostioikeuksia tarvitaan.

3 Profiilien luonti

Jo pitkään oli tiedostettu sekä ServiceDeskissä että myös esihenkilöiden taholla, että varsinkin uusille henkilöille tarvittavien pääsyoikeuksien määrittely on esihenkilöille erittäin haasteellista. Varsinkin sellaisissa tiimeissä, joissa henkilöstön vaihtuvuus on suhteellisen pientä, ei kaikkia oikeuksia huomata pyytää heti aloitusvaiheessa. Puuttuvia oikeuksia pyydetään sitten yksi kerrallaan ja oikeuksia joudutaan sitten odottelemaan, joskus jopa useita päiviä riippuen siitä joudutaanko tunnuksia ja oikeuksia pyytämään kolmannelta osapuolelta. Lisäksi kun pääsyoikeuksia pyydetään yksitellen, se myös työllistää ServiceDeskiä aivan turhaan, kun tarvittavat oikeudet voitaisiin kaikki luoda yhdellä kertaa.

Lähdin pohtimaan ongelmaa ensin oman työparini kanssa, ja otimme lähtöajatukseksi jo Yrityksen toiminnanohjausjärjestelmässä käytössä olevan rooliajattelun. Siellä eri tasoisille tehtäville on määritelty erilaisia sovelluskokonaisuuksia, joita on helppo hallita uusien käyttäjien määrittelyssä tai työtehtävien vaihtuessa. Mietimme mikä voisi olla sopiva yhdistävä tekijä, jota voitaisiin käyttää pääsyoikeuksien hallinnassa. HR-järjestelmässä ovat tallennettuna Laatujärjestelmän tarpeisiin suunnitellut vastuutoiminnot -määritykset. Näistä ei kuitenkaan meille ole sinällään apua, koska vastuutoiminnot monesti kattavat liian erilaisia tehtäviä, joihin pitää pystyä kuitenkin eriyttämään eri järjestelmien pääsyoikeuksia. Määrittelimme sitten, että yhdistävänä tekijänä käytettäisiin tehtävänimikkeitä kustannuspaikoittain. Tällä saadaan eroteltua eri tiimien hieman eroavat pääsyoikeudet, vaikka tehtävänimike olisikin sama.

Esittelimme tätä ajatusta ensin omalle esihenkilöllemme, ja lisäksi muutamalle liiketoimintayksikön esihenkilölle. Saimme muutamia rakentavia lisäehdotuksia ja -toiveita, mutta palaute oli erittäin myönteistä. Totesimme myös, että tässä alkuvaiheessa rakennetaan vain uusien henkilöiden tai tehtäviä vaihtavien henkilöiden pääsyoikeusprofiilit. Olemassa oleviin pääsyoikeuksiin ei tässä yhteydessä otettaisi kantaa, koska heillä on nykyisiin tehtäviinsä riittävät pääsyoikeudet.

3.1 Perusprofiilien luonti

Heti projektin varhaisessa vaiheessa huomattiin, että Yritykselle tarvitaan ns. perusprofiili. Tämä profiili voidaan luvittaa käyttäjälle heti HR-järjestelmän ServiceDeskille lähettämän aloitusilmoituksen perusteella. Todettiin myös, että tällainen perusprofiili pitää saada käyttöön nopeasti, ja se päätettiin luoda tehtävänimikkeisiin perustuvien profiilien lisäksi ja niitä ennen.

Perusprofiililla luvitetaan seuraavat peruspalvelut, jotka tulevat aivan kaikille Yrityksen käyttäjälle riippumatta millaisiin tehtäviin hän tulee:

- Windows-tunnus (ns. perustunnus)
- sähköpostilaatikko
- yrityksen oppimisympäristön oikeudet
- laatujärjestelmän lukuoikeudet
- yrityksen/konsernin viestintäkanavan oikeudet
- henkilön toimipaikan (Vantaa tai Tampere) mukainen sähköpostin jakelulista.

