Haaga-Helia
ammattikorkeakoulu Oy

Ratkaisusuunnittelijana kunnallisessa julkishallinnossa Helsingin kaupungilla: IT-generalistin päiväkirja

Lauri Virkamäki

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2022

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

13.04.2022

Tekijä(t)
Lauri Virkamäki

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Ratkaisusuunnittelijana kunnallisessa julkishallinnossa Helsingin kaupungilla: IT-generalistin päiväkirja

Sivu- ja liitesivumäärä
71 + 3

Opinnäytetyön otsikko englanniksi
Working as a solutions engineer for City of Helsinki: the diary of an IT-generalist

Tämä opinnäytetyö on portfoliomainen päiväkirjamuodossa toteutettu opinnäytetyö, jossa tarkastellaan IT-yleisosaajan, eli IT-generalistin, työtehtäviä ja omaa työssäni kehittymistä. Päiväkirjan seurantajakson ajankohta on 17.1.2022 - 11.3.2022, ja se koostuu 40 työpäivästä.

Työpaikkani raportointijakson aikana oli Helsingin kaupungin kaupunginkanslian digitalisaatioyksikön tukipalvelut-tiimi, joka vastaa erityisesti kaupungin toimialojen, liikelaitosten ja virastojen IT-perustuen tarjoamisesta ja sen kehittämisestä.

Opinnäytetyön aikana toteutuneet työtehtävät keskittyivät erityisesti erilaisten automaatioratkaisujen toteuttamiseen, prosessien suunnitteluun ja tietoturva- ja tietosuojatarpeiden havainnointiin ja niiden vaatimusten mukaisten ratkaisujen kehittämisen. Opinnäytetyössä sivutaan myös joitakin vaativampia ongelmanratkaisutapauksia, sekä omaan ajanhallintaan liittyviä ongelmia.

Seurantajakson aikana jouduin pohtimaan erityisesti eurooppalaisen yleisen tietosuoja-asetuksen (GDPR) ja tietoturvan soveltamista erilaisissa järjestelmissä, pohtimaan ajankäytön hallintaa, suunnittelemaan organisaation prosesseja, sekä kehittämään teknistä osaamistani eri teknologioissa. Näistä nousivat esiin erityisesti Universal Print -ratkaisu, Remote Desktop Services-järjestelmäkokonaisuus, sekä skriptauksessa Powershell ja WPF (Windows Presentation Foundation).

Työn aikana laajensin myös osittain tiedonhakutapojani normaaleiden teknisten lähteiden lisäksi tieteellisempään kirjallisuuteen. Tästä oli hyötyä esimerkiksi master datan hallintaprosessien pohtimisessa.

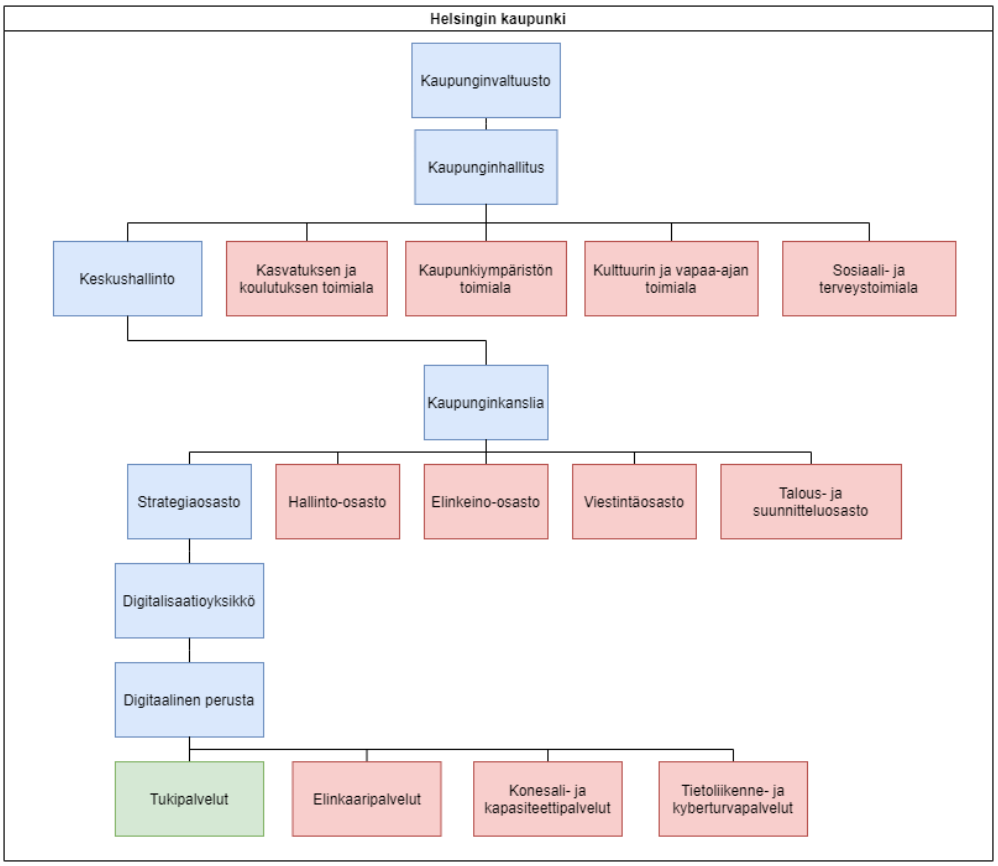
Asiasanat
automaatio, tietosuoja, tietoturva, järjestelmäarkkitehtuuri, ajanhallinta

Sisällys

1 Johdanto

Tämän päiväkirjamuotoisen opinnäytetyön suoritusajankohta on välillä 17.1.2022 - 11.3.2022. Raportointi tapahtuu päivittäisellä työtehtävien kuvaamisella, minkä lisäksi tehdään viikoittainen syvällisempi analyysi.

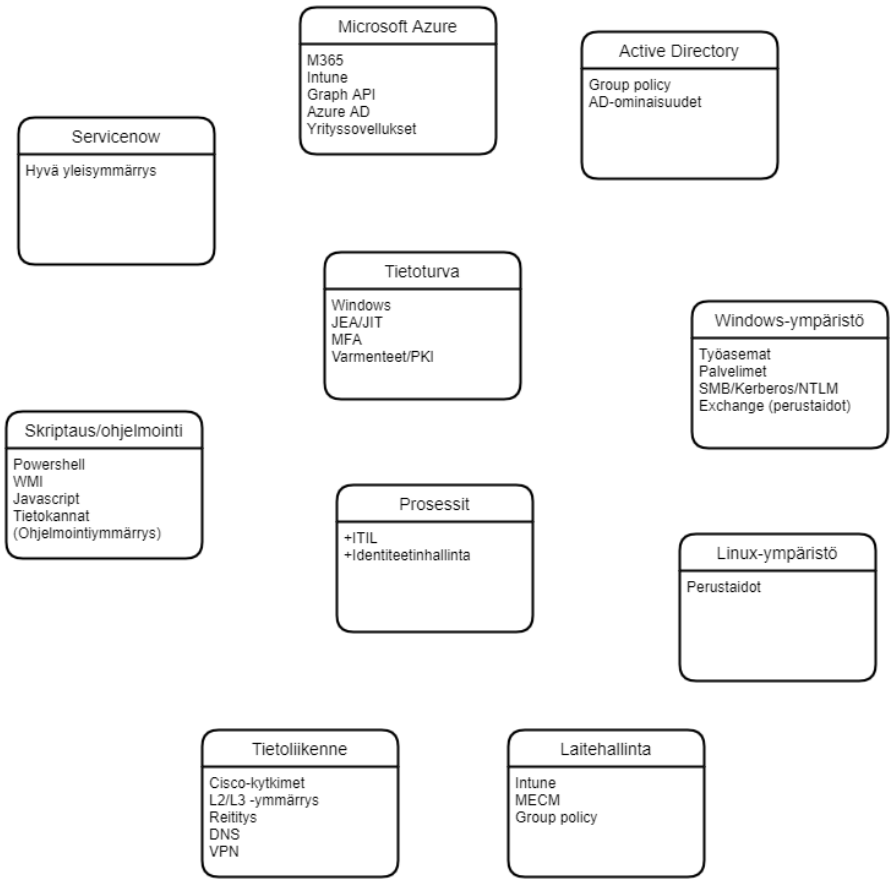
Työskentelen Helsingin kaupunginkanslian strategiaosaston digitaalinen perusta -yksikössä tukipalvelut-tiimissä. Kyseessä on uusi vuoden 2021 alusta toimintansa aloittanut keskitettyjä kaupungin sisäisiä perustietotekniikan palveluita tarjoava palveluorganisaatio. Helsingin kaupunginkanslia toimii Helsingin kaupunginhallituksen alaisena virastona kaupunkiorganisaatiossa. Tarkempi typistetty organisaatiokaavio oman yksikköni sijoittumisesta on esitetty kuvassa 1.



Kuva 1. Helsingin kaupungin organisaatio kaupunginkanslian ja tukipalvelut-yksikön sijoittumisesta kaupunkiorganisaatiossa. Sininen väri kuvaa tukipalvelut-tiimin organisaatiopolun, punainen merkittävimmät rinnakkaiset organisaation osat. Sijaitsen itse vihreällä merkityssä tukipalvelut-yksikössä.

Tukipalvelut-tiimissä työskentelee erilaisissa asiantuntijatehtävissä noin 10 henkilöä tukipalveluista vastaavan palvelupäällikön alaisuudessa. Tukipalvelut-tiimillä on lisäksi neljä eri alitiimiä, joista kukin vastaa oman alueensa lähituesta.

Oma tehtävänimikkeeni on ICT-projektipäällikkö, mutta se ei kuvaa varsinaisissa työtehtävissäni tarvittavaa osaamista kovinkaan hyvin. Kuvaavampi nimike voisi mielestäni olla ICT-arkkitehti, sillä suuri osa työtehtävistäni koostuu vaativista ongelmanselvitys- ja kehitystehtävistä. Joka tapauksessa työtehtävissäni tarvittava osaaminen on erittäin laaja-alaista, ja siihen kuuluvat kaikki osa-alueet tietoliikenteestä tietoturvaan ja Active Directory -toimialuehallinnasta Azure Active Directoryyn ja erilaisiin pilvipalveluihin. Teknisten taitojen lisäksi tärkeitä ovat myös erilaiset sosiaaliset taidot ja erityisesti asiakkaiden ja muiden sidosryhmien tarpeiden ymmärtäminen. Kuvassa 2 on tuotu esille työtehtävissäni jatkuvasti tarvittavia tietotekniikan osaamisen osa-alueita ja niiden yhteyksiä, sekä niihin liittyviä protokollia ja käsitteitä, joiden ymmärtäminen on työtehtävien kannalta erityisen tärkeää. Kyseiset lyhenteet ja niiden merkitykset on avattu tarkemmin liitteessä 1.



Kuva 2. Työtehtävissä vaadittavaa osaamista eri osa-alueilta.

Tarvittavan osaamisen laaja-alaisuus johtuu erityisesti siitä, että ratkaisujen kehittäminen ja löytäminen vaatii ymmärrystä sekä tarjolla olevista teknologioista, että esimerkiksi organisaation tietoturvavaatimusten soveltamista ja noudattamista, kuin myös asiakkaiden tarpeiden sovittamista kyseisiin reunaehtoihin. Työtehtävissä tulee siis ymmärtää ympäristön

lisäksi myös se, että miksi ympäristö ja olemassa olevat ratkaisut on suunniteltu ja rakennettu kyseisellä tavalla.

Työtehtävieni tietoperustaa ei voi kiteyttää vain muutamaan lähdeteokseen, vaan kyseessä on jatkuvaa tietoperustan kehittämistä ja hyödyntämistä vaativa työtehtävä. Merkittävin osa tietoperustaa on eri teknologioihin liittyvän referenssimateriaalin lukeminen, kuten esimerkiksi Microsoftin tekniset internet-sivut ja erilaisten ohjelmistojen muu referenssimateriaali. Tämän lisäksi kokonaisuuksien hahmottamisessa on paljon apua erilaisten yksittäisten aihealueiden asiantuntijoiden kirjoitusten, mielipiteiden ja esimerkkien lukemisesta, sillä tämä antaa useimmiten kyseisestä aihealueesta paremman kokonaiskuvan kuin pelkkä referenssimateriaalin lukeminen. Tietoperustan ylläpitämiseen kuuluu myös uusiin teknologioihin tutustuminen ja niiden kehittymisen seuranta.

Opinnäytetyön suorittamisen aikana työtehtäväni painottuivat erityisesti erilaisten automaatioratkaisuien toteuttamiseen, tietoturvaa parantavan ympäristön käyttöönottoon, sekä myös prosessisuunnitteluun, ja opinnäytetyön näkökulma keskittyy erityisesti näihin aihealueisiin. Työtehtäviin kuuluivat myös jatkuvasti erilaiset vaativat ongelmanselvitystehtävät, mutta tyypillisesti ne perustuivat aiemmin hankkimaani tietoon ja eivät siten ole keskeisesti opinnäytetyössä esillä.

Henkilökohtaisesti haluan kehittyä erityisesti siinä, miten saisin tietoa ja vastuuta jaettua muille työkavereille, kuin myös tunnistaa muiden mahdollisesti piilevät taidot ja tuotua niitä esille jonkinlaisen mentoroinnin tai muunlaisen kannustamisen kautta. Myös erilaisten hallinnollisten taitojen kehitys kiinnostaa tietyiltä osin, vaikka ensisijainen kiinnostuksenaiheeni onkin erilaisiin prosesseihin liittyvät tekniset automaatioratkaisut.

2 Lähtötilanteen kuvaus

Tässä kappaleessa kuvataan opinnäytetyötä edeltävää työtilannetta, työhöni liittyviä sidosryhmiä, sekä työssäni tarvittavia vuorovaikutustaitoja.

2.1 Oman nykyisen työn analyysi

Kuten johdannosta ja kuvan 2 osaamistarpeista ilmenee, on työni luonne hyvin laaja-alaista. Työtehtävät keskittyvät erityisesti erilaisten teknisten haasteiden ratkaisemiseen, mutta ratkaisujen kehittäminen vaatii myös hyvän ymmärryksen prosesseista ja niihin liittyvistä vaatimuksista. Ratkaisujen löytämisessä tulee myös huomioida erilaiset sidosryhmien tarpeet ja se, tuleeko esimerkiksi olemassa olevia prosesseja muuttaa erilaisiksi.

Alla on listattuna erilaisia tätä opinnäytetyötä edeltäviä työtehtäviä:

- Tekninen projektivastuu ylläpitotunnusten tietoturvan parantamiseen liittyvässä projektissa.
- ITSM-järjestelmän (Servicenow) ongelmanhallintaprosessin käyttöönotto
- Laajan toimintaympäristöön liittyvän kokemuksen ja tietopohjan hyödyntäminen ongelmanratkaisussa.
- Identiteetinhallinnan automatisointi ja siihen liittyvien IT-prosessien valmistelu.
- Palvelinten siirtoprojektin käyttäjähakemistojen siirron automatisointi.
- Ajoittainen sisäisten koulutusten suunnittelu/vetäminen tarpeen mukaan.
- Yleinen kollegoiden neuvonta ja tiedon jakaminen.

Työtehtävissä tärkeimpänä yhteisenä tekijänä on syvällinen IT-ympäristön ymmärtäminen. Tämä ymmärrys on syntynyt reilun kymmenen vuoden uran aikana erilaisissa IT-tehtävissä kyseisessä organisaatiossa, kuin myös itsenäisen opiskelun kautta. Käytännössä osaamisen hankkimisen kannalta itsenäinen opiskelu tarkoittaa omalla kohdallani sitä, että uuteen lyhenteeseen, järjestelmään tai korkean tason konseptiin törmätessä käytän vähän aikaa sen tutkimiseen. Tähän saattaa kuulua pikainen googlettaminen, referenssimateriaalin selailu tai muun vastaavan korkean tason lähdemateriaalin luku. Tarvittaessa perehdyn aiheeseen syvemmin itseopiskelun tai koulutusten kautta.

Edellä mainitussa listassa on mainittu useampia eri projekteja, mutta niissä työtehtäväni ovat keskittyneet projektitehtäviin, eivätkä projektien johtamiseen. Nimikkeenä ICT-projektipäällikkö on täten jokseenkin harhaanjohtava, Osassa projekteista olen kyllä koordinoinut jotain projektin teknistä osaa, ja varmistanut että siihen liittyvät vaatimukset saadaan

toteutettua aikataulun mukaisesti. Esimerkkinä juuri listassa mainittu "tekninen projektivastuu", mikä käytännössä tarkoittaa sitä, että olin vastuussa projektin teknisen puolen toteutumisesta mutta varsinaisena projektipäällikkönä toimi eri henkilö.