Lisäksi määriteltiin, mitä lisäoikeuksia tarvitaan toimistotehtävissä sekä varaston perustoiminnoissa.

Henkilön tullessa työskentelemään toimistoon, hänen perustunnukseensa lisätään seuraavat ns. toimistohenkilöstön käyttäjätunnukset ja järjestelmäpääsyt:

- ulkoisen extranet-palveluportaalin käyttäjätunnus perusoikeuksilla
- mahdollisuus tehdä etätöitä
- konsernin koulutusympäristön oikeudet
- oikeudet erilaisiin tiimityöskentelyyn tarvittaviin sovelluksiin.

Kun henkilö tulee työskentelemään varastoon, hänelle luodaan perustunnuksen lisäksi varaston keräilytehtävissä tarvittavat käyttöoikeudet.

3.2 Tiimikohtaisten tehtävänimikkeisiin perustuvien profiilien luonti

Kun perusprofiilit olivat valmiit ja otettu käyttöön, aloitettiin kustannuspaikkakohtaisten profiilien laatiminen.

Yrityksen kustannuspaikoista laadittiin listaus, ja ne laitettiin käsittelyjärjestykseen. Ensimmäisessä vaiheessa otettiin käsittelyyn varaston kustannuspaikat, joissa on paljon henkilöstöä samankaltaisissa tehtävissä. Varaston kustannuspaikoilla on myös henkilöstön vaihtuvuus kaikkein suurinta. Seuraavina käsiteltiin sitten liiketoiminnan eri yksiköitä kustannuspaikkanumeron mukaisessa järjestyksessä. Muutamia yksiköitä nostettiin listalla ylemmäs, kun tuli tietoon, että näihin yksiköihin on tulossa uusia henkilöitä, ja haluttiin saada profiilit käyttöön sitä ennen.

HR-järjestelmästä otettiin Excel-taulukkomuotoinen listaus kaikista henkilöistä, heidän kustannuspaikoistaan ja esihenkilöistä sekä heidän työnimikkeensä. Samankaltaiset työnimikkeet pyrittiin harmonisoimaan aina yhden yksikön sisällä tähän projektin listaukseen, HR-järjestelmään syötettyihin työnimikkeisiin ei tässä projektissa tehty muutoksia.

Käyttäjien pääsyoikeustietoja on Yrityksessä tallennettuna useisiin eri paikkoihin. Kunkin käyttäjän pääsyt tarkistettiin/listattiin yksitellen seuraavista paikoista:

- sisäinen Active Directory (security ryhmät, jakelulistat, verkkokansiot)
- Exchange -järjestelmä (yhteiskäyttöiset postilaatikot)
- ulkoinen Active Directory (ns. extranet-sovellukset)
- käyttöoikeuksien rekisteri AccessRegister (erillistunnukset).

Active Directoryn tiedot haettiin kahdella PowerShell -skriptillä, joista ensimmäinen tekee yhteen listaukseen käyttäjälle määritellyt security-ryhmät, sähköpostin jakelulistat sekä yhteiskäyttöisten verkkokansioiden oikeudet. Toinen skriptirivi hakee sähköpostijärjestelmästä listauksen postilaatikoista, joihin annetulla käyttäjätunnuksella on oikeudet. [2, 3.]

skripti1.ps1

```
1
2  Get-ADPrincipalGroupMembership -Identity <userID> | select name
3
4  Get-Mailbox -ResultSize Unlimited -OrganizationalUnit "<baseOU>" | Get-MailboxPermission -User <userID> | Format-Wide -Column 1 Identity
5
```

Kuva 1 Powershell-skriptit. Ylinnä skriptirivi Active Directoryn listausta varten, alemmalla rivillä haetaan yhteiskäyttöiset postilaatikot sähköpostijärjestelmästä, joihin käyttäjällä on oikeudet.