Yhtenä erityisenä työtehtäviäni yhdistävänä tekijänä on ohjelmointitaustani, josta on hyötyä miltei poikkeuksetta. Se mahdollistaa toistuvien työtehtävien automatisoinnin, kuin myös auttaa automatisaatiota tukevassa prosessiajattelussa. Erilaisia tehtäviä ja projekteja tehdessäni olen huomannut sen, että usein automatisoitava prosessi yritetään rakentaa suorana kopiona manuaaliprosessille, ilman että siihen tehdään automaatiota tukevia muutoksia. Yhtenä esimerkkinä tästä voisi olla allekirjoituksen saaminen dokumenttiin. Aiemmassa prosessissa sähköinen dokumentti tulostetaan, minkä jälkeen siihen saadaan allekirjoitus, ja se arkistoidaan paperisena. Uudessa sähköisessä prosessissa voi olla houkuttelevaa lisätä olemassa olevan prosessin loppuun dokumentin skannaus ja arkistointi sen sijaan, että koko prosessi alusta loppuun toimisi sähköisenä. Vuosien saatossa tärkeäksi kysymykseksi itselleni onkin muodostunut "mitä haluat tehdä?", sen sijaan että keskittyy menetelmään ("miten haluat tehdä?") . Tässä esimerkissä väärä kysymys on "miten saan allekirjoitetun fyysisen dokumentin arkistoitua sähköisessä muodossa?", ja oikea kysymys on "miten saan tämän prosessin toteutettua tehokkaasti ja/tai sähköisenä?".

Omien taitojeni osalta kykenen myös indeksoimaan tietoa erittäin tehokkaasti. Usein jokin vuosien takainen tiedonjyvänen nousee tietoisuuteen juuri oikea-aikaisesti oikean ärsykkeen saatuani. Tehtävän laaja-alaisuuden takia en voi olla erittäin syvällinen asiantuntija kaikilla osa-alueilla, mutta kykenen korkean tason ymmärryksen perusteella syventämään tietoani jollakin osa-alueella hyvin nopeasti. Työtehtävieni kannalta tämä indeksointikyky ei ole välttämättä pakollinen, mutta työtehtävät vaativat generalistin (yleisosaaja) luonteen ja melko nopean oppimis- ja ymmärtämisnopeuden.

Osaamiseni työtehtävissä on erittäin korkealla tasolla. Olen käytännössä pystynyt seuraamaan ympäristön kehittymistä noin kymmenen vuoden ajan, ja samalla kehittää osaamistani työtehtävien vaatimusten mukaisesti. Vaikka työtehtäväni ovatkin painottuneet erittäin paljon teknisten ratkaisujen löytämiseen ja toteuttamiseen, olen myös saanut muiden tekemisiä seuraamalla ja kysymyksiä esittämällä perehdyttyä jossain määrin esimerkiksi talous- ja muihin toiminnan kannalta tärkeisiin prosesseihin.

Nykyisellään oma näkemykseni on se, että pystyn ymmärtämään, selittämään ja ratkaisemaan miltei minkä tahansa teknisen tai IT-prosessiin liittyvän ongelman itsenäisesti, kuin myös kehittämään niihin liittyviä toimintamalleja organisaation tarpeiden mukaisesti. Olen

myös pitänyt useampia sisäisiä koulutuksia, minkä lisäksi pyrin parantamaan kollegoiden toimintaedellytyksiä niiltä osin kuin se nähdään tarpeelliseksi ja hyödylliseksi. Tähän kuuluvat esimerkiksi erilaisten työtä tehostavien työkalujen kehittäminen, henkilökohtainen opastaminen kuin myös dokumentaation laatiminen erilaisista parhaiksi tai toimiviksi havaituista käytännöistä.

Oman kehittymiseni osalta koen tärkeänä pysyä selvillä teknologian ja toimintamallien kehityksestä. Aiemmin mainitsemani nopean oppimisen ja generalistin luonteen takia tämä ei kuitenkaan ole merkittävin kehittymisen kohde, ja sen merkittävyys koskee lähinnä ns. "työkalupakin" ajan tasalla pitämisessä. Teknisen asiantuntijuuden ja osaamisen osalta kehittyminen koskee lähinnä uusiin teknologioihin tutustumista, että niitä voi tarvittaessa hyödyntää käytännössä.

Yksi asia, mihin minun pitää kiinnittää enemmän huomiota on ajankäyttö ja erilaisten tehtävien priorisointi. Usein huomaan, että vaihdan liiankin helposti erilaisten tehtävien välillä, kuten esimerkiksi hyppään yhden ongelman ratkaisemisesta täysin siihen liittymättömän dokumentaation kirjoittamiseen, ja saatan välissä kirjoittaa muutaman sähköpostin. Paljon ohjelmointia harrastaneena ja myös työssäni automaatiotyökaluja tehneenä huomaan, että keskittymiskohdetta vaihtaessa kestää jonkin aikaa, että tehtävän suorittamistehokkuus palaa optimitasolle. Osaltaan keskittymisen herpaantumiseen vaikuttavat tietenkin modernin maailman pikaviestimet ja sähköposti-ilmoitusten kilahtelu. Eräillä kollegoillani onkin viikolta varattu esimerkiksi tunnin tai parin ajanjaksoja keskittymistä vaativille tehtäville, jolloin heihin ei välttämättä saa pikaviestimillä yhteyttä. Tämänkaltainen ajanhallinnan kehittäminen on käynyt myös itselläni mielessä, mutta en ole sitä vielä toteuttanut.

Taitojen osalta seuraavat kehittämiskohteeni sijaitsevan teknisten asioiden ulkopuolella, sillä koen omaavani riittävät tekniset taidot ja kyvyn omaksua mihin tahansa tekniseen toteutukseen liittyvät taidat nopeasti. Eräitä asioita, joita pyrin erityisesti oppimaan teknisten taitojen ohella, ovat taloudenhallinta ja johtamiseen liittyvät taidot. Tämä johtuu siitä, että vaikka teknisten ongelmien ratkaiseminen on mielenkiintoista, toivon myös pystyväni auttamaan muita omassa kehittymisessään, jolloin jonkinlaiset johto- tai esimiestehtävät olisivat mahdollinen looginen työuran edistysaskel jossain vaiheessa.

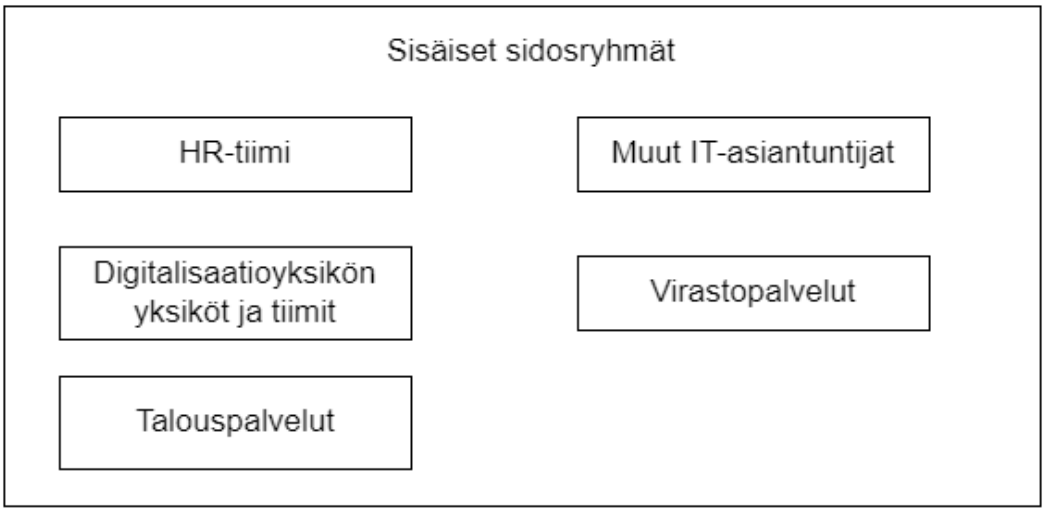
2.2 Sidosryhmät työpaikalla

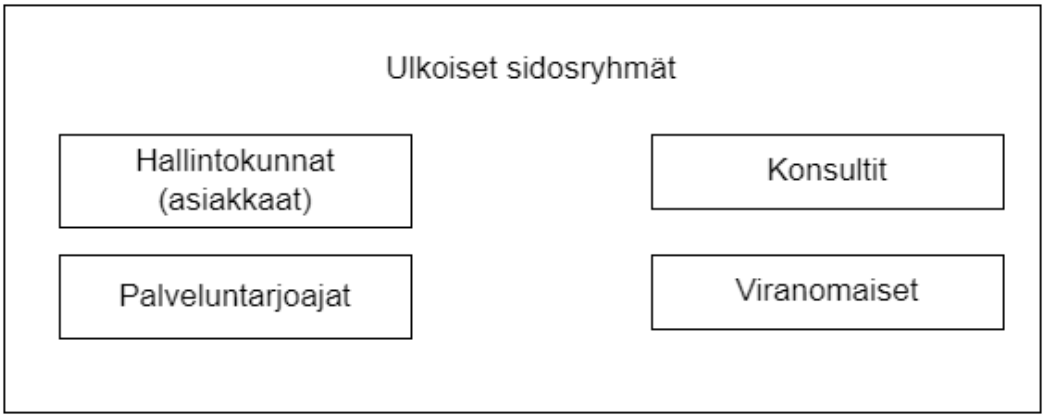
Työtehtävissäni olen usein tekemisissä sekä ulkoisten että sisäisten sidosryhmien kanssa. Sisäisiin sidosryhmiin kuuluvat erityisesti digitaalinen perusta -yksikön muut aliyksiköt, sillä kullakin on oma vastuualueensa kokonaisuudesta. Tämän lisäksi sisäisiin

sidosryhmiin kuuluvat erilaiset tukitoiminnot, kuten HR- ja talousyksiköt ja virastopalveluihin luettavat postitus-, aula- ja kokouspalvelut.

Sisäisten ja ulkoisten sidosryhmien luokittelu on joiltain osin välillä haastavaa, sillä digitaalinen perusta tarjoaa perustietotekniikan palveluita muille kaupungin hallintokunnille, ja on näin periaatteessa erillään muusta kaupunginkanslian organisaatiosta. Näin luokittelisin tietyissä tapauksissa esimerkiksi talousyksikön ulkoiseksi sidosryhmäksi (asiakkaaksi), kun taas tietyissä tapauksissa se toteuttaa digitaalinen perusta -yksikölle sisäisiä talouspalveluita, jolloin se on taas sisäinen sidosryhmä.

Selkeämpiä ulkoisia sidosryhmiä ovat erilaiset palveluntuottajat, mihin kuuluvat esimerkiksi laitetoimittajat, järjestelmien ylläpitäjät ja erilaiset konsulttipalvelut. Tämän lisäksi ulkoisiin sidosryhmiin kuuluvat muut Helsingin kaupungin organisaation osat asiakkaiden roolissa, eli toimialat, liikelaitokset ja virastot (hallintokunnat). Sekä asiakkaiden tarpeet että sisäisen kehityksen projektit ovat merkittävimmät omiin työtehtäviini vaikuttavat asiat. Sidosryhmät on kuvattu hyvin korkealla tasolla kuvassa 3.





Kuva 3. Sidosryhmät sisäisiin ja ulkoisiin sidosryhmiin eroteltuna.

2.3 Vuorovaikutustaidot työpaikalla

Työni on suurelta osin melko itsenäistä, ja merkittävimmät vuorovaikutustilanteet ovat viimeisen vuoden aikana liittyneet pikaviestimen (Microsoft Teams) kautta järjestettyihin kokouksiin tai puheluihin. Merkittävin syy tähän on käytännössä yhtäjaksoisesti jatkunut etätyö koronaviruspandemian seurauksena. Hyvin aikaisessa vaiheessa nykyisellä työnantajallani ollessa havaitsin kuitenkin sen, että erittäin merkittävä vuorovaikutuksen muoto työtovereiden kanssa on ns. "puskaradio", eli tiedon jakaminen päivittäisessä kanssakäymisessä työpaikalla luonnollisen keskustelun kautta ja esimerkiksi lounastauoilla. Tämänkaltaista luonnollista tiedonjakoa on paljon haastavampaa toteuttaa pikaviestinten kanssa, ja vuorovaikutus on rajoittunut lähinnä säännöllisiin yksikköpalavereihin, pikaviesteihin, sähköpostiin sekä puheluihin.

Asiakkaiden suuntaan vuorovaikutus on keskittynyt erilaisiin kokouksiin, joissa käydään pääsääntöisesti jotain tiettyä tarvetta tai mahdollisesti projektin etenemistä läpi. Tämän lisäksi digitaalisella perustalla on tietenkin erilaiset pysyvämmät tiedotuskanavat, kuten esimerkiksi Microsoft Teamsissä olevat kanavat, joilla tärkeitä muutoksia tai tiedotteita viestitetään asiakkaiden suuntaan. Erilaisissa asiakkaiden vuorovaikutustilanteissa koen tärkeäksi sen, että pystyn katselemaan tilannetta asiakkaan näkökulmasta, ja sovittamaan oman vuorovaikutukseni asiakkaan tarpeita parhaiten palvelevaksi. Aina tämä ei onnistu ensimmäisellä kerralla, sillä erilaisilla asiakkailla on erilaiset toiveet esimerkiksi teknisten yksityiskohtien seikkaperäisestä selostamisesta. Jotkut asiakkaat haluavat tunteen, että asia on hyvissä käsissä, kun taas toiset haluavat tietää mahdollisimman tarkasti, että mitä milläkin hetkellä tapahtuu.

Muiden ulkoisten sidosryhmien, kuten esimerkiksi palveluntarjoajien osalta, tulee taas pitää mielessä se, että minä toimin asiakkaan roolissa, kun taas sidosryhmän edustaja toimii myyjän tai palveluntoimittajan roolissa. Tämän pitäminen mielessä on silloin tällöin haastavaa, erityisesti jos vuosien kuluessa tiettyjen henkilöiden kanssa on syntynyt hyvä keskusteluyhteys. Näissä tapauksissa esimerkiksi palvelutason rikkomisesta reklamoinnin kynnys saattaa olla korkeammalla kuin mitä sen pitäisi olla, erityisesti jos se ei aiheuttanut kyseisessä tilanteessa merkittävää haittaa.

Osana pitkää työuraani nykyisellä työnantajalla olen kuitenkin ollut käytännössä jatkuvasti jonkinlaisessa asiakasrajapinnassa palveluntarjoajan roolissa, alkaen IT-tukihenkilön tehtävistä. Tämän takia erilaisissa vuorovaikutustilanteissa ilmenevät haasteet ovat useimmiten kertaluonteisia, ja kykenen sopeutumaan niihin pääsääntöisesti hyvin.

3 Päiväkirjaraportointi

3.1 Seurantaviikko 1

Maanantai 17.01.2022

Viikon ensimmäisenä päivänä kalenterista löytyy useampi kokous, jotka jo etukäteen vievät ajallisesti yli puolet päivästä. Näistä noin puolet ovat enemmän seurantatyyppisiä kokouksia, joissa käydään läpi projektien etenemistä ja niihin liittyviä kysymyksiä, kun taas toinen puolisko painottuu työstökokouksiin. Päivän tavoitteena on saada valmistauduttua erityisesti työstökokouksiin riittävästi, sekä edistää muulla ajalla käyttäjätunnushallinnan elinkaareen liittyvää dokumentaatiota, jota olen työstänyt jo aiemmin.

Kokoukset etenivät suunnilleen suunnitellusti. Aamun ensimmäinen tietoturvaan liittyvä kokous koski enemmän hallinnollisia asioita ja vastuunjakoja sidosryhmän kanssa, joten se ei vaatinut vielä osaltani aktiivista osallistumista, vain kuuntelua. Seuraavat kaksi kokousta käsittelivät erästä laajempaa datansiirtoprojektia, johon olen aikaisemmin rakentanut automaatiota. Kokouksissa ilmeni automaatioon lisäominaisuustarpeita ja niissä myös aikataulutettiin datansiirron aloittamista seuraavalle viikolle, mikä vaatii tältä viikolta ajankäyttöä. Päivän viimeinen kokous koski toimipisteisiin liittyvän tiedon ylläpitoa ja erityisesti useamman tietolähteen yhdistämistä. Tästä päästiin suunnilleen yhteisymmärrykseen niin, että siitä voidaan tehdä ehdotus jatkokäsittelyä varten. Loppupäivä meni sähköposteihin vastaamisessa, erääseen tietoturva- ja hallintaprojektiin liittyvien tietojen tiedusteluun sähköpostitse ja muutamassa ongelmassa avustamisessa kollegoiden kanssa. Käyttäjätunnushallinnan dokumentaatio jäi siis tavoitteista tekemättä, mutta varasin sille kalenterista erikseen aikoja vähemmän kokoustäytteisinä päivinä.

Tiistai 18.01.2022

Päivä on hyvin kevyt kokousten osalta, joten tavoitteena on edistää kesken olevia aiempia tehtäviä. Näitä ovat ainakin käyttäjätunnushallinnan dokumentaation kirjoittaminen, datansiirtoprojektin automaation muutostarpeiden suunnittelu ja toteutuksen aloittaminen, sekä HR-järjestelmän ja Active Directoryn välisen data-automaation toteutuksen edistäminen. Päivän aikana tavoitteena on myös tarkistaa kesken olevien palvelupyyntöjen tilanne.

Tämän päivän suunnitelma ei täysin toteutunut, sillä keskelle päivää tuli uutta toimipistettä koskeva suunnittelukokous, jossa käytiin läpi IT- ja muita tarpeita. Tämän lisäksi aamuisessa projektin seurantapalaverissa löytyi ongelma, joka pitää ratkaista jollakin tavalla

projektin vaatimusten täyttämiseksi. Kyseessä on tekninen ongelma liittyen siihen, miten älykorteilla kirjaudutaan Microsoftin Remote Desktop Gatewayn kautta RDP-yhteydellä RDS-palvelimelle. Tästä seurasi odottamatonta ongelmanselvitystä ja ratkaisun tai vastausten löytäminen voi vaatia yhteydenottoa Microsoftin asiantuntijoiden suunnalle, eli ongelma ei vielä ratkennut.

Tämän lisäksi datansiirtoprojektin aikataulu tarkentui siten, että kohtuullisen suuret datansiirrot alkavat seuraavalla viikolla, joten automaatioon tarvittavien muutosten teko nousi korkeammalle prioriteetille, että automaatio on kyseisten tarpeiden osalta valmis seuraavalla viikolla. Tästä huolimatta sain edistettyä dokumentaation kirjoittamista, vaikkakaan en aivan niin paljoa kuin oli tavoitteena. Edellä mainittujen asioiden lisäksi päivään sisältyi myös viikoittainen työasemaympäristöön liittyvä seurantakokous, jossa käydään läpi ajankohtaisia työasemiin ja niiden ylläpitoon liittyviä asioita. Rutiininomaisena näihin asioihin kuuluvat päivitysten seuraaminen, työasemaympäristöön liittyvistä laajoista muutoksista päättäminen, sekä tiedonjako digitaalisen perustan eri yksiköiden välillä. Tavoitteista palvelupyyntöjen sekä HR- ja AD-järjestelmien data-automaation edistäminen jäävät käytännössä seuraavalle päivälle, tosin palvelupyyntöjä sain tarkistettua sen verran, että kiireellisiä palvelupyyntöjä ei jäänyt tekemättä.

Ongelmanselvityksen takia päivän aikana tuli syvennettyä tietämystä RDP-protokollan toiminnasta Remote Desktop Gatewayn yhteydessä, ja siitä miten siihen liittyvä tietoturvaominaisuus NLA, eli Network Level Authentication, toimii taustalla. Tämän lisäksi sain luettua hieman datansiirtoprojektin automaatioon liittyvän tarpeen toteuttamisesta, mikä liittyy WPF-ikkunoiden (Windows Presentation Framework) elementtien tapahtumien laukaisemisesta Powershell-kielellä. Tähän voi kuulua esimerkiksi ikkunassa näkyvän napin painamisen simulointi ohjelmallisesti.

Keskiviikko 19.01.2022

Päivän alussa kalenterissa on vain kaksi kokousta, joista toinen on säännöllinen tiimipalaveri ja toinen on tiettyjen ylläpito-oikeuksien käyttöön liittyvä ongelmanselvityskokous. Loppuajan päivästä olen suunnitellut käyttäväni jo edellisinä päivinä mainittuun käyttäjätunnushallinnan ohjeistuksen ja datansiirtoprojektin automaation työstämiseen. Kumpikaan ei todennäköisesti valmistu vielä tänään, paitsi jos kaikki menee hyvin ja yllättäviä ongelmia ei synny. Tavoitteena on kuitenkin saada kumpikin sen verran valmiiksi, että pystyn viimeistelemään ne viimeistään seuraavana päivänä.

Päivän tavoitteista sain edistettyä melkein suunnitelman mukaisesti käyttäjätunnushallinnan ohjeistusta, mutta olin tavoitteissani taas ylioptimistinen. Päivän aikana tuli pari palvelupyyntöä ratkaistavaksi, ja iltapäivän ongelmanselvityskokouksesta tuli myös hieman ylimääräistä tehtävää. Ongelmanselvityksestä nousi tarve erilaisten vanhempien skriptien kokoamisesta yhteiseen sijaintiin, josta ne ovat kaikkien digitaalisen perustan henkilöiden hyödynnettävissä. Tästä käytiin jonkin verran keskustelua, ja keskustelussa nousi esille esimerkiksi tarve huomioida versionhallinta ja selkeät pelisäännöt, joilla yhteiset skriptit saatetaan kaikkien saataville ja niitä kehitetään. Omalta osaltani en erittäin lyhyellä aikavälillä ehdi syventyä asiaan johtuen aiempina päivinä mainitsemistani projekteista, mutta se voi olla mahdollinen kehityskohde joidenkin viikkojen jälkeen. Datansiirtoprojektin automaation työstäminen jäi pahasti jälkeen tavoitteesta, ja se onkin seuraavien päivien pääprioriteetti, sillä muutosten tulee olla tuotantovalmiita seuraavan viikon alkupuolella. Pääpiirteittäin päivän työtehtävät olivat rutiininomaisia ja eivät vaatineet muuta kuin referenssimateriaalin tarkastelua ja tiedossa olevan prosessin tuottamista luettavaan muotoon.

Torstai 20.01.2022

Päivästä on taas varattu leijonanosa erilaisille kokouksille ja päivä jakautuu käytännössä tyhjään aamupäivään ja kokousputkeen puolestapäivästä päivän loppuun asti. Aamupäivän olen varannut etukäteen data-automaation muutosten toteuttamiselle ja jos aikaa jää jäljelle, käyttäjätunnushallinnan ohjeistuksen jatkamiseen. Kokousten aiheet ovat hyvin vaihtelevia, ja liittyvät erään hallintokunnan datasiirron aikataulukseen ja teknisiin kysymyksiin, Microsoftin Power BI -työkalun käyttämän datan tietosuojan varmistamiseen ja käyttäjätunnushallinnan ohjeistuksen läpikäyntiin. Tämän lisäksi mukana on yksi laajempi työpaja, jossa käsitellään laajempaa organisaatiouudistusta liittyen in-house-yhtiön perustamiseen. Yöllä on myös poikkeuksellisesti normaalin työajan ulkopuolista työtä johtuen tietoliikennemuutoksesta, joka koskee myös tiettyä palvelinjoukkoa. Käytännössä yöllä pitää varmistaa, että palvelinten verkkoyhteydet toimivat odotetusti muutoksen jälkeen.

Tällä kertaa päivän tavoitteet toteutuivat hyvin. Data-automaation muutokset olivat vähemmän työläitä kuin olin arvioinut, ja sain ne testattua ja siirrettyä tuotantoon aikataulussa viikonloppua ja seuraavaa viikkoa varten. Automaatioon liittyy vielä joitakin tarvittavia ominaisuuksia mutta niiden toteutus ei ole yhtä aikakriittistä, ja niitä tarvitaan vasta parin viikon päästä. Kokoukset sujuivat pääosin odotetusti, ja niistä ei vielä syntynyt itselleni uusia tehtäviä, vaan Power BI -kokouksessa toimin lähinnä teknisenä asiantuntijana vastaten alustaan liittyviin teknisiin kysymyksiin. Datansiirtopalaverista syntyi rutiininomainen tehtävä kyseisen hallintokunnan pilottisiirtojen aloittamiseksi, mutta se ei ole työläs.

Käyttäjätunnushallinnan ohjeistuksen läpikäyntipalaverissa nousi esille AD-ympäristön kehittäminen siten, että toimenpiteiden ja hyväksynnän hankinta voitaisiin automatisoida mahdollisimman pitkälle. Tästä nousi tehtäväksi automaation prosessien kuvaaminen, johon toivottavasti saan varattua vapaata aikaa, sillä nykyään suuri osa asioista on manuaalista työtä ja dokumentoinnin löytäminen voi tietyissä tapauksissa olla haasteellista. Sain päivän aikana myös suljettua joitakin vanhempia palvelupyyntöjä, sekä toteutettua erään kollegoiden työtä helpottavan skriptin.

Päivän työtehtävät ammensivat lähinnä olemassa olevasta tiedosta ja osaamisestani, ja en joutunut hakemaan merkittävästi uutta tietoa. Illan verkon yliheitosta johtuvan testaamisen aikana sain kuitenkin seurattua datansiirtoa, ja pyrin hankkimaan tietoa siirtonopeuden optimoinnista. Tähän liittyvät erityisesti käytössä olevien säikeiden määrä, sillä liian suuri määrä säikeitä voi aiheuttaa siirron hidastumista, kun säikeet taistelevat rajallisista levyresursseista. Päivän aikana sain myös syvennettyä ymmärrystä tiistaina mainitsemaani RD Gatewayhin liittyen, ja aiempi teoria NLA:n osuudesta ongelmassa osoittautui todennäköisesti vääräksi. Ulkoisen palveluntarjoajan konsultin avulla löytyi toimiva ratkaisu, joka testien perusteella näyttäisi toteuttavan ympäristöön liittyvät tarpeet.

Perjantai 21.01.2022

Viikon viimeisenä päivänä ei ole yhtä lyhyttä ongelmanselvityspalaveria lukuun ottamatta mitään kiinteitä rajoitteita ajankäytölle. Päivän tavoitteina on edistää HR-järjestelmän ja Active Directoryn välistä dataintegraatiota, sekä jatkaa käyttäjätunnushallinnan ohjeistuksen kirjoittamista. Kumpikaan tavoitteista ei todennäköisesti tule vielä tämän päivän aikana valmiiksi, mutta pidemmän ajan tavoite on saada molemmat valmiiksi seuraavan viikon aikana. Päivän aikana pitää myös tiedottaa tukipalveluita ja service deskiä seuraavalla viikolla käynnistyvistä tuhansien käyttäjätunnusten datasiirroista, mistä voi seurata joitakin ylimääräisiä tukipyyntöjä ja ohjeistuksen tarvetta. Mahdollisten tarpeellisten ajattelutaukojen osalta pyrin tutkimaan vanhempia osoittamattomia tukipyyntöjä ja saamaan niitä suljettua.

Päivä sujui täysin suunnitelman mukaisesti, ja sain edistettyä hyvin HR-järjestelmän ja Active Directoryn välistä dataintegraatiota. Käytännössä työstettävänä olevan skriptin tavoitteena on se, että HR-järjestelmässä olevat tiedot ovat henkilöiden AD-tunnuksissa vastaavalla tavalla ja että AD-tunnuksien muutoksien teko manuaalisesti pystyttäisiin minimoimaan. Käyttäjätunnushallinnan ohjeistus ei ole yhtä korkealla prioriteetilla, joten siihen en saanut käytettyä yhtään aikaa. Päivän mittaan sain myös suljettua joitakin vanhoja ilman vastuuhenkilöä olevia palvelupyyntöjä. Päivällä oli yksi hieman pidempi

ongelmanselvitystuokio kahden kollegan kanssa liittyen Onedrive-pilvitallennustilan toimimattomuuteen. Kyseisessä ongelmassa ratkaisuna oli poistaa Onedrive ja luoda se uudelleen, sillä vuosien takaisten tunnusmuutosten takia henkilön Onedrive oli sotkeutunut kahden eri henkilöllä olleen tunnuksen välillä tehden siitä käyttökelvottoman. Ongelma olisi todennäköisesti ollut ratkaistavissa myös ilman datan katoamista, mutta koska dataa ei tarvinnut säästää, oli tämä selkein ja varmin ratkaisutapa muutaman aiemman epäonnistuneen korjausyrityksen jälkeen.

Viikkoanalyysi

Ensimmäisellä raportointiviikolla työtehtävät keskittyivät melko pitkälti neljään eri projektiin. Muut työtehtävät olivat enemmän kertaluonteisia ja pohjautuivat aiempaan kokemukseen ja tietoon, joten ne eivät tällä viikolla vaatineet merkittävää osaamisen kehittämistä tai asiaan perehtymistä. Viikon keskeisimmät työtehtävät liittyivät seuraaviin kokonaisuuksiin:

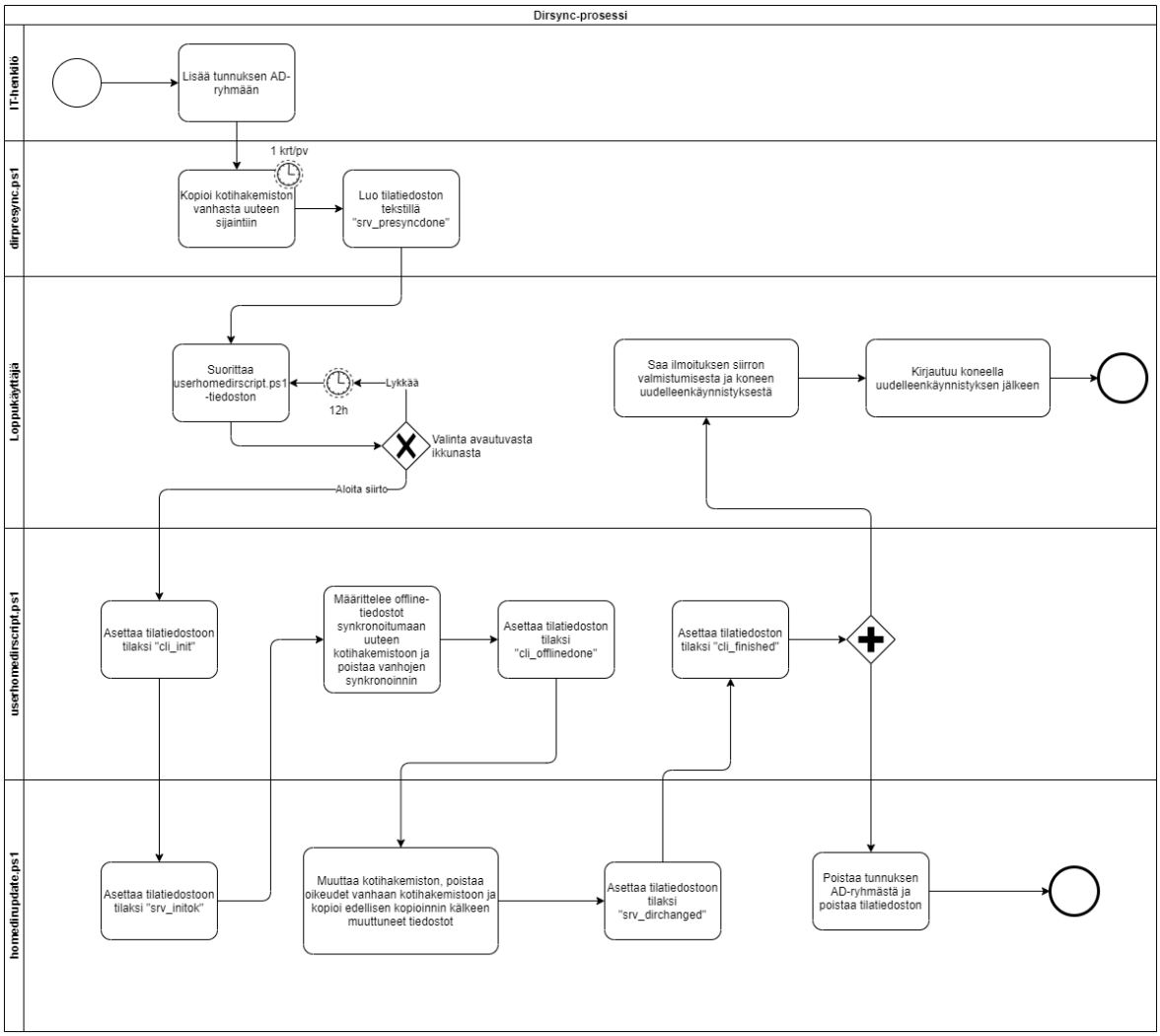
- Datansiirtoprojektin siirtoautomaation kehittäminen ja toteutus
- RDS-hallintaympäristöprojekti, jossa pyritään parantamaan ylläpitotunnusten tietoturvaa
- HR-järjestelmän ja Active Directoryn välisen dataintegraation toteuttaminen
- Käyttäjätunnushallinnan elinkaaren ja käytäntöjen dokumentointi

Keskityn tässä viikkoanalyysissä kahteen ensimmäiseen, sillä käyttäjätunnushallinnan elinkaaren dokumentointi on pitkälti todetun nykytilan kuvaamista ja HR-järjestelmän ja Active Directoryn dataintegraatio koostuu lähinnä skripteistä, jotka automatisoivat ns. master datan tuomisen Active Directoryyn, jota käytetään useissa järjestelmissä kertakirjautumiseen sekä henkilön perustietojen tuomiseksi kyseiseen järjestelmään. Keskeisin ongelma, eli Active Directory -tunnuksen ja HR-järjestelmän käyttäjän yhdistäminen toisiinsa on mahdotonta automatisoida täydellisesti, sillä niillä ei ole yksiselitteistä yhdistävää tekijää. Organisaatio on niin laaja, että samannimisiä henkilöitä on organisaatiossa useampi. Tällä viikolla edistyminen ja tehtävän ajankäyttö oli kuitenkin suhteellisen vähäistä, ja tämän takia en tässä viikkoanalyysissa keskity kyseiseen työtehtävään tarkemmin.