Samaa AD-skriptiriviä käytettiin niin sisäiseen kuin ulkoiseen Active Directoryyn. AccessRegisteristä haettiin käyttäjäkohtaiset pääsytiedot sovelluksen raporttitoiminnolla.

Kunkin käyttäjän pääsyoikeudet koottiin yhteen Excel-taulukkoon. Jokainen kustannuspaikka laadittiin omalle välilehdelleen ja ko. kustannuspaikan kaikki tehtävänimikkeet kopioitiin kukin omaan sarakkeeseensa. Samaan sarakkeeseen kerättiin kaikkien ko. kustannuspaikalla tällä tehtävänimikkeellä toimivien henkilöiden pääsyoikeudet. Kustakin sarakkeesta poistettiin duplikaatit, jolloin jäljelle jäivät vain tällä kustannuspaikalla ja tällä tehtävänimikkeellä olevien henkilöiden pääsyoikeudet ottamatta kantaa, onko kyseinen oikeus yhdellä vai useammalla henkilöllä.

	A	B	C	D
1	**Varastoesimies**	**Varastotyöntekijä 1**	**Varastotyöntekijä 2**	**Varastotyöntekijä 3**
2	Sovellus1	Sovellus3	Sovellus3	Sovellus22
3	Sovellus2	Sovellus4	Sovellus4	Sovellus4
4	Sovellus3	Sovellus6	Sovellus6	Sovellus6
5	Sovellus4	Sovellus8	Sovellus8	Sovellus8
6	Sovellus5	Sovellus9	Sovellus9	Sovellus10
7	Sovellus6	Sovellus10	Sovellus10	Sovellus12
8	Sovellus7	Sovellus12	Sovellus12	Sovellus19
9	Sovellus8	Sovellus15	Sovellus14	Sovellus23
10	Sovellus9	Sovellus14	Sovellus18	
11	Sovellus10	Sovellus18	Sovellus19	
12	Sovellus11	Sovellus19	Sovellus20	

Kuva 2 Ote Excel-taulukosta pääsyoikeuksineen

Kun yhden kustannuspaikan kaikkien käyttäjien tiedot oli koottu taulukkoon omiin sarakkeisiinsa, ko. kustannuspaikan tiedot kopioitiin Word-dokumenttiin esiteltäväksi esihenkilölle.

Sovellusrivit jaoteltiin tällä hetkellä käytössä olevan tunnustilaus-lomakkeen jaottelun mukaisesti seuraavasti:

1. Yleiset järjestelmät
2. Kansio- ja postilaatikko-oikeudet
3. Toiminnanohjausjärjestelmä
4. Liiketoiminnan järjestelmät
5. Raportoinnin järjestelmät
6. Talouden järjestelmät
7. Viestinnän järjestelmät
8. Asiakaspalvelun järjestelmät
9. Logistiikan järjestelmät
10. Kiinteistön ja huollon järjestelmät
11. IT-järjestelmät
12. Muut.

Sovellusluetteloista poistettiin merkinnät sellaisista pääsyoikeuksista, jotka sisältyvät ylempänä kuvattuihin perusprofiileihin ja jäljelle jäivät vain juuri tälle kustannuspaikalle ja tehtävänimikkeelle ominaiset pääsyoikeudet sekä mahdolliset kuhunkin järjestelmään liittyvät määrittelyt ja oikeustasot. Lisäksi Word-listalta poistettiin esim. sellaiset AD security -ryhmät, jotka tarvitaan jonkun tai joidenkin määrättyjen sovellusten käyttöön mutta eivät sinällään oikeuta minkään sovelluksen käyttöön. Tällaisia ryhmiä ovat esim. Citrix-järjestelmään liittyvät järjestelmän määritysryhmät, jotka kuitenkin näkyvät käyttäjäkohtaisissa listauksissa ja jotka ovat mukana myöhemmin tässä dokumentissa kuvattavassa ServiceDeskin työkalussa.

4 Profiilien käyttöönotto

Kun kunkin kustannuspaikan kaikkien henkilöiden pääsyoikeudet oli saatu kartoitetuksi ja listatuksi, niistä luotiin Word-dokumentti. Kaikista kustannuspaikan tehtävänimikkeistä tehtiin oma listauksensa, johon lueteltiin ko. tehtävään liittyvät pääsyoikeudet. Aiemmin mainitut perusoikeudet jätettiin pois kustannuspaikkakohtaisista dokumenteista, näistä vain mainittiin dokumentin alussa.

4.1 Käyttöönotto yksiköissä

Kustannuspaikkojen esihenkilöiden kanssa käytiin läpi, millaisia pääsyoikeuksia heidän tiiminsä tehtävänimikkeille löytyi. Aluksi muutaman ensimmäisen tiimin osalta lähetin kutsut koko tiimille, mutta hyvin nopeasti havaitsin, että koko tiimin saaminen koolle varsinkin isompien tiimien osalta oli melko hankalaa ja palaverien ajankohdat venyivät liian pitkälle. Dokumentin läpikäynti myös koko tiimin kanssa ei tuntunut järkevältä toimintamallilta.

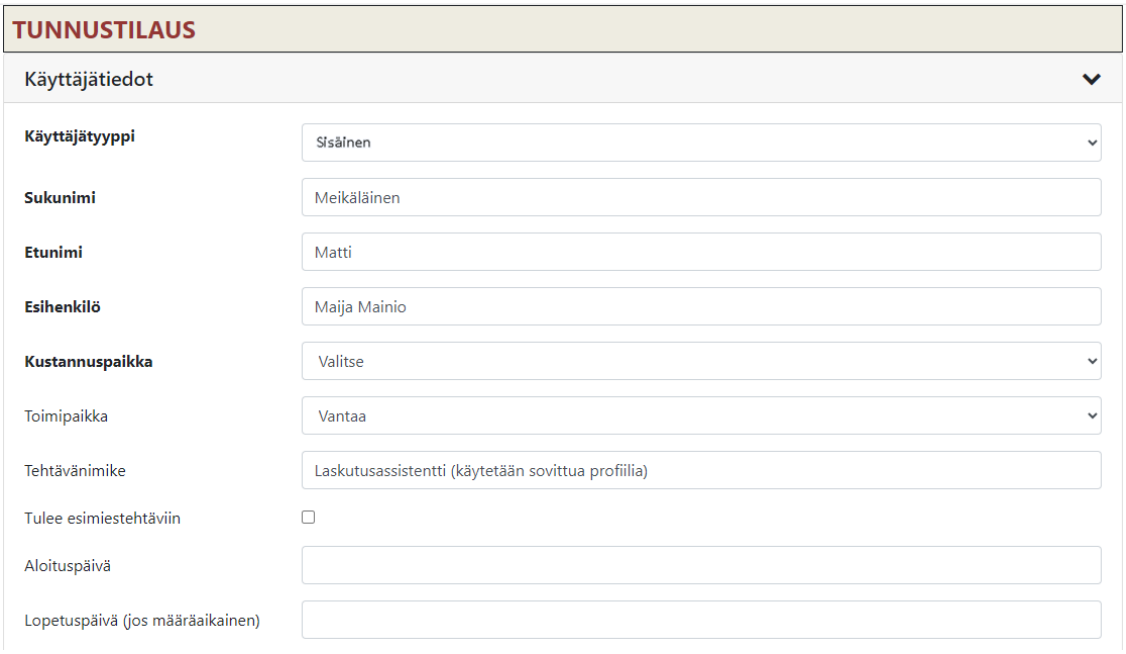
Hyvin nopeasti totesin, että järkevintä on lähettää Teams-palaverikutsu vain kunkin kustannuspaikan esihenkilölle. Esihenkilöt saivat mielellään välittää kutsua myös omille tiimiläisilleen oman näkemyksensä mukaan. Kutsussa lähti mukana ko. kustannuspaikan profiilidokumentti jo etukäteen tutustuttavaksi.