Datansiirtoprojektiin taas kului huomattavasti enemmän aikaa, johtuen sen ajankohtaisuudesta. Projektissa omana teknisenä osa-alueenani on käyttäjien ns. kotihakemistojen, eli henkilökohtaisten tiedostojen siirto vanhoilta palvelinalustoilta uusille. Haastavan tästä osiosta on tehnyt se, miten Windows-käyttöjärjestelmässä käsitellään kotihakemiston muutokset, kun kansioiden uudelleenohjaus (folder redirection) on käytössä. Käytännössä

tietokoneelle kirjauduttaessa kansioiden uudelleenohjauksen muutokset tulevat voimaan vain, jos tietokoneella on yhteys toimialueen ohjauskoneeseen. Tätä ei sanota aivan suoraan Microsoftin dokumentaatiossa mutta kun löytää hieman vanhemmasta CSE-dokumentaatiosta (client side extension) kansioiden uudelleenohjausta koskevan osan, siinä mainitaan, että kyseinen toiminto vaatii synkronisen prosessoinnin (Microsoft 2019). Covid 19-pandemian takia suuri osa työntekijöistä tekee kuitenkin etätöitä, ja VPN-ratkaisun takia yhteyttä toimialueen ohjauskoneelle ei ole mahdollista saada ennen tietokoneelle kirjautumista. Tämän seurauksena kansioiden uudelleenohjauksen muutokset vaativat työpisteellä käyntiä.

Microsoftin dokumentaatiosta löytyy ohjeistus sille, miten kansioiden uudelleenohjauksen voisi muuttaa ilman erikoistyökaluja. Ohjeessa vaaditaan kuitenkin huomattavasti käyttäjäinteraktiota, sekä koordinaatiota muutoksen teon ajankohdan ja työpaikalla käymisen kanssa (Microsoft 2021). Pandemian takia liian monen henkilön yhtäaikaista paikallaoloa on tullut välttää ja tämän seurauksena kyseiseen koordinointiin käytettävät henkilöresurssit olisivat olleet suuria. Siirrettäviä kotihakemistoja, ja siten koordinoitavia työpaikalla käyntejä, on kymmeniä tuhansia ja dataa kymmeniä teratavuja. Siirtoautomaatio on käytännössä erillisratkaisu, joka automatisoi datan siirron ja kansioiden uudelleenohjauksen muutoksen niin, että se tapahtuu, kun kukin henkilö on käymässä työpaikalla. Kuluneen viikon aikana olen viimeistellyt työkalun käyttöön liittyviä viimeisiä toiminnallisuuksia ja ensimmäiset laajemmat siirrot alkavat seuraavalla viikolla. Tuolloin on tärkeää seurata työkalun toimintanopeutta, ja sitä skaalautuuko se tuhansiin samanaikaisiin kotihakemistosiirtoihin. Automaatio on toisaalta suunniteltu niin, että siitä voi luoda useampia instansseja eri palvelimille suorittamaan siirtoja rinnakkain, mutta ei ole varmaa tarvitseeko kyseistä optiota ottaa käyttöön. Tämä selviää viimeistään seurantaviikolla 3, kun suurin massa otetaan edeltävänä viikonloppuna käsittelyyn. Kuvassa 4 on prosessikaavio automaation toiminnasta.



Kuva 4. Dirsync-kotihakemistosiirtoautomaation prosessikuvaus.

RDS-hallintaympäristöprojekti on toinen projekti, jossa olen teknisessä vastuussa työpaikkani puolelta. Kyseisessä projektissa tosin koko järjestelmän suunnittelu on toteutettu hankintana, ja oma roolini on sovittaa järjestelmän toiminta ja jatkokehitys työpaikan tarpeisiin. Kyseisessä projektissa pyritään parantamaan ympäristön tietoturvaa mahdollistamalla ja myöhemmin pakottamalla ylläpitotunnuksille MFA (Multi-factor authentication) eli monivaiheinen tunnistautuminen, ja parantamalla ylläpitotunnusten identiteetinhallintaa ja toimenpiteiden lokittamista. Käytännössä projektissa pyritään toteuttamaan Microsoftin aiempaa moniportaista hallintamallia, mutta siinä huomioidaan myös tästä kehitetty modernimpi hallintamalli, joka huomioi myös erilaiset pilvipalvelut. Microsoftin dokumentaatiossa vanhempi malli kulkee nimellä "legacy tier model", kun taas modernimpi versio tästä on "enterprise access model" (Microsoft 2021b). Projektin yhteydessä on myös huomioitu muita moderneja tietoturvasuosituksia, kuten esimerkiksi salasanakäytäntöjen muuttaminen. Yhtenä esimerkkinä on salasanojen vanhentumisen poistaminen käytöstä, joka mainitaan esimerkiksi julkaisussa NIST (2017, 14).

Molemmat projektit ovat olleet jo pidempään käynnissä mutta odotettavissa on, että niihin palataan jatkuvasti seurantajakson aikana. Tämän takia olen kuvannut niiden sisältöä laajemmin kuin mitä kuluneen viikon aikana on yksinään tapahtunut. Kokonaisuutena ensimmäinen seurantaviikko on ollut melko rutiininomainen ja suurin osa työtehtävistä ei ole vaatinut merkittävää kehittymistä tai pohdintaa. Viikon aikana tuli kuitenkin esille pari asiaa, jotka liittyvät ns. master datan käsittelyyn ja hallintaan. Näitä ovat HR-järjestelmän ja AD-ympäristön välinen integraatioautomaatio, sekä toimipisteisiin liittyvän datan ylläpito ja ylläpitovastuut. Tähän liittyen olen jo alustavasti tehnyt joitakin tietohakuja, mutta en vielä saanut tutustuttua kattavasti erilaisiin parhaisiin käytäntöihin ja näihin asiaankuuluviin toimintamalleihin. Aiheeseen syvällisempi tutustuminen jää todennäköisesti seuraavalle kahdelle viikolle edistettäväksi, vaikka aiemman kokemukseni perusteella koen olevani jokseenkin perillä aihealueesta. Tästä huolimatta kyseisenlaisen datan ajantasaisena pitämisessä tuntuu aina olevan ongelmia, joten keskityn tiedonhaussa erityisesti tuohon näkökulmaan parhaiden käytäntöjen osalta.

Käyttäjätunnushallinnan dokumentoinnissa päivitin olemassa olevaa dokumenttia nykyisten prosessien ja käytäntöjen mukaiseksi, joten siinä ei varsinaisesti suunnitella uusia prosesseja. Tietyt osa-alueet voivat kuitenkin vaatia lähdekirjallisuuteen tutustumista, sillä pohjana käytetty dokumentti on jo noin kymmenen vuotta vanha ja jotkin myöhemmät osiot, joihin en ole vielä ehtinyt paneutua kunnolla, voivat vaatia modernien vaatimusten tarkistamista. Esimerkiksi EU:n yleistä tietosuoja-asetusta (GDPR) ei alkuperäisen dokumentin tekohetkellä ollut olemassa, ja siihen voi olla aiheellista tehdä tietyissä kohdissa viittauksia.

3.2 Seurantaviikko 2

Maanantai 24.01.2022

Suunnittelin pitäväni hieman lyhyemmän päivän kertyneiden saldotuntien poispitämiseksi. Joka tapauksessa päivään kuuluu kiinteinä menoinen taas useampi kokous, ja näihin kuuluvat kulunvalvontajärjestelmään liittyvä palaveri, datasiirron aikataulutuksen palaveri, PowerBI-palvelutunnuksen tekemiseen liittyvä palaveri, kuin myös viikoittainen sisäinen ITSM-palaveri. Jäljelle jäävänä aikana suunnittelen edistäväni edellisellä viikollakin mainitsemiani asioita, mutta maanantaisin tulee yllättävän usein kiireellisempiä asioita esille, jotka saattavat taas puskea muita asioita myöhemmäksi.

Päivä sujui suunnilleen odotusten mukaisesti. En päässyt juurikaan jatkamaan viime viikon rästiin jääneitä työtehtäviä, sillä kokouksista syntyi taas uusia tehtäviä.

Kulunvalvontakokouksesta syntyi kiireaikataululla verkkotarpeiden ja palvelimen saatavuuden selvitystä, ja datasiirron aikataulutuskokouksessa selvisi yksi tärkeä ominaisuus datasiirtoautomaatiolle, joka olisi hyvä saada toteutettua mahdollisimman nopeasti. Tämä liittyy siirron aloituksen pakottamiseen, että käyttäjät eivät lykkää siirron aloittamista ikuisesti. Tämän lisäksi autoin paria kollegaa, työstin paria palvelupyyntöä ja sain myös toimeksiannon suodattaa HR-datasta organisaation nimikkeet ja niiden lukumäärät seuraavaksi päiväksi. Päivän tehtävät olivat siis käytännössä rutiininomaisia, ja eivät vaatineet uuden tiedon hakemista tai omaksumista.

Tiistai 25.01.2022

Päivä on kokousten osalta melko tyhjä, ja tavoitteena on saada HR-järjestelmän ja AD:n välinen integraatio siihen kuntoon, että sillä voi päivittää AD-dataa kunnolla. Täysautomaattiseksi en sitä vielä kuitenkaan saa, sillä tietojen yhdistämisessä on aina jokin virheprosentti, jos niillä ei ole ennestään yhdistävää tekijää. Keskiviikkona on kuitenkin tähän liittyvä kokous, joten automaation olisi hyvä olla sellaisessa kunnossa, että näihin kysymyksiin voi pohtia vastauksia. Tämän päivän kokoukset ovat viikoittaisia kokouksia, liittyen RDS-hallintaympäristöön ja työasemaympäristöön yleisemmin.

Päivän tavoitteet täyttyivät, ja yhtä yllättävää kokousta lukuun ottamatta suuria yllätyksiä ei tapahtunut. Aamupäivästä sain edistettyä integraatiota, joka koostuu siis Powershell-skripteistä. Käytännössä ongelmallisin osuus on HR-järjestelmän ja AD-tunnuksen yhdistäminen yhteisellä tunnisteella, koska tätä ei voi tehdä automaatiolla luotettavasti. Varsinaiset automatisoitavat asiat ovat kuitenkin tästä riippuvaisia, joten olen vielä toistaiseksi keskittynyt siihen, miten kyseisen yhdistämisen saa tehtyä manuaalisesti mahdollisimman tehokkaasti. Ennen huomista kokousta alan käydä massaa hiljalleen läpi tunnisteiden saattamiseksi kohdilleen. Dataa läpikäymällä saa myös ns. huomioitavia reunatapauksia selville, ja se voi selventää myös ongelmia nykyprosesseissa, esimerkiksi jos henkilöllä ei ole tunnusta tai henkilöllä on jostain syystä useampia tunnuksia.

RDS-hallintaympäristökokouksessa taas päästiin lähemmäs projektin viemistä maaliin, kun päästiin tiettyjen toiminnallisuuksien toteutuksesta yhteisymmärrykseen selkein etenemisaskelin. Tämä oli vaatinut tarkempaa tutustumista Microsoftin JEA-dokumentaatioon (Just Enough Administration) sekä omalta että ulkoisen palveluntarjoajan asiantuntijan puolelta, mutta ymmärsimme asian samalla tavalla ja päädyimme yksinkertaiseen ratkaisuun. Jos ympäristön käyttöoikeuksien roolitus monimutkaistuu ja se alkaa vaikuttaa hallittavuuteen on myös tiedossa, miten teknistä mallia voi muuttaa. Tämä vaatii kuitenkin sen verran kehitystyötä, että sitä ei kannata tehdä vielä tässä vaiheessa ennakoivasti. Itselleni

syntyi tästä taas lisää tulevia työtehtäviä, joihin liittyy Powershell-moduulin rakentaminen sekä ympäristön dokumentointi niin, että sitä pystyy hyödyntämään mahdollisimman tehokkaasti. Tekninen dokumentaatio tietenkin on olemassa ja sitä ylläpitää ympäristöä ylläpitävä palveluntarjoaja, mutta se ei ole varsinainen käyttöohje.

Datansiirtoihin liittyen löytyi myös eräs ongelma, mutta lokeja tutkiessa sille ei löytynyt selkeää syytä. Ongelmalla ei ole käyttäjänäkyvyyttä ja se ei vaikuta siirtojen onnistumiseen, mutta käytännössä vanhassa sijainnissa olleiden kotihakemistojen uudelleennimeäminen epäonnistuu korkealla prosentilla. Uudelleennimeämistä tarvitaan lähinnä siihen, että siirretyt kansiot on helppo tunnistaa myöhempää poistoa varten. Tähän on kuitenkin nopeampaa tehdä vaihtoehtoinen ratkaisu kuin alkaa selvittämään ongelman juurisyytä. Tässä tapauksessa vaihtoehtoisratkaisuna on sijoittaa vanhojen sijaintien kansioiden sisään tiedosto, josta ilmenee siirron tapahtuminen ja sen ajankohta.

Keskiviikko 26.01.2022

Keskiviikkona ei ole kovin montaa kiinteästi aikataulutettua asiaa, lukuun ottamatta HR-järjestelmän integraatioon ja uuteen HR-järjestelmään liittyvä kokous, sekä toinen ajankohtaisia asioita käsittelevä kokous. Aamupäivällä suunnittelen jatkavani HR-datan ja AD:n integraation tekoa, ja seuraan miten datansiirrot edistyvät. Tarkoituksena on myös alkaa tehdä manuaalista vertailua ja alkaa saattaa tunnisteita kohdalleen. Tämä tulee jatkumaan pienissä pätkissä toistaiseksi, sillä minkäänlaisen automaation pohjalla on pakko olla luotettavat tunnisteet ja myös prosessi niiden pitämiseksi luotettavina. Toivon myös ehtiväni toteuttamaan datansiirtoautomaatioon liittyvän ominaisuuden, ja vieväni sen tuotantoon.

Aamupäivä meni suunnilleen odotusten mukaan ja sain täytettyä tavoitteet HR-järjestelmän ja AD:n välisen automaation osalta. Sain myös käytyä läpi useamman sata tunnusta, joilla oli duplikaattitunnisteet, eli sama tunniste oli useammalla tunnuksella. Tunnusten läpikäynnin aikana kehitin myös työkalua edelleen, minkä takia siihen meni odotettua enemmän aikaa. Ikävänä yllätyksenä aamupäivällä selvisi, että aiemmin mainittu kulunvalvontaan liittyvä palvelin vaatii sellaisen Linux-alustan, mitä ei löydy suoraan palveluntarjoajan valikoimasta, eli tästä pitää järjestää kokous asian selvittämiseksi.

HR-järjestelmään liittyvässä kokouksessa syntyi paljon kysymyksiä uuden HR-järjestelmän määrittelyyn liittyvistä asioista, ja kokouksen jälkeen sain kyseisiä määrittelydokumentteja katselmoitavaksi. En ehtinyt tutustua niihin vielä tänään, mutta tavoite on saada ne katselmoitua ainakin sillä tasolla, että näen, onko niihin kommentoitavaa. Päivän

aikana ratkaisin myös muutaman palvelupyynnön ulkoisten konsulttien tunnuksiin liittyen, sillä ne tarvittiin kiireellisesti toimintaan.

Datansiirtoautomaatio synnytti jonkin verran selvitystyötä, sillä datansiirroissa löytyi muutama reunatapaus, jotka aiheuttivat epäonnistumisia kotihakemistojen muutoksessa. Prosentuaalisesti tapauksia ei ollut paljoa ja ne eivät aiheuttaneet muuta haittaa kuin datansiirron viimeistelyn estymisen. Pienikin prosentti aiheuttaa kuitenkin paljon tukipyyntöjä ja manuaalista työtä, jos kokonaisuutena käsitellään kymmeniä tuhansia hakemistoja. Lokien tutkimisesta löytyi joitakin outoja verkko-ongelmia, joiden seurauksena automaatio luuli pääsyn uuteen sijaintiin puuttuvan, minkä takia siirtoa ei saanut viimeisteltyä. Tämän lisäksi oli joitain tapauksia, joissa tilatiedostoon oli syntynyt tyhjä merkintä varsinaisen tilan sijasta. Tapausten ollessa näin harvinaisia juurisyiden löytäminen voi olla vaikeaa, ja tämän takia lisään tarkistuslogiikkaan vaihtoehtoisia tarkistustapoja sillä oletuksella, että ongelma liittyy käytettyyn funktioon, eikä henkilön tietokoneen tilaan. Tilannetta pitää kuitenkin seurata tarkasti seuraavina päivinä, sillä koronapandemian takia työntekijät saattavat käydä toimistolla jonain päivänä varta vasten datansiirron suorittamiseksi, ja jos se epäonnistuu tai ei ala odotetusti, saatetaan tarvita uusi käynti toimistolla. Automaation tavoitteena on minimoida datansiirroista sekä IT-hallinnolle että käyttäjille aiheutuva vaiva ja ajankäyttö.