Kunkin palaverin aluksi kävin läpi, mistä koko projektissa on kyse ja kerroin miten profiilidokumentin tiedot oli kerätty. Sen jälkeen palaverissa käytiin läpi, millaisia tehtävänimikkeitä ko. kustannuspaikalle oli löydetty ja mitä nimikkeitä oli ehkä yhdistetty. Ensimmäisissä palavereissa profiilit käytiin läpi hyvinkin tarkalla tasolla rivi kerrallaan. Havaitsin kuitenkin, että yhteiset dokumentin lukuistunnot olivat ajankäytöllisesti turhia.

Tehokkaimmaksi toimintamalliksi muodostui käytäntö, jossa ensin esittelin projektin ja sen tavoitteet, ja sen jälkeen kustannuspaikan profiilit ja niiden pääsyoikeudet. Tämän jälkeen esihenkilöt saivat kukin omalla tahollaan käydä dokumentin läpi oman tiiminsä kanssa sillä näkökulmalla, että kullakin profiililla luodaan uuden tiimissä aloittavan henkilön (joko täysin uuden työntekijän tai tiimiä

vaihtavan henkilön) pääsyoikeudet. Olemassa olevien tiimiläisten pääsyoikeuksia ei pääsääntöisesti muutettu. Muutamalle kustannuspaikalle tehtiin olemassa olevien tehtävänimikkeiden lisäksi myös valmiiksi ns. kausiapulaisten profiilit. Näihin profiileihin tiimit poimivat muita suppeammat pääsyoikeudet, joita voidaan käyttää esimerkiksi kesäapulaisten kohdalla.

Palavereiden lopuksi kävin vielä esihenkilöiden kanssa läpi, miten profiileja niiden hyväksymisen jälkeen käytetään. Tähän asti esihenkilön on pitänyt määritellä kaikki henkilölle avattavat pääsyoikeudet yrityksessä käytössä olevalla web-lomakkeella, joka lähetetään ServiceDeskille sähköpostilla. Profiilien käyttöönoton jälkeen käytetään edelleen samaa web-lomaketta, mutta esihenkilö määrittelee lomakkeelle vain käytettävän profiilin nimen. Lisäksi, jos henkilölle jostain syystä tarvitaan jotain profiilista poikkeavia lisäoikeuksia, ne voidaan tilata samalla lomakkeella.



Kuva 3 Näkymä tunnustilauslomakkeen perustiedoista.

Kun esihenkilö oli yhdessä tiimin kanssa hyväksynyt profiilien sisällöt, merkitsin päivitetyn dokumentin loppuun profiilien hyväksymispäivän ja muutoslokin. Profiilidokumentista luotiin pdf-muotoinen versio tiimin muistilistaksi ja se tallennettiin Yrityksen intranet-hakemistoon.

4.2 Käyttöönotto ServiceDeskissä

Kun aiemmin mainitut koko yrityksen perusprofiilit oli saatu määritellyksi, ne otettiin heti käyttöön, vaikka kustannuspaikkakohtaiset profiilit vielä olivatkin kesken. Joillakin varastotehtävillä riittää pelkkä varastohenkilön perustunnus, eikä heille tarvita muita oikeuksia, koska he käyttävät varasto- ja toiminnanohjausjärjestelmiin geneerisiä tunnuksia.