Torstai 27.01.2022

Tälle päivälle on jo etukäteen varattu paljon kokouksia, joten aikaa muiden työtehtävien edistämiselle ei ole suhteessa kovin paljoa. Työtehtävistä keskityn data-automaation tilanteen seuraamiseen ja mahdollisten korjausten toteuttamiseen ennen viikonlopun massasiirtoja. Toissijaisena, jos aikaa jää, jatkan HR- ja AD-datan integraatiota. Kokoukset ovat rutiininomaisia, mutta päivän viimeisenä kokouksena on RDS-hallintaympäristön ohjausryhmä, johon on useampia asioita vietävänä päätettäväksi. Se vaikuttaa myös tulevien viikkojen työtehtäviin kyseisen projektin osalta.

Päivä eteni kokousten osalta odotetusti, ja mitään ihmeempiä yllätyksiä ei sattunut. Ohjausryhmästä saatiin tarvittavat päätökset RDS-hallintaympäristöprojektin etenemiseen. Muista päivän työtehtävistä syntyi yllättävä onnistuminen, koska spekulaatiot edellisenä päivänä ilmenneistä datansiirtoautomaation tilatiedostojen tyhjistä merkinnöistä osoittautuivat oikeaksi. Juuriongelmana on se, että tiedostojen muokkaus ei ole atominen operaatio, vaan se koostuu useammasta operaatiosta, jotka tässä tapauksessa ovat tiedostojen tyhjennys ja sitten uuden datan kirjoittaminen. Tilatiedostoa seurataan viiden sekunnin välein, ja jos luku sattuu juuri tyhjennyksen ja kirjoituksen väliselle ajanhetkelle, näkee

automaatio tiedoston sisällön tyhjänä. Ratkaisuni tähän on se, että automaatio jättää lyhytaikaiset tyhjät arvot huomiotta, jolloin seuraavalla lukukerralla luetaan oikea arvo. Toisena ratkaisuna taata tiedoston kirjoitus atomisena operaationa olisi kirjoittaa data toiseen tiedostoon, ja sitten poistaa aiempi tiedosto ja uudelleennimetä uusi tiedosto vanhan nimellä. Tämä tosin on monimutkaisempi ratkaisu toteuttaa ja ei mielestäni tarjonnut lisäarvoa toteutuneelle ratkaisulle.

HR- ja AD-datan integraatio eteni myös, ja sain edistettyä datan läpikäyntiä. Dataa läpikäydessä on myös syntynyt joitain havaintoja, joita voin hyödyntää varsinaisissa automaattisissa käsittelyalgoritmeissa myöhemmin, kunhan toteutuksessa edetään sinne asti.

Perjantai 28.01.2022

Aamun tavoitteena on saada käyttäjätunnushallinnan elinkaaridokumentaatio valmiiksi tai miltei valmiiksi. Päivän aikana on lisäksi taas useampi kokous, tosin suurin osa päivästä on vapaina kesken jääneiden muiden työtehtävien hoitamiselle. Kokoukset liittyvät kulunvalvontajärjestelmän palvelinhankintaan, edellä mainitun dokumentaation läpikäyntiin, sekä tietojenluokittelun kohdistamisen teknisen ratkaisun suunnitteluun. Päivällä on myös joka toinen viikko pidettävä ITSM-järjestelmän kehitystarpeiden priorisointikokous, mutta se ja toinen kokous ovat päällekkäin, eli en välttämättä pääse osallistumaan siihen. Tulen päivän aikana myös seuraamaan datansiirtoprojektin etenemistä aktiivisesti ja erityisesti siirtopalvelimen kuormaa, sillä viikonloppuna samanaikaisten siirtojen määrä nousee 2000:sta 10000:een.

Aamulla sain kirjoitettua käyttäjätunnushallinnan elinkaaridokumentaatiota suurin piirtein odottamani verran. Joka tapauksessa tämä oli riittävästi, sillä sen läpikäyntikokouksessa ei saatu käytyä kaikkia muutoksia läpi varatussa ajassa siitä syntyneen keskustelun takia, joten sitä varten pitää varata vielä yksi kokous seuraavalle viikolle. Kaksi teknisempää palaveria, eli kulunvalvontajärjestelmän palvelimeen ja tietojenluokittelun tekniseen toteutukseen liittyvät kokoukset saatiin taas lopetettua etuajassa, sillä niissä ilmenneisiin kysymyksiin löytyi suorat vastaukset.

Päivän aikataulut menivät kuitenkin hieman sekaisin, sillä yhden henkilön datansiirrossa näytti siltä, että datan katoamista olisi tapahtunut ja tämän tutkimiseen meni jonkin verran aikaa. Datan katoamista ei kuitenkaan tapahtunut, vaan syyksi selvisivät epäjohdonmukaiset käyttöoikeuslistan merkinnät, joiden takia siirtoautomaatiolla ei ollut osaan tiedostokansioista käyttöoikeuksia. Kyseinen skenaario oli käynyt mielessä aiemmin automaatiota kehittäessäni, mutta siihen liittyvät tarkistukset olettivat, että koko tiedostokansion

käyttöoikeudet olisivat olleet puutteelliset, eivätkä vain joidenkin alikansioiden, joten automaation näkökulmasta ongelmaa ei ollut ja jotkin tiedostot jäivät vain kopioimatta. Varauduin tähän kuitenkin myös sillä, että lähdedataa ei poisteta siirron yhteydessä, vaan sen poistaminen tehdään myöhemmin osana eri prosessia, kun siirron onnistumiset on saatu todettua.

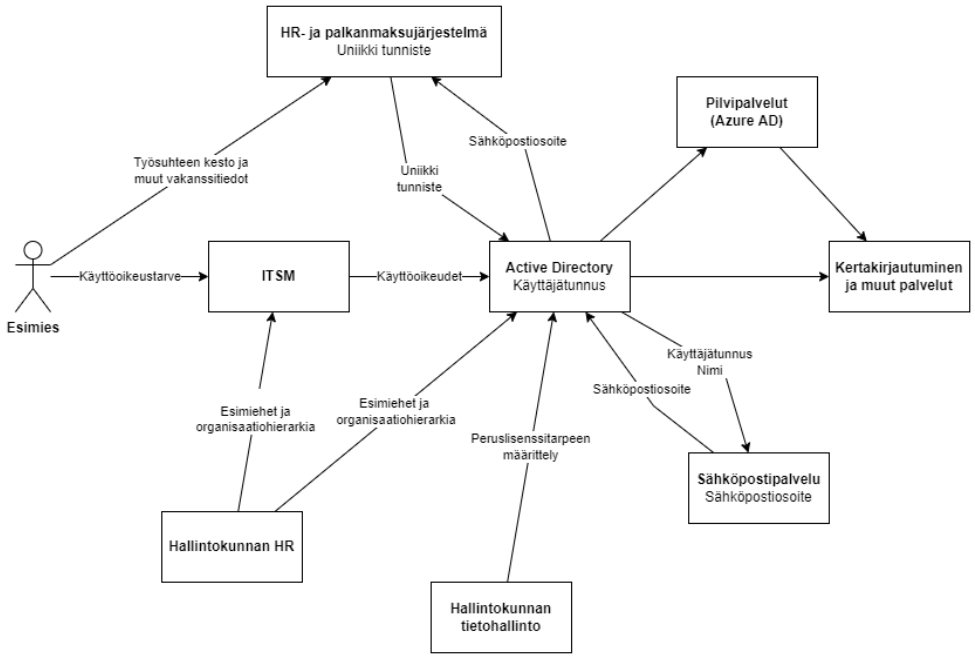
Olin myös tietoinen siitä, että Windows-käyttöjärjestelmässä on olemassa erityiset käyttöoikeustasot, SeBackupPrivilege ja SeRestorePrivilege, jotka mahdollistavat tiedostojen luvun riippumatta tiedostoissa olevista käyttöoikeusmäärittelyistä (Microsoft 2021c). Niiden hyödyntäminen vaatii kuitenkin ylimääräisiä käyttöoikeuksia ja yhtenä suunnittelufilosofiana oli niin sanottu vähimpien käyttöoikeuksien periaate (principle of least privilege). Tämä on ensimmäinen suurempi yksittäinen ongelma, joka datansiirrossa on tullut vastaan ja kyseiset tiedostokansiot on pääsääntöisesti luotu automaatilla, joka varmistaa kansioiden käyttöoikeuksien yhdenmukaisuuden. Tämän perusteella en siis vielä ole suunnittelemassa automaatioon muutoksia. Joka tapauksessa siirtopalvelimen kuorma oli päivän aikana sellainen, että siirrettävien kansioiden määrän viisinkertaistumisen ei pitäisi aiheuttaa tulevalla viikolla ongelmia.

Viikkoanalyysi

Kuluneella viikolla sain edistettyä useampia projekteihin liittyviä tehtäviä, joista merkittävimmät olivat datansiirtoautomaatio, RDS-hallintaympäristö ja HR- ja AD-järjestelmien integraatio. Datansiirtoautomaation osalta sain korjattua viikon aikana useampia virheitä, kuin myös haettua tietoa tietyistä siihen vaikuttavista teknisistä yksityiskohdista. Yksi liittyi tiedostokopiointien rinnakkaisajoon, eli kuinka montaa rinnakkaista kopiointia kannattaa suorittaa samanaikaisesti siirtonopeuden maksimoimiseksi. Tähän ei löytynyt täysin yksiselitteisiä vastauksia, mutta erilaisten yksittäisten internet-kommenttien perusteella sain arvioitua tälle todennäköisen ala- ja ylärajan. Tämän jälkeen kokeilin erilaisia vaihtoehtoja ja valitsin mielestäni sopivan, mutta varsinainen optimin löytäminen olisi tietenkin vaatinut enemmän testausta. Päädyin lopuksi 8 samanaikaiseen kopiointiin, joista jokainen käyttää 20 säiettä. Tiedostokopioinnissa syntyi myös hieman aiemman tiedon kertaamista, kun jouduin käymään perjantaina läpi epäonnistunutta tiedostokopiointia, siihen liittyneitä syitä ja miten ongelman olisi voinut estää. Käytännössä ongelman korjaamiseksi voin parantaa virheentarkistusta tai muuttaa automaation vaatimaan SeBackupPrivilege-oikeutta, jolloin tiedostokohtaisten käyttöoikeuksien puuttuminen ei aiheuta ongelmia. Tämä kuitenkin taas lisäisi merkittävästi automaatiotunnukselle myönnettäviä käyttöoikeuksia.

RDS-hallintaympäristöprojektissa käytiin läpi erityisesti JEA-ominaisuuteen liittyviä komentojen rajaamismahdollisuuksia, joita on kuvattu Microsoftin dokumentaatiossa (Microsoft 2021d). Kyseisestä dokumentista selvisi, että komentojen parametrien rajoittaminen onnistuu vain ennalta määrätyille merkkijonoille, ja niitä ei kyseisessä tiedostossa voi rajata dynaamisesti niin, että ne säilyisivät myös ylläpidettävinä ja käytettävinä. Tämän seurauksena päädyimme ns. wrapperiratkaisuun, jossa käyttäjän kutsuma funktio määritellään asiakasjärjestelmän puolella, ja se suorittaa tarpeelliset parametrien dynaamiset muokkaukset ennen varsinaisen JEA-funktion kutsumista. Toisena vaihtoehtona olisi ollut käyttöoikeustarkistuksen lisääminen JEA-funktion sisälle, mutta silloin olisimme joutuneet käytännössä toteuttamaan JEA-moduulissa: olemassa olevan roolipohjaisen käyttöoikeuksien hallinnan omatoimisesti funktion sisällä. Tämä olisi vaatinut huomattavasti enemmän työtä ja olisi sisältänyt riskin siitä, että oma toteutuksemme olisi ollut jollain tavalla haavoittuvainen ja siten vähemmän tietoturvallinen.

Viikon mielenkiintoisin aihe oli omasta mielestäni HR- ja AD-integraation edistäminen. Pääsin viikon aikana siihen pisteeseen, että pystyin vertailemaan ohjelmallisesti HR-järjestelmän ja AD:n välisen datan paikkansapitävyyttä. Pelkkiä uniikkiin tunnisteeseen liittyviä epäyhteneväisyyksiä löytyi tässä yhteydessä tuhansia. Organisaatio on sen verran laaja, että samannimisiä henkilöitä voi olla töissä jopa saman hallintokunnan sisällä, ja AD-puolen data voi olla vuosia vanhaa verrattuna HR-dataan. Tunnisteen päivittäminen vanhoilta tunnuksilta on siis käsityötä, mutta viikon aikana sain myös pohdittua koko prosessiin liittyviä ongelmia ydintietojen (master data) osalta. Tähän liittyy keskeisenä osana käsite ydintietojen hallinta (master data management, MDM). Kuvassa 5 on kuvattu tämänhetkisiä eri ydintietojen lähteitä organisaatiossa HR-datan ja AD:n näkökulmasta ja niiden datavirtoja.



Kuva 5. Merkittävimpien ydintietojen (master datan) lähteet ja datavirrat HR-järjestelmän ja AD:n näkökulmasta. Vahvennettu teksti kuvaa järjestelmää tai toimijaa, tavallinen teksti datavirran suuntaa tai sen lähdettä. ITSM = IT Service management, eli palvelunhallinta-järjestelmä.

Käytännössä AD toimii monissa tilanteissa henkilöihin liittyvien ydintietojen lähteenä, sillä esimerkiksi järjestelmien kertakirjautumiset on rakennettu joko ADFS-palvelun tai Azure AD:n kautta toimiviksi. AD-tietojen tulisi taas päivittyä HR-, ja palkanmaksujärjestelmästä, esimiesten toimittamista tiedoista, ITSM-järjestelmässä käsiteltävistä palvelupyynnöistä, ja nykytilanteessa myös itsepalveluna päivitettävistä tiedoista. Tietojenpäivitysprosessissa on aina manuaalisia työvaiheita, sillä itsepalveluna suoritettavissa päivityksissä syntyy aina joitakin virheitä ja ydintietojen muoto on hyvin löyhästi määritelty ja määrittelyt voivat vaihdella hallintokunnittain.

Ydintietojen hallinnan arkkitehtuurin suunnittelu on riippuvainen organisaatioon liittyvistä yksityiskohdista. Arkkitehtuurille ei ole yhtä selkeää mallia, joka sopii jokaiseen organisaatioon, vaan siinä tulee huomioida kunkin organisaation rakenne, tiedon hajautuminen ja heterogeenisyys, kuin myös ydintietojen hallintaan liittyvät organisatoriset ja tekniset tarpeet. (Otto 2012, 344.) Kyseinen tilanne käy ilmi myös kuvasta 5, sillä kuvassa mainittuja hallintokuntia ja siten HR- ja tietohallintoyksiköitä on organisaatiossa noin kymmenen, vaikka ne on mallinnettu vain yhtenä tekijänä. Kaikkea AD:n kannalta relevanttia tietoa ei viedä mihinkään keskitettyyn järjestelmään, vaan se pitää saada suoraan hallintokunnilta tarvittaessa. Tätä prosessia ei kuitenkaan ole millään tavoin automatisoitu ja tästä syystä

AD:ssa oleva tieto pääsee usein vanhenemaan ja se päivitetään vasta kun joku havaitsee puutteen.

Otto (2012, 341-342) tuo Boschin esimerkissä esille neljä erilaista arkkitehtuurin lähestymismallia, jotka määrittelevät miten tieto siirtyy järjestelmien ja MDS:än (master data server) eli ydintietojen hallintapalvelun välillä. Näistä malleista löytyy selkeitä yhtäläisyyksiä kuvan 5 tietovirtakaavion kanssa, ja käytännön eroina kahden parhaiten soveltuvan mallin välillä on se, että tuodaanko ydintiedot keskitetylle ydintietoalustalle ja käsitellään siellä yhdenmuotoisiksi (tutkimuksessa coexistence-malli), vai pilkotaanko käsittelyä lähemmäs toimintayksikköjä (parallel-malli). Oman näkemykseni mukaan organisaation rakenne ja sen eri tarpeet vaativat sitä, että ydintietojen käsittely on edelleen osittain hajautettua. Tässä tapauksessa on tärkeää, että IT-organisaation ja toimintayksiköiden välillä syntyy yhteistyötä ja ydintietojen vastuista on selkeä yhteinen näkemys (Otto 2012, 344).