ServiceDeskin työkaluksi laadittiin ServiceDesk-tiimin Sharepoint-hakemistoon Excel-taulukko, johon kirjattiin sekä toimisto- että varastohenkilöiden perustunnukset heti niiden valmistuttua. Näille perustunnuksille määritettiin geneerinen kustannuspaikka xxxx. Samaan taulukkoon lisättiin kustannuspaikkakohtaiset profiilit tiimien hyväksynnän jälkeen. Taulukkoon kirjattiin seuraavat tiedot:

- kustannuspaikka
- profiilin nimi
- toimipaikka
- pääsyoikeuden/järjestelmän nimi ja mahdollinen oikeustaso
- pääsyoikeuteen liittyvät mahdolliset AD-ryhmät
- tieto, kuuluuko pääsyoikeus perustunnukseen vai kustannuspaikkakohtaiseen profiiliin
- tieto, mihin järjestelmään ko. pääsyoikeudet luodaan tai jos pääsyoikeus pyydetään kolmannelta osapuolelta
- tunnustilauslomakkeella käytetty jaottelu.

Kustannus-paikka	Profiilin nimi	Toimipaikka	Sovellus	Lisättävä AD-ryhmä	perustunnus/ sovellus/ toimisto/ varasto	Järjestelmä	Tunnustilauksen osio

Kuva 4 ServiceDeskin työkalun otsikkorivi filttereineen

Kun ServiceDeskiin tulee HR-järjestelmästä uuden henkilön aloitusilmoitus, aloitetaan perustunnuksen teko jo ennen esihenkilön lähettämää tunnustilausta. Profiilin mukaiset pääsyoikeudet lisätään sitten perustunnukseen esihenkilön lähettämän tunnustilauksen perusteella. Näin saadaan tikettijärjestelmään merkintä, että esihenkilö on määritellyt ko. henkilölle hänelle tarvittavat oikeudet.

Tehtävänimike saattaa olla eri kuin käytettävä profiili. Auditoinneissa saatetaan kysyä evidenssiä esim. toiminnanohjausjärjestelmään tehtyjen tunnusten pyynnöistä.

Kun pääsyoikeuksia lähdetään määrittelemään, tarkistetaan ensin, onko henkilölle jo luotu perustunnus. Jos perustunnusta ei vielä ole, valitaan taulukkoon ensin perustunnuksen geneerinen kustannuspaikka sekä toimisto- tai varastohenkilön profiili. Tämän jälkeen lisätään taulukkoon henkilön oma kustannuspaikka, esihenkilön määrittelemän profiilin nimi sekä toimipaikka. Jos perustunnus on jo luotu, voidaan perustunnuksen profiilin tiedot jättää valitsematta.

Kun taulukko on filtteröity valmiiksi, siitä tallennetaan kopio tikettijärjestelmään esihenkilön tunnustilauksen liitteeksi. Näin saadaan dokumentoitua käyttäjälle luodut pääsyoikeudet.

Käyttäjätunnukset ja pääsyoikeudet luodaan sitten järjestelmä- ja sovelluskohtaisten erillisten ohjeiden mukaisesti. Luodut käyttäjätunnukset ja salasanat välitetään käyttäjälle oman prosessinsa mukaisesti erillisillä viesteillä.

4.3 Käyttöönoton kommunikointi

Kun kaikkien käyttäjien perusprofiilit saatiin määritellyiksi, kaikille esihenkilöille sekä HR:lle lähetettiin asiasta tiedote. Viestin liitteenä lähetettiin tiedoksi dokumentti kaikille työntekijöille määriteltävistä oikeuksista.

Kullekin tiimille kommunikoitiin aina heidän kustannuspaikkakohtaisen profiilinsa valmistumisesta ja sovittiin profiilien käyttöönotosta. Samassa yhteydessä esihenkilöiden kanssa myös käytiin läpi tunnusten tilaaminen tunnustilauslomakkeella profiileja käyttäen. ServiceDeskin käyttäjähallinta-tiimi seurasi profiilien valmistumista projektidokumentaatiosta tiimin omassa kansiossa.

Kun kaikki profiilit olivat valmistuneet, yrityksen sisäisellä viestintäkanavalla julkaistiin asiasta yleisellä tasolla oleva uutinen.