Spruit & Pietzka (2015) käsittelee tutkimuksessaan eräänlaista ydintiedon hallinnan maturiteettimallia, ja pyrkii määrittelemään ydintiedon hallinnalle osa-alueita, joiden kautta hallintamallia voidaan edistää ja arvioida. Tämä koostuu viidestä eri osa-alueesta ja kolmestatoista eri yksittäisestä arvioitavasta kohteesta, jotka on kuvattu taulukossa 1.

Taulukko 1. MD3M-mallin osa-alueet ja arvioitavat kohteet (Spruit & Pietzka 2015, 1071, muokattu)

Data model	Definition of master data
	Master data model
	Data landscape
Data quality	Assessment of data quality
	Impact on business
	Reasons/sources for poor quality
	Improvement
Usage & ownership	Data usage
	Data ownership
	Data access
Data protection	Data protection
Maintenance	Storage
	Data lifecycle

Käytännössä kuvassa 5 kuvatun prosessin ydintietojen maturiteettitaso on erittäin alhainen, sillä monia maturiteettimallin osa-alueita ei ole määritelty tai edes vielä käsitelty.

Tämä maturiteettimalli kuitenkin kuvaa selkeämmän sekä prosessin, että ydintietojen käsittelylle ja ehkä vielä tärkeämpänä listaa asiat, jotka tulee huomioida projektin edetessä. Projektin aktiivisena tavoitteena ei kuitenkaan ole ydintietojen hallintamallin kehitys, mutta se on saatava tarpeeksi hyvin määritellyksi, että IT- ja HR-järjestelmien yhteensopivuus saadaan parannettua automatisoitavalle tasolle. Tähän liittyy osittain myös käyttäjätunnushallinnan elinkaaridokumentti, jota olen myös sivunnut päivittäisissä merkinnöissä. Kyseisessä dokumentissa määritellään tiettyjen käyttäjätunnuksen kenttien muotovaatimukset, ja tässä nouseekin nyt esille se, että todennäköisesti myös ydintietojen hallintaa ja erityisesti niiden lähteitä tulisi käsitellä kyseisessä dokumentissa muotoseikkojen lisäksi.

3.3 Seurantaviikko 3

Maanantai 31.01.2022

Maanantaina on muutama palaveri, joten valtaosa päivästä on vapaana muille tehtäville. Tänään on kuitenkin ensimmäinen päivä, jonka aikana viikonloppuna kopioituneiden noin 10000 kotihakemiston käyttäjät voivat viimeistellä siirron, joten olen varannut ainakin aamupäivästä aikaa siirtokuorman seuraamiselle, kuin myös mahdollisten ongelmien selvittämiselle. Muilta osin edistän HR- ja AD-integraation datan läpikäyntiä ja prosessin luonnostelua sekä käyttäjätunnushallinnan elinkaaridokumentaatiota, jos aikaa jää.

Aamupäivällä siirtojen etenemistä seuratessani havaitsin, että kuorma oli huomattavasti suurempi kuin mitä olin arvioinut edellisen viikon etenemisen perusteella. Pahimmillaan samanaikaisia prosesseja oli käynnissä noin 200, mikä aiheutti merkittävää kuormittumista lähdepalvelimen levylle. Tästä ei kuitenkaan aiheutunut nähtävästi merkittäviä käyttäjähaittoja, sillä kansioiden uudelleenohjaukseen liittyy myös offline-tiedostot-toiminto, joka ylläpitää paikallisia kopioita verkossa olevista tiedostoista. Jos siis palvelinjako hidastuu liikaa, siirrytään käyttämään paikallisia offline-kopioita, ja kun palvelin palaa toimintaan normaalisti, synkronoidaan muutokset takaisin verkkoon. Tämän ylikuormituksen olisi voinut välttää toteuttamalla rajoituksen samanaikaisten prosessien määrään, mutta koronaviruksen aiheuttaman etätyösuosituksen ja edellisen viikon kuorman perusteella en nähnyt sitä tarpeelliseksi. Lisäsin nyt ominaisuuden työlistalle, sillä kesää kohti mennessä etätyösuositustakin tullaan todennäköisesti purkamaan ja edessä on vielä samankaltainen määrä siirrettäviä kotihakemistoja.

Siirrosta syntyi myös jonkin verran tukipyyntöjä, mutta standardiratkaisut toimivat niihin. Siirtoja seuratessani havaitsin myös sen, että lähde- ja kohdepalvelinten tilankäyttö erosi toisistaan merkittävästi, mikä aiheutti myös tutkittavaa. Tälle löytyi kuitenkin selvä syy, eli

tiettyjä yhteiskäyttöisiä tunnuksia ei ollut otettu siirtoihin mukaan, joten tämä ei ollut siirtoautomaation virhetilanne. Muilta osin päivä oli suunnilleen odotusten mukainen, tosin näiden selvittelyjen takia en ehtinyt edistämään muita tehtäviä. Kulunvalvontaprojektin seurantapalaverissa syntyi myös verkkoarkkitehtuurin osalta lisäselvitystyötä, jota pitää pyrkiä edistämään mahdollisimman nopeasti.

Tiistai 01.02.2022

Päivälle on taas varattu reilummin kokouksia, mikä rajoittaa muiden työtehtävien edistämistä. Pyrin kuitenkin taas edistämään HR- ja AD-integraatiota, sekä käyttäjätunnushallinnan dokumentaatiota. Aamupäivällä seuraan taas datasiirtojen edistymistä mutta en odota, että siitä syntyy samanlaista kuormaa kuin maanantailta, joten seuraaminen on passiivisempaa. Kaksi päivän kokouksista liittyy datansiirtoprojektiin, toisessa suunnitellaan seuraavan hallintokunnan siirtojen aloittamista ja toisessa seurataan aiempien etenemistä. Kaksi muuta kokousta ovat viikkokokouksia, joista toinen koskee RDS-hallintaympäristöä ja toinen yleisemmin työasemaympäristöä.

Aamun siirtokuorma jäi noin puoleen maanantaisesta, joten en kokenut sen aktiivista seuraamista alun jälkeen tarpeellisena. Siirrosta syntyi kuitenkin tukipuolella kysymyksiä, ja myös tukipyyntöjä alkoi tulla jonkin verran enemmän siihen liittyen. Oletan että ohjeistuksessa vakioratkaisuna oleva koneen uudelleenkäynnistys ei ole optimaalinen toimintaohje, sillä uudelleenkäynnistyksen jälkeen verkkoyhteyden käynnistymisessä voi olla joidenkin sekuntien viive, erityisesti langattoman verkon osalta. Jos käyttäjä ehtii kirjautua sisään ennen verkkoyhteyden syntymistä ja tiettyjen palveluiden käynnistymistä, voi uuden kotihakemistosijainnin aktivoituminen epäonnistua kyseisessä kirjautumisessa. Tämän seurauksena muutan ohjeen niin, että siinä suositellaan vain ulos- ja sisäänkirjautumista, jolloin verkkoyhteys ei katkea ja sen käynnistymistä ei tarvitse odotella, ja mainitaan että tämä kannattaa tehdä kolme kertaa ennen yhteydenottoa tukipalveluihin. Lisääntyneet tukipyynnöt koskivat nimittäin yksinomaan sitä, että kotihakemisto ei toimi uudelleenkäynnistyksen jälkeen.

Datasiirtojen seuranta- ja suunnittelupalavereissa ei syntynyt mitään yllätyksiä, ja ne etenivät suunnitellusti. RDS-hallintaympäristöpalaverissa ei myöskään tapahtunut yllätyksiä, ja tietyt edellisen kokouksen jälkeiset asiat olivat edenneet odotetusti. Iltapäivän viikoittaisessa työasemien seurantakokouksessa ei niin ikään syntynyt yllätyksiä, tosin siellä keskusteltiin ryhmäkäytäntömuutosten hyväksymisprosessin muutoksesta. Tämä saattaa poikia joitain suunnittelukokouksia myöhemmin. Kyseinen vastuualue kuuluu kuitenkin eri tiimille, eli välitöntä vaikutusta työtehtäviini ei synny. Päivän aikana selvisivät myös

vastaukset eilisestä kulunvalvontaprojektin kokouksesta syntyneisiin kysymyksiin, kun sain keskusteluyhteyden järjestelmätoimittajan tekniseen asiantuntijaan, ja vastausten perusteella nykyinen verkkoarkkitehtuuri on riittävä. Varmistan tämän kuitenkin vielä myöhemmin tällä viikolla oman organisaationi tietoliikenneasiantuntijoilta.

Keskiviikko 02.02.2022

Tämä on viikon ensimmäinen päivä, jolloin kalenterissa on enemmän vapaata aikaa kesken olevien työtehtävien edistämiselle. Tästä huolimatta kokoukset vievät taas useamman tunnin aikaa. Ensimmäisessä kokouksessa käsitellään käyttöoikeuslomakkeiden tekoa, mikä liittyy myös aiemmin työstämiini HR- ja AD-integraatioihin, sekä käyttäjätunnushallinnan elinkaareen. Toinen kokous on laajempi kuukausittainen tietoteknisten sidosryhmien (palveluntoimittajien ja hallintokuntien tietohallintojen) kesken järjestettävä kokous, jossa käydään läpi ajankohtaisia ja tulevia ympäristömuutoksia. Tavoitteenani päivälle on saada HR- ja AD-integraatioon liittyvä uniikin väliaikaisen tunnisteen luonti- ja seuranta-automaatio pilotointitasolle ja prosessi määriteltyä prosessikaavion kautta, sekä saada käyttäjätunnushallinnan elinkaaridokumenttia edistettyä. Datansiirtoautomaation kehitystyön jätän loppuviikolle tai seuraavalle viikolle, sillä niillä ei ole vaikutusta käynnissä oleviin datansiirtoihin.

Sain edistettyä integraatioskriptiä, sekä myös käytyä enemmän HR-dataa läpi. Seuraavana askeleena on alkaa toteuttaa eri HR-datan päivittämistä automaattisesti tekevää automaatiota. Toteutuksessa pitää huomioida HR-järjestelmän uusiutuminen seuraavien kuukausien aikana, mikä tuo lisämahdollisuuksia dataintegraation toteuttamiselle. Nykyisellä toiminnallisuudella saa pidettyä järjestelmien välisen yksilöivän tunnisteen ajan tasalla, sekä löydettyä elinkaaren päässä olevia tunnuksia. Nämä ovat edellytyksiä muun AD-datan automaattiseen ajan tasalla pitämiseen.

Käyttöoikeuslomakkeita koskevassa kokouksessa syntyi hyvää keskustelua sekä käyttäjätunnuksen tilausprosessista, että käyttämisen helppouden näkökulmasta. Yhdeksi suosituksi näkökulmaksi tuli ns. "yhden lomakkeen periaate", eli uuden työntekijän kohdalla esimiehen tulisi täyttää vain yksi lomake, jolla saisi tilattua kaikki tarvittavat IT-työvälineet sekä -oikeudet. Tämä on haastavaa siksi, koska kyseiseen toimenpiteeseen liittyvät vastuut ovat erillään eri yksiköissä, ja kukin tuottaa omia erillisiä tilauslomakkeita järjestelmään. Näitä ovat esimerkiksi työpuhelimen, työtietokoneen sekä IT-oikeuksien tilauslomakkeet. Teknisesti tähän on olemassa ratkaisuja, mutta toteutuksessa tulee pohtia myös ratkaisun ylläpidettävyyttä. Jos ratkaisusta tulee niin monimutkainen, että pienetkin muutokset vaativat pitkän kehitystyön, ei se pidemmällä aikavälillä ole kannattavaa.

Torstai 03.02.2022

Päivän suunnitelmana on taas edistää kesken olevia tehtäviä, ja saada HR-data käytyä loppuun ja raportoitua siihen liittyviä tuloksia, sekä saatua käyttäjätunnushallinnan elinkaaridokumenttia työstettyä valmiiksi asti. Päivä on toisaalta erittäin täynnä erilaisia kokouksia, joihin kuuluvat kulunvalvontaprojektin tietoliikenteen suunnittelukokous, kahden eri yksikön yksikkökokoukset, seuraavan hallintokunnan datasiirtojen suunnittelukokous, sekä viikoittainen Service deskin seurantakokous. Tämän takia on epävarmaa, kuinka paljon saan kyseisiä tehtäviä edistettyä.

Aamulla syntyi heti ennalta suunnittelematon HR- ja käyttäjätunnushallintaprosessiin liittyvä puhelu erään hallintokunnan asiantuntijan kanssa. Tästä syntyi hyviä huomioita, joita olen jo pohtinut, mutta toisen hallintokunnan näkemys asiaan kirkasti myös tarpeita. Prosesseissa tulee nimittäin ottaa huomioon noin kymmenen eri hallintokunnan tarpeet, joihin voi liittyä esimerkiksi vuokratyöntekijöiden laajempi käyttö, suurempi henkilöstön vaihtuvuus ja muut vastaavat asiat. Automatisoitavien prosessien luotettavuuteen tulee myös kiinnittää huomiota, sillä ilman yksiselitteisiä eri järjestelmiä yhdistäviä tunnisteita ei automaatiolla ole mahdollista yhdistää eri tietolähteitä oikein. Esimerkkinä jopa saman hallintokunnan sisällä voi olla samannimisiä ja miltei samoja työtehtäviä hoitavia henkilöitä ja näiden sekoittaminen voi aiheuttaa tietosuojaongelmia, jos palvelussuhdetietojen näkyvyys syntyy väärälle henkilölle. Tämän takia aiemmin mainitsemani tunnisteiden manuaalinen läpikäynti on pakollista.

Suunnitelma toteutui HR-datan läpikäynnin osalta, ja sain edistettyä ensimmäistä automaation osaa, joka varmistaa hallintokunnan lyhenteen oikean muodon, sekä lisää tunnuksille tarvittaessa väliaikaisen uniikin tunnisteen eri järjestelmiin pääsemiseksi. Tämä on tarpeen, sillä nykyisessä HR-prosessissa henkilön tiedot voivat päätyä HR-dataan viikkojen viiveellä, johtuen vanhasta HR-järjestelmästä. Käyttäjätunnushallintaprosessiin liittyvää dokumenttia en ehtinyt kuitenkaan käydä läpi ollenkaan, eli se jää seuraavalle aamulle.

Muihin päivän työtehtäviin kuuluivat kulunvalvontaprojektin tietoliikennesuunnittelun valmistuminen, seuraavan hallintokunnan datansiirtojen suunnittelun aloituskokous, useamman kollegan tekninen avustaminen erilaisissa ongelmissa, sekä muutaman palvelupyynnön ratkaiseminen. Näiden osalta ei kuitenkaan tapahtunut mitään yllättävää, ja asiat etenivät odotetusti.

Perjantai 04.02.2022

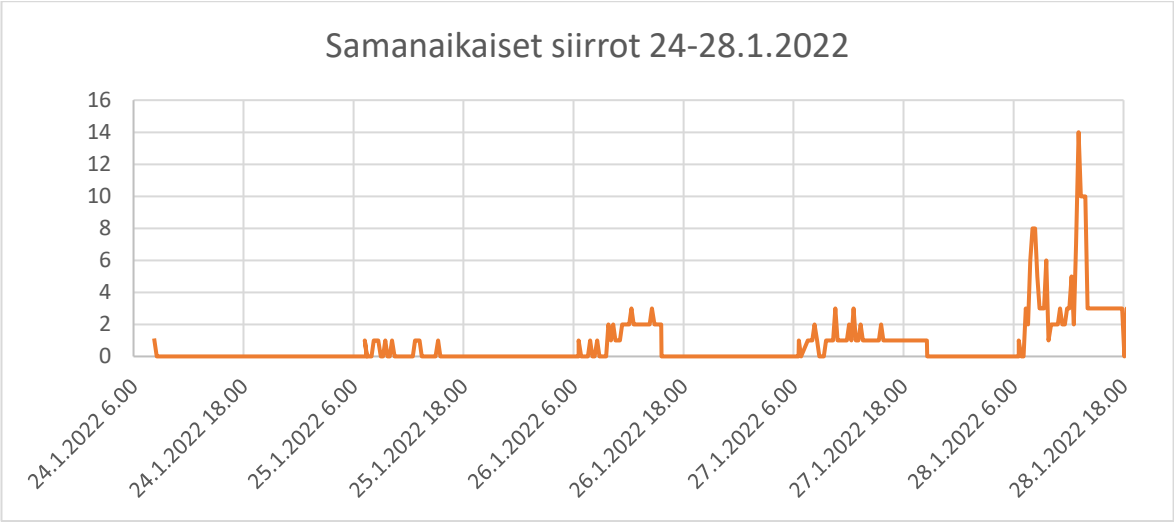
Aamupäivästä suunnittelen saavani käyttäjätunnushallinnan elinkaaridokumentin valmiiksi. Tähän liittyen on palaveri iltapäivällä, jossa dokumentti käydään loppuun. Tämän lisäksi aamupäivästä on toinen kehityskokous ITSM-palveluportaaliin liittyen. Muuten päivälle ei ole varattu kokouksia, joten edellä mainitun dokumentin lisäksi työstän HR-automaatiota toivottavasti saaden sen pilotointikuntoon. Alan myös suunnitella muutoksia datansiirtoautomaatioon samanaikaisten siirtojen määrän rajoittamiseksi, sekä siirron automaattisen aloittamisen mahdollistamiseksi käyttäjien puolesta.