5 Profiilien jatkokehittäminen

Nyt luotuja perustunnuksia päivitetään tarpeen mukaan, kun uusia järjestelmiä tulee käyttöön tai poistuu käytöstä, joko toimistoon ja/tai varastohenkilöille. Koska perustunnusten sisältöä ei ole erikseen listattu kustannuspaikkakohtaisessa dokumentaatiossa, yhden dokumentin päivittäminen riittää. Tehdystä muutoksesta tiedotetaan kaikille esihenkilöille Yrityksen viestintäkanavilla.

Tiimien kanssa on sovittu, että profiileja voidaan tarkistaa aina tarvittaessa, mutta kuitenkin vuosittain. Tällöin tiimin esihenkilölle lähetetään kehotus tarkistaa oman kustannuspaikkansa profiilit intranet-hakemiston dokumentista ja heiltä pyydetään kuittaus ja mahdolliset muutostarpeet vastausviestinä. Kun kuittaus on saatu, dokumentin muutoslokiin merkitään tarkistuspäivämäärä sekä tehdään pyydetyt muutokset profiileihin.

Profiileihin voi tulla muutoksia sekä esihenkilön pyynnöstä tai jos järjestelmissä, jakelulistoissa tai kansiorakenteissa tapahtuu muutoksia. Jos profiiliin tarvitaan muutoksia tarkistusten välillä, näistä tehdään merkinnät dokumentin muutoslokiin. Lokiin kirjataan seuraavat tiedot:

- muutoksen päivämäärä
- muutoksen pyytäjä (esihenkilö tai ServiceDesk)
- muutoksen sisältö; mitä muutettu ja missä profiilissa.

Päivitetty profiilidokumentti tallennetaan Sharepointin kansioon ja ServiceDeskin Excel-taulukko päivitetään muutosten osalta.

Tiimikohtaiset työnimikkeisiin perustuvat käyttooikeusprofiilit ovat olleet käytössä nyt noin vuoden ajan. Profiilien käytöstä on saatu pelkästään positiivista palautetta niin esihenkilöiltä kuin HR:stä. Esihenkilöt ovat kokeneet, että valmiiksi rakennetut käyttöoikeusmallit ovat helpottaneet huomattavasti uusien työntekijöiden oikeuksien määrittelyä. Myös ServiceDeskin tarvitsemat lisätietokyselyt ovat vähentyneet. Työtehtävien muuttuessa on helpompaa myös määritellä ja ylläpitää mahdollisesti poistettavia oikeuksia/käyttäjätunnuksia.

Profiilien laajentamista on pohdittu myös ns. konsultti-käyttäjien käyttöoikeuksiin. Tämä on kuitenkin asiantuntijatiimien kanssa käydyissä keskusteluissa todettu haastavaksi, koska näillä käyttäjillä käyttöoikeudet vaihtelevat suurestikin heidän tehtäviensä mukaan, eikä yhdistäviä tekijöitä ole samalla tavalla löydettävissä kuin Yrityksen sisäisille käyttäjille.

Esihenkilöiden käyttöön ollaan yrityksessä suunnittelemassa portaalisovellusta, jotta ensivaiheessa uusien työntekijöiden oikeuksien määrittely olisi entistä helpompaa. Käyttöön ollaan suunnittelemassa myös automaatiota, jossa HR-järjestelmään syötetyistä uuden työntekijän tiedoista saadaan luotua ns. perustunnus automaattisesti. Tämän jälkeen ServiceDesk vain tarkistaa tunnuksen oikeellisuuden, sekä aktivoi tunnuksen työsuhteen alkaessa. Kun tunnus on aktivoitu, esihenkilö määrittelee portaalissa käytettävän profiilin pudotusvalikosta. Lisäksi voidaan henkilölle tilata sellaisia oikeuksia, joita profiiliin ei sisälly. Portaalin työnkulkuihin määritellään mahdollisuuksien mukaan tarvittavat tunnukset ja käyttöoikeudet muodostumaan automaattisesti, tai pyynnöstä lähtee palvelupyynnöt niitä toteuttaville tiimeille. Automaatio myös päivittää tällä hetkellä manuaalisesti ylläpidettävän pääsyoikeuksien rekisterin.

Jatkopohdinnassa on vielä edelleen automaation laajentaminen siten, että HR-järjestelmässä käytettävät tehtävänimikkeet laukaisevat uusien tunnusten ja käyttöoikeuksien luomisen suoraan ilman ServiceDeskin toimenpiteitä. Vain kolmansilta osapuolilta pyydettävät tunnukset ja käyttöoikeudet joudutaan silloin luomaan käsin.

6 Yhteenveto

Yksikkökohtaiset käyttöoikeusprofiilit ovat olleet nyt käytössä noin vuoden ajan. Jo nyt niiden käyttöönotosta on havaittu merkittäviä etuja organisaation sisäisessä työnkulussa.

Profiilien määrittely ja käyttö on helpottanut työtä sekä tiimeissä että Service-Deskissä. Vaikka profiilien luonti osoittautui aluksi melko työlääksi sekä Service-Deskin tiimille että esihenkilöille, on profiilien käyttöönotto helpottanut työskentelyä huomattavasti kaikille osapuolille. Työaikaa on säästynyt molemmilla tahoilla, koska tarkentavia kysymyksiä käyttöoikeuksien määrittelyssä ei enää tarvita.

Yhteistyö eri ryhmien kanssa oli erittäin rakentavaa. Profiilien tiimoilta on käyty useita hyviä keskusteluja, jotka ovat edistäneet yhteistä ymmärrystä organisaation työprosesseista. Esihenkilöille on ollut erittäin herättelevää ja avaavaa nähdä miten monipuolisia oikeuksia tiimiläisillä on. Tämä on auttanut esihenkilöitä ymmärtämään paremmin tiimiläisten erilaisia rooleja sekä vastuita.

Yrityksessä käytössä olevien eri järjestelmien määrä ja niistä käytettävät eri nimitykset ovat tulleet monelle esihenkilölle yllätyksenä. Tämä on osoittanut kuinka monimutkainen ja monipuolinen Yrityksen IT-infrastruktuuri oikeasti on. Esihenkilöt ymmärtävät nyt paremmin miten eri järjestelmät toimivat yhdessä ja miten ne tukevat Yrityksen toimintaa.

Kaiken kaikkiaan tehtävänimikkeisiin perustuvien käyttöoikeusprofiilien käyttöönotto on ollut merkittävä askel kohti tehokkaampaa ja sujuvampaa työskentelyä. Vaikka profiilien luominen ja käyttöönotto vaati paljon työtä, on niiden avulla saavutettu monia hyötyjä, jotka hyödyttävät kaikkia osapuolia niin IT:ssä kuin myös liiketoiminnan yksiköissä.

Lähteet

1. Microsoft-koulutusmateriaali. Active Directory Domain Services Overview. Verkkoaineisto. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>. Luettu 11.10.2023.

2. Microsoft-koulutusmateriaali. Get-ADPrincipalGroupMembership. Verkkoaineisto. <https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adprincipalgroupmembership?view=windowsserver2022-ps>. Luettu 26.6.2023.

3. Microsoft-koulutusmateriaali. Get-Mailbox. Verkkoaineisto. <https://learn.microsoft.com/en-us/powershell/module/exchange/get-mailbox?view=exchange-ps>. Luettu 26.6.2023.

4. .PDF-tiedostopääte. Verkkoaineisto. <https://tiedosto.info/extension/pdf.html> Luettu 6.1.2024

5. Usein kysyttyä EU:n tietosuoja-asetuksesta. Tietosuojavaltuutetun verkkomateriaali. < https://tietosuoja.fi/gdpr>. Luettu 25.10.2023.

6. Yrityksen sekä emoyhtiön sisäiset intranet-sivut.