Päivän aikana sain käyttäjätunnushallinnan elinkaaridokumentin valmiiksi ja se saatiin katselmoitua loppuun. Seuraavaksi dokumentti lähtee laajemmalle kommentointikierrokselle, sillä se määrittelee lopulta käyttäjätunnushallinnan elinkaaren prosessit. Päivän toinen kokousten ulkopuolinen tavoite, eli HR- ja AD-automaation saattaminen pilotointikuntoon, ei sujunut odotusten mukaisesti. Kyseisenlaisten automaatioiden tärkeänä osana on jäljitettävyys, eli on pystyttävä myöhemmin todentamaan, onko jokin muutos järjestelmän tekemä sekä milloin se on tehty. Aliarvioin tähän liittyvään lokitukseen ja tietokannan suunnitteluun kuluvaa aikaa, sillä lokituksessa tulee huomioida myös virhetilanteet mahdollisimman hyvin, että ne tulevat lokitettua eivätkä jää piiloon.

ITSM-järjestelmän kehityskokouksessa löytyi hyviä kehitystarpeita, ja annoin niistä joihinkin teknisiä näkemyksiä. Päivällä oli myös yksi tiimin sisäinen vapaampi jutustelutuokio, jossa käytiin myös läpi joitain teknisiä ongelmia. Kyseisen viikoittaisen "kahvituokion" tarkoituksena on toimia osittaisena korvikkeena lähityössä tapahtuvalle spontaanille keskustelulle ja tiedonjaolle, joita syntyy esimerkiksi kahvitaukojen aikana. Omasta mielestäni se on toiminut hyvin, ja siinä on voinut puhua sekä työasioista että muista työyhteisöä kiinnostavista asioista.

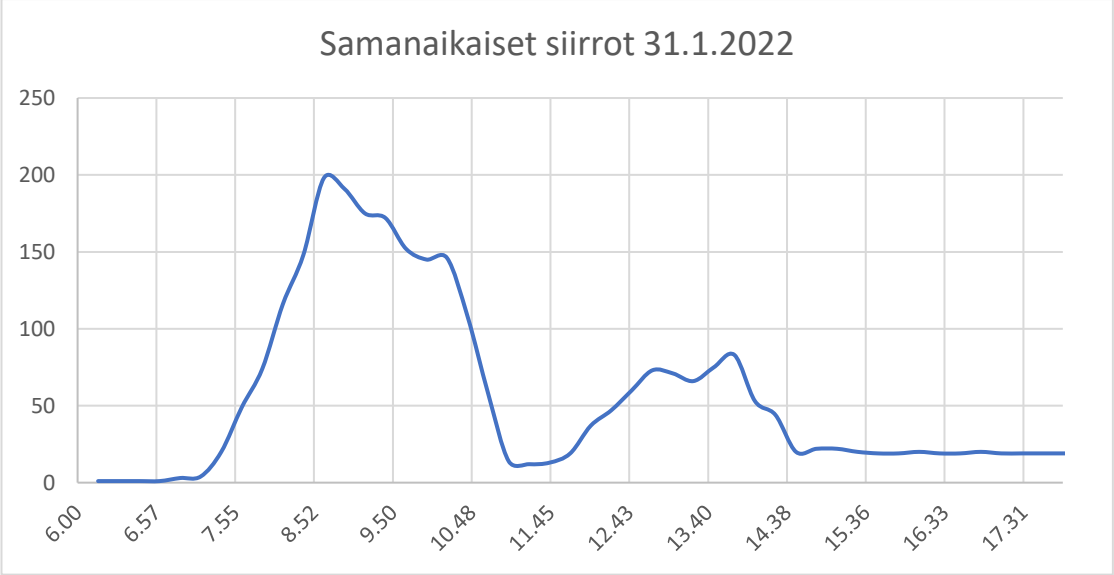
Viikkoanalyysi

Alkuviikon keskeisin työtehtävä oli datansiirtoautomaation kohdistaminen noin 10000 samanaikaiseen tunnukseen edellisen viikon noin 2000 lisäksi. Tässä syntyi joitakin ongelmia, mutta siirtoon liittyi myös yksi itse tekemäni virhearvio. Aiemman viikon perusteella olin arvioinut, että samanaikaisten siirtojen määrä nousisi noin viisinkertaiseksi, koska kotihakemistojen yhteismäärä viisinkertaistui. Tehtyäni edeltävän viikon aikana seurantaa havaitsin sen, että samanaikaisia siirtoja oli kyseisellä viikolla korkeimmillaan hieman yli 10, joten arvioin samanaikaisten siirtojen korkeimmaksi määräksi noin 50-70. Kuviossa 1 on kuvattu samanaikaisten siirtojen määrät kyseisellä viikolla.



Kuvio 1. Samanaikaisten kotihakemiston siirtojen määrät eri ajanhetkillä aikavälillä 24.1-28.1.2022. Datan lähteenä ovat siirtojen lokitiedostot.

Kuten kuviosta 1 näkyy, siirtojen määrä vaihteli viikon aikana huomattavasti, ja suurin samanaikaisten siirtojen määrä oli 14 kappaletta. Suuri osa siirroista ei näy tässä esitysmuodossa, sillä se kuvaa tilanteen 15 minuutin välein. Kyseisellä viikolla yksittäisissä siirroissa meni muutamasta sekunnista pariin minuuttiin. Tilanne kuitenkin muuttui 31.1.2022 maanantaina, jolloin loput noin 10000 kotihakemistoa tulivat siirtoon mukaan. Kyseisen päivän samanaikaisten siirtojen määrä on kuvattu kuviossa 2.



Kuvio 2. Samanaikaisten kotihakemiston siirtojen määrät eri ajanhetkillä 31.1.2022. Datan lähteenä ovat siirtojen lokitiedostot.

Kuten kuviosta 2 näkyy, samanaikaisten siirtojen määrä oli enimmillään noin 200, mikä oli 3-4 kertaa arvioimaani suurempi. Pahimmillaan yksittäinen siirto saattoi kestää melkein

tunnin. Tämän takia seurasin siirtoja myös erittäin intensiivisesti 31.1 ja 1.2, koska moninkertaisen kuorman takia halusin varmistua lähdepalvelimen kapasiteetin riittävyydestä. Pahimmassa tapauksessa virhearvio olisi voinut johtaa palvelunestohyökkäyksen (DoS, Denial of Service) kaltaiseen lopputulokseen. Samanaikaisten siirtojen määrän virhearvioinnista huolimatta olin kuitenkin arvioinut etukäteen siirtoja liikakuormittumisen näkökulmasta. Tähän liittyvät merkittävimmät arvioimani asiat ovat listattuna alla:

- Koronaviruspandemian takia vain noin neljännes henkilöstöstä on kerrallaan lähitöissä.
- Kansioiden uudelleenohjauksen yhteyteen IT-ympäristössä on määriteltynä automaattiset offline-tiedostot tärkeimmille kotihakemiston sijainneille. Jos palvelin ei ole käytettävissä tai se toimii liian hitaasti, siirtyy tietokone käyttämään paikallisella tietokoneella olevassa välimuistissa olevia versioita tiedostoista, ja synkronoi ne verkkoyhteyden palattua (Microsoft 2021e).
- Tarkistin etukäteen, että siirtojen lähteenä olevalla levyllä ei sijaitse mitään muuta kuin siirrettäviä kotihakemistoja, joten vaikutusta muihin palveluihin ei synny.
- Suunnittelin seuraavani palvelimen ja levyn kuormitusta aktiivisesti siirtopäivinä ja keskeyttäväni siirrot, jos kuormituksesta syntyy käyttäjähaittaa.

Siirtojen aikana havaitsin pahimmillaan merkittävää kotihakemistojen tiedostojaon hidastumista, ja siirtojen väliaikainen keskeyttäminen oli melko lähellä toteutumista. Tiedostojako oli kuitenkin jatkuvasti käytettävissä, joten tähän vaihtoehtoon ei ollut lopulta tarvetta turvautua.

Siirtojen samanaikaisen määrän virhearvioinnin arvioin johtuvan kahdesta erillisestä seikasta. Ensimmäinen syy on edellisen viikon noin 2500 siirtoautomaation piiriin lisätyn henkilön porrastettu lisääminen. Maanantaina lisättiin muutama sata, tiistaina ja keskiviikkona hieman enemmän, ja torstaina yli tuhat. Näin kyseisten henkilöiden siirrot jakautuivat viidelle päivälle yhden päivän sijasta. Tämän seurauksena samanaikaisten siirtojen arvio olisi pitänyt kertoa noin kahdella.

Tämän lisäksi aiemman kokemukseni perusteella viikonpäivällä on myös merkitystä. Näkemykseni mukaan henkilöt ovat perjantaisin huomattavasti passiivisempia sekä aloittamaan erilaisia päivitystoimintoja, että ilmoittamaan ongelmista. Maanantaina taas on tyypillisempää, että erilaiset ongelmat otetaan esille, jos ne ovat vielä viikonlopun jälkeen olemassa. Maanantaina myös erilaisten keskitettyjen päivitysten, joihin tämäkin tavallaan kuuluu, hoitaminen on taas aktiivisempaa käyttäjien suunnalta. Oma olettamukseni on siis se, että perjantaisen maksimin käyttäminen maanantaista maksimia arvioitaessa johtaa

kyseisen maksimin aliarviointiin tässä yhteydessä. En löytänyt tähän liittyviä tutkimuksia, joten nämä arviot perustuvat täysin edellisen yli 10 vuoden kokemukseeni työnantajani IT-ympäristöstä ja käyttäjäkunnasta, mutta kyseinen hypoteesi voisi olla mielenkiintoinen tutkimuskohde.

Virhearviointi antoi myös tärkeää dataa siitä, mikä on sopiva yläraja siirtojen maksimimäärälle palvelinta kohden. Oma arvioni on edelleen noin 75-100, mikä ei näkemykseni mukaan aiheuttanut tiedostojakoihin käyttäjille näkyvää hidastumista. Kyseisen rajoituksen toteuttaminen siirtoautomaatioon onkin yksi tulevien viikkojen tehtävistä, ennen kuin seuraavia massasiirtoja aletaan toteuttaa.

Sain viikon aikana myös käyttäjätunnushallinnan elinkaaridokumentaation valmiiksi, ja se saadaan nyt lausuntokierrokselle eri sidosryhmille. Se määrittelee tietyt elinkaarenhallintaan liittyvät prosessit, joten se on hyvin keskeinen dokumentti ja siinä on tärkeää huomioida erilaiset sidosryhmien erityistarpeet. Kyseistä dokumenttia lähellä on myös työstämäni HR- ja AD-järjestelmien integraatio, sillä sen pyrkimyksenä on vähentää kyseiseen prosessiin liittyvää manuaalista työtä, ja se onkin kuvattu osittain dokumentissa. HR-järjestelmä on uusiutumassa, ja koska tämä aiheuttaa HR-prosesseihin muutoksia, voi sillä olla myös vaikutusta erityisesti käyttäjätunnusten elinkaaren alkuvaiheisiin ja vaatia dokumentin päivittämistä noin puolen vuoden sisällä.

Muut viikon työtehtävät olivat pääsääntöisesti rutiininomaisia, ja niiden suorittaminen ei vaatinut muuta kuin aiemmin hankkimani tiedon soveltamista. Datansiirtoautomaation kautta tuli kuitenkin taas havaittua se, että riittävä toimintojen lokitus on tärkeää. Ilman kyseisiä lokeja siirtojen analysointi jälkikäteen olisi ollut mahdotonta, jolloin jatkotoimenpiteiden arviointi olisi ollut hetkellisen seurannan ja siitä syntyneiden muistikuvien varassa.

3.4 Seurantaviikko 4

Maanantai 07.02.2022

Päivän aikana on taas useampia teknisiä kokouksia. Odotettavissa kuitenkin on, että ne ovat melko rutiininomaisia. Muilta osin päivän suunnitelmana on saada edistettyä HR- ja AD-järjestelmien välistä automaatiota, sekä pohtia siihen liittyviä prosesseja tarkemmin. Tästä pitää alkaa myös valmistelemaan erillistä dokumenttia.

Aamupäivän suunnitelmat menivät hieman uusiksi, sillä jouduin ratkaisemaan joitakin palvelupyyntöjä, ja en saanut edistettyä suunnittelemiani muita tehtäviä suunnitelmieni mukaisesti. Pääasiassa tämä johtui siitä, että sain erääseen toiseen suunniteltuun dokumentaation ja automaation parantamiseen liittyvään toiminnallisuuteen liittyviä ajatuksia, ja työstin kyseisellä aiheelle dokumenttipohjan jatkotyöstöä varten. Kyseisestä aiheesta on ollut jonkin verran keskustelua aikaisemmin, mutta se ei ole ollut prioriteetissa korkealla. Siihen liittyvät ajatukset sattuivat kuitenkin tarkentumaan muun ajattelutyön yhteydessä. Kyseessä on käytännössä lisäysten suunnittelu ja teko AD-schemaan, jonka tarkoituksena on saada AD-objektit dokumentoitua määrämuotoisemmin ja niin, että niiden muutoksia on mahdollista automatisoida ja tietojen ajantasaisuutta seurata paremmin.

Päivän teknisiin kokouksiin liittyi ongelmanselvitystä, mutta nämä olivat rutiininomaisia ja etenivät odotetusti. Yhtenä ongelmana oli Azure AD -vierastilien sähköpostin verkkodomainin muutos massatoimenpiteenä, ja toisena erään etähallintatyökalun toiminnallisuuden testaaminen. Ensimmäinen toimenpide on suoraviivainen, mutta sen varsinainen tekeminen kuuluu eri yksikölle, joten tämä oli lähinnä ohjeistamiskokous, sekä eri vaihtoehtojen läpikäyntiä. Etähallintatyökalun toiminta taas oli vain riippuvainen puuttuvasta Applocker-säännöstä, jonka toteutuksen laitoin myös tilaukseen. Päivään kuului myös hieman ITSM-järjestelmän palvelupyyntöjen seurannan pohdintaa, ja miten eri yksiköiden välistä tiedonkulkua saataisiin parannettua.

Tiistai 08.02.2022

Tänään on taas hieman kevyempi päivä kokousten osalta, ja yritän saada HR- ja AD-integraation dokumentaatiota tehtyä. Käytännössä kyseinen dokumentaatio pitää saada kuntoon, ennen kuin automaatiota voi viedä tuotantoympäristöön, joten tämän takia kyseisen tehtävän prioriteetti on nyt korkeammalla. Päivän kokouksista kaksi on taas viikoittaisia seurantakokouksia, toinen RDS-hallintaympäristöstä ja toinen työasemaympäristöön liittyvä. Lisäksi ylimääräisenä kokouksena on ITSM-järjestelmään liittyvien kehitystarpeiden läpikäynti.

Alkupäivästä minulle osoitettiin muutama datansiirtoautomaatioon liittyvä palvelupyyntö, jotka eivät ratkenneet standardiohjeilla. Jouduin käyttämään hieman aikaa näiden selvittämiseen, ja päivittämään dokumentaation. Ongelmien määrä ei ollut mitenkään kovin suuri suhteessa siirrettyihin kotihakemistojen määrään, mutta niiden ratkaisujen dokumentointi nopeasti on tärkeää, että asiakkaat saavat nopeasti avun ja tukipalveluilta ei mene turhaan aikaa samojen ratkaisujen keksimisessä itsenäisesti.

Sain myös HR-integraation dokumentaatiota edistettyä päivän aikana, mutta tässä pitää pyrkiä keskittymään lähinnä nykytilan ja toteutuksessa olevan automaation dokumentointiin. Luonnostelin samalla jo uuden HR-järjestelmän mahdollisia prosesseja, mutta kyseisen järjestelmän käyttöönottoon on vielä kuukausia, joten sen osion dokumentista voi jättää myöhemmäksi. Päivän aikana jouduin myös kertaamaan hieman ympäristön keskitettyjä tietoturva-asetuksia, sillä edellisenä päivänä mainitsemaani etähallintatyökalun käyttöön liittyy tiettyjä asetuksia, jotka ovat ympäristössämme tiukempia kuin mitä sen käytössä suositellaan. Tässä hyödynsin STIG-määrittelyitä, jotka ovat teknisiä tietoturvan kokoonpanoon liittyviä standardeja, ja joihin ympäristön tietoturva-asetukset osittain perustuvat. Samalla kävin tarkistamassa Microsoftilta tämänhetkisen suosituksen kyseisten asetusten käyttöön. Näiden perusteella en suosittele kyseisiä asetuksia otettavan käyttöön, sillä niillä on oman arvioni mukaan pieni vaikutus käyttökokemukseen, kun ne taas lisäävät kohtuuttomasti erilaisia tietoturvaan liittyviä riskejä. Kyseisten asetusten puute ei siis estä etähallintatyökalun käyttöä.

Päivän kokoukset etenivät odotetusti, ja niistä syntyi joitakin ylimääräisiä työtehtäviä. Näistä merkittävimmät liittyivät RDS-hallintaympäristön käyttöönoton edistämiseen. Sain myös datansiirtoautomaation dokumentaation päivitettyä ilmenneiden ongelmien osalta, ja se pitää saada nyt viestittyä mahdollisimman laajasti, ettei palvelupyyntöjä jää turhaan roikkumaan ja ettei dokumentoituja ongelmia siirretä eteenpäin tutkittavaksi, vaikka ratkaisu on jo olemassa.

Keskiviikko 09.02.2022

Tämä päivä on käytännössä täynnä kokouksia, ainoastaan keskellä päivää on pieni väli, jossa voin edistää muita työtehtäviä, kuten HR- ja AD-järjestelmien integraatiota ja sen dokumentaatiota. Tämän lisäksi yksi viivästynyt työtehtävä on muutosten tekeminen erääseen ITSM-järjestelmän lomakkeeseen, ja se on todennäköisesti tänään ensisijaisena kokousten ulkopuolisena tehtävänä, sillä viikon lopussa on kaksiviikkoisen kehityssyklin julkaisupäivä, ja muutokset olisi hyvä saada siihen mukaan.

Päivän kokouksista huolimatta sain mainitsemiani muita työtehtäviä edistettyä hyvin. ITSM-järjestelmän lomakkeen muutokset tulivat valmiiksi, ja se saatiin siirrettyä testiympäristöön, josta se huomisen testauksen jälkeen siirretään tuotantoympäristöön. HR- ja AD-järjestelmien integraatiodokumentti edistyi myös sen verran, että se on melkein valmis, ja uskon saavani sen valmiiksi seuraavana päivänä.

Päivän kokouksista kaksi liittyivät uuden ensimmäisen asteen tukipalvelun käyttöönottoon, ja niissä määriteltiin vastuita, eskalaatiopolkuja, sekä korkean tason prosesseja. Kolmas liittyi yleisesti HR-prosesseihin ja AD-integraatioon, ja sain siinä alustavasti esiteltyä suunnitelman uuteen HR-järjestelmään liittyvästä AD-integraatiosta. Tämä eroaa aiemmin mainitsemastani automaatiosta, jolla pyrin parantamaan tiettyjä nykyisen järjestelmän ja prosessin ongelmia. Tämän jatkokehitykseen ei kuitenkaan kannata käyttää liikaa aikaa, sillä uusi järjestelmä tulee odotettavasti parin kuukauden päästä käyttöön. Muut kokoukset olivat joka toinen viikko pidettäviä yleisempiä kokouksia.

Päivän aikana jouduin selvittämään Chrome-selaimeen liittyvää ongelmaa, sillä eräs vanhempi sisäinen järjestelmä lakkasi toimimasta. Tähän löytyi nopeasti syy Chromen versiopäivityksestä versioon 98, jossa TLS 1.0 ja 1.1-protokollat poistettiin käytöstä lopullisesti. Ratkaisuna oli tehdä ryhmäkäytäntö, jolla voidaan palauttaa Chrome väliaikaisesti aiempaan versioon. Pysyväisratkaisuna tietenkin on järjestelmän päivitys, sillä erityisesti selaimet ovat alttiita eri verkkosivujen tietoturvariskeille, jos niitä ei pidetä päivitettyinä. Päivän aikana tuli myös joitakin palvelupyyntöjä kotihakemiston siirtoautomaatioon liittyen, mutta ne ratkesivat toimenpiteellä, jota ei ollut vielä dokumentoitu tietämyskantaan.

Torstai 10.02.2022

Tänään kalenterissa on vielä enemmän kokouksia ja ainoastaan aamusta on pari tuntia vapaata aikaa. Tavoitteena on saada HR-integraatiodokumentti kirjoitettua loppuun, sekä saada ITSM-lomakkeen testaus testiympäristössä suoritettua, että se saadaan vietyä huomenna tuotantoympäristöön. Päivän kokoukset ovat hyvin laaja-alaisia, ja niihin kuuluu AD-tunnushallinnan automatisointia, ITSM-järjestelmän kaksiviikkoisen kehityssyklin demo, yhteistyökokous yhden sidosryhmän kanssa, RDS-hallintaympäristön ohjausryhmä, eräs viikoittainen seurantakokous, sekä kulunvalvontaan liittyvä tekninen läpikäyntikokous.

Päivän tavoitteet täyttyivät, ja sain HR-integraatiodokumentin valmiiksi ja laitettua alustavalle kommenttikierrokselle. Jos kyseinen ehdotus hyväksytään johtoportaassa, syntyy siitä todennäköisesti projekti, jossa määritellään tarkemmin tekninen ratkaisu, sekä toteutetaan se. Ehdin tehdä myös ITSM-lomakkeen testauksen, joten sekin pysyi suunnitellussa aikataulussa. Aamupäivän kokousten lomassa jouduin auttamaan verkko-ongelman ratkaisussa erään järjestelmän testiympäristössä, ja jouduin hälyttämään lähitukea paikalle. Ongelma oli tuen paikalle päästyä yksinkertainen, eli laitteelta oli poistunut IP-asetuksen määrittely. Sain dokumentaatiosta tarkistettua oikeat asetukset, ja paikalla ollut lähituki sai laitteet toimimaan.

Päivän kokouksista ei syntynyt merkittäviä huomioita, ainoastaan sidosryhmän yhteistyökokouksesta syntyi lisää tulevia tehtäviä, kun siellä päätettiin erään prosessin automatisoinnista. Tästä järjestetään myöhemmin määrittelykokous, johon minut kutsuttiin mukaan asiantuntijana.

Perjantai 11.02.2022

Perjantaina on vain yksittäinen kokous, joten oletan saavani koko päivän edistettyä muita työtehtäviä. Yhtenä tavoitteena on saada HR-integraatiodokumenttiin löyhästi liittyvä AD-automaatiodokumentti valmiiksi ja kommentoitavaksi, sillä molemmat ovat tärkeitä automaatioon ja sitä kautta manuaalisen työn vähentämiseen tähtääviä dokumentteja. Niitä voisi kuvata alustaviksi projektiehdotuksiksi, joista syntynee varsinainen tarkempi projektisuunnitelma, mikäli niistä ei kommenttikierroksella löydy merkittäviä puutteita. Jos näistä jää aikaa, edistän automaatioskriptejä, jotka ovat jääneet prioriteetissa viime aikoina alemmas.

Päivän aikana sain tuotettua AD-automaatiodokumentin suunnitelmien mukaisesti, sekä laitettua sen kommentoitavaksi. Kommenteilla haen sellaisia teknisiä tai prosessiin liittyviä ehdotuksessa olevia virheitä, jotka voivat vaikuttaa varsinaisen projektisuunnitelman tekemiseen. Itse en tietenkään usko, että ehdotuksissa olisi kyseisenlaisia puutteita, mutta olen huomannut työssäni, että pelkät erilaiset näkökulmat voivat tuoda esille hyviä ajatuksia, vaikka kommentoivalla henkilöllä ei kyseisen aihealueen syvällistä osaamista olisikaan.

Suunniteltujen tehtävien lisäksi päivälle osui hieman monimutkaisempi ongelmanselvitystapaus. Siirtoautomaatioon liittyen oli alkanut syntyä omituisia palvelupyyntöjä, joissa varsinainen datansiirto oli onnistunut, mutta käyttäjällä kotihakemisto näytti siltä, että se ei toimisi. Ongelmakoneiden lokeja tutkimalla syyksi paljastui se, että koneiden offline-tiedostot siirtyivät offline-tilaan slow-link moden takia. Käytännössä tämä tarkoittaa sitä, että käyttöjärjestelmä tarkkailee verkkoyhteyden laatua, ja mikäli se laskee liian huonoksi, asettaa se offline-tiedostoja sisältävät tiedostojaot offline-tilaan. Tällöin kyseisestä tiedostojaosta ovat käytettävissä vain synkronoidut tiedostot, ja tyypillisesti koko kotihakemisto ei ole synkronoitu, jolloin vain pieni osa tiedostoista on käytössä.

Ratkaisuna ongelmaan oli slow-link moden poistaminen käytöstä ryhmäkäytännöillä. Ongelmaa ei ilmennyt vanhassa sijainnissa, sillä siellä se oli jo poistettu käytöstä, mutta tämänkaltaisen asetuksen havaitseminen olemassa olevilla muutoshallinnan prosesseilla

etukäteen oli käytännössä mahdotonta. Teoriassa tästä syntyneet palvelupyynnöt ja käyttäjähaitta olisivat olleet estettävissä, mutta se vaatisi paljon nykyistä raskaamman muutoksenhallintaprosessin.

Viikkoanalyysi

Tälle viikolle kohdistui käytännössä kahden toisiinsa liittyvän mutta kuitenkin toisistaan erillä olevan prosessin suunnittelu ja toteutusehdotuksen tekeminen. Ensimmäinen prosessi oli HR- ja AD-datan integraatio. Tässä prosessissa tavoitteena on vähentää manuaalista työtä ja yhdenmukaistaa työntekijöiden käyttäjätunnusten luonti. Aiemmin automaation toteuttamisen ongelmana on ollut nykyisestä HR-järjestelmästä merkittävällä viiveellä saatu data. Uudessa järjestelmässä tämä viive on kyseisen järjestelmän projektiryhmän mukaan minimoitu, jolloin työntekijän tiedot järjestelmään syötettäessä ne saadaan siirrettyä nopeasti tämän jälkeen integraatioon suunnitellulle automaatiolle, jolloin henkilön perustietoja ei tarvitse täyttää useampaan eri paikkaan. Tätä kävin jo läpi seurantaviikon 2 viikkoanalyysissä ja kyseisen prosessin korkean tason kuvaus on esitetty kuvassa 5. Nyt kyseinen prosessi- ja alustava tekninen dokumentti on kommentoitavana, ja se saadaan toivottavasti projektoitua riittävän nopeasti niin, että uuden HR-järjestelmän dataa päästään kyseisen suunnitellun automaation kautta hyödyntämään nopeasti sen käyttöönoton jälkeen. Tämä vähentäisi merkittävästi tietohallinnon työtä, sekä parhaassa tapauksessa nopeuttaisi työntekijöiden tunnusten saamista.

Toinen viikon aikana tekemäni prosessin suunnittelu kohdistui AD:ssa olevien objektien omistajuuden ja siihen liittyvien elinkaarenhallintaprosessien suunnitteluun. Nykytilassa ongelmana on se, että AD:n objektien (esim. käyttöoikeusryhmät, palvelimet, palvelutunnukset, yhteiskäyttöiset sähköpostitilit) omistajuuden dokumentaatio, ja sitä kautta käyttöoikeusvaltuutusten hallinta, on vähintäänkin ongelmallista. Kyseisten objektien omistajuus on hajanaisesti ja usein epäselvästi dokumentoitu, ja pahimmassa tapauksessa perustuu suulliseen historiatietoon. Kyseisen prosessidokumentin tavoitteena on määritellä objekteille selkeät tietokentät, mihin objektien omistajuus dokumentoidaan, sekä automaatiot, jotka varmistavat, että omistajuustietoa ylläpidetään koko elinkaaren ajan. Muista järjestelmistä kokemuksia saaneena kullakin objektilla tulee olla vähintään kaksi määriteltyä omistajaa, sillä muuten työpaikan tai työtehtävien muutokset jättävät objektin omistajuuden tyhjäksi suurella todennäköisyydellä. Automaatio taas varmistaa, että jokaisella objektilla ovat nämä vähintään kaksi omistajaa määriteltynä. Jos näin ei ole, alkaa se lähettämään viestejä määritellyn eskalaatiopolun kautta ongelman korjaamiseksi, minkä lisäksi se pyytää omistajia varmistamaan tietojen oikeellisuuden kerran tai kaksi vuodessa.

Omistajuustiedon ollessa kunnossa ja määrämuotoisessa tietokentässä mahdollistuu myös esimerkiksi automaattisten hyväksymiskiertojen toteuttaminen.

Valtuutusketjujen selkeyttäminen on myös tärkeä osa prosessin suunnittelua. Tällä tarkoitetaan sitä, että kenellä on valtuus myöntää jollekin henkilölle tietty käyttöoikeus. Valtuutusketju syntyy, kun kyseinen valtuuttava henkilö valtuuttaa jonkin toisen henkilön myöntämään oikeuksia puolestaan. Tästä esimerkkejä ovat esimerkiksi esimiehen valtuutus sihteerilleen hoitaa tiettyjä henkilöstöön liittyviä rutiiniasioita, tai järjestelmän omistajan esimiehille antama valtuutus käyttöoikeuksien valtuuttamisesta alaisilleen. Prosessissa pitää siis selkeästi erottaa henkilöt, joilla on käyttöoikeudet tehdä jokin toimenpide, ja kenellä taas on valtuudet määrätä kyseinen toimenpide tehtäväksi. IT-maailman ulkopuolisena esimerkkinä postinkantajalla on esimerkiksi IT-sanastoa käyttäen käyttöoikeudet (mahdollisuus) avata jokainen hänen kuljettamansa postipaketti, mutta hänellä ei ole siihen valtuuksia (laillista oikeutta). Prosessiin kuuluu olennaisena osana valtuutuksen juuren eli omistajan määrittely, mutta myös valtuutusketjujen huomioiminen ja myöhempi jäljitettävyys.

Kyseinen prosessidokumentti ja siihen liittyvä alustava tekninen ehdotus valmistuivat viikon loppupuolella, ja menivät myös eteenpäin kommentoitavaksi. Odotan, että tästäkin ehdotuksesta syntyy toteutettava projekti, sillä ehdotuksen toteuttaminen vaatii resursseja sekä johtotason hyväksyntää, sillä se vaikuttaa myös sidosryhmien tietohallintojen toimintatapoihin. Toisaalta on odotettavissa, että projektin toteuttamisesta syntyy merkittäviä resurssisäästöjä uusien automaatiomahdollisuuksien toteutuessa.

Viikon aikana työtehtäviin kuului prosessisuunnittelun lisäksi myös joitakin hieman monimutkaisempia ongelmanselvitystilanteita. Nämä eivät kuitenkaan olleet varsinaisesti uudempia ongelmia, vaan niiden ratkaisut perustuivat aiemmin hankkimaani tietoon. Yhtenä ongelmana oli Google Chrome-selaimen päivittyminen versiosta 97 versioon 98, joka poisti käytöstä TLS 1.0 ja 1.1-tuen. Tämä aiheutti ongelmia eräässä kohtuullisen tärkeässä järjestelmässä ja ongelma ilmeni selaimen virheilmoituksena. Kyseisenlaisia ongelmia on tullut aiemminkin selaimen päivittyessä ja tietoturvan parantuessa, joten nämä oireet johtivat nopeasti varmistamaan diagnoosin kyseisen selaimen teknisestä dokumentaatiosta. Google (2022) toteaa, että "In M-98, the error will no longer be bypassable", jossa M-98 on viittaus Chromen versioon 98.

Ongelma ei ollut suoraan ratkaistavissa muuten kuin hyödyntämällä Chromessa olevaa aiemman version palautusmekanismia. Tästä syntyi toinen tutkittava asia, sillä kyseinen asetus ei toiminut odotetulla tavalla. Lyhyen tutkimisen jälkeen havaitsin, että erääseen

ryhmäkäytäntöobjektiin oli jäänyt kyseisen mekanismin estävä asetus päälle, ja se oli prioriteetissa (linkitysjärjestyksessä) korkeammalla kuin määritetty asetus. Tähän mennessä oli kuitenkin selvinnyt se, että ongelmallinen järjestelmä tullaan päivittämään hyvin nopealla aikataululla, joten palautusmekanismin käyttötarve poistui. Kyseinen linkitysjärjestyksen ongelma kuitenkin korjattiin vastaavien ongelmien välttämiseksi tulevaisuudessa.

Toinen hieman syvällisempää selvitystä vaatinut ongelma oli offline tiedostot-ominaisuuden hitaan linkkimoodin (slow-link mode) aiheuttaman ongelman tutkiminen. Seurantaviikon edetessä datansiirtoprojektissa alkoi syntyä ongelmia kotihakemistojen käytössä siirtojen jälkeen, ja tämä vaati itseltäni hieman työasemien tapahtumalokien tutkimista ongelman selvittämiseksi. Offline-tiedostojen lokeissa näkyi selviä mainintoja slow-link moden aktivoitumisesta, ja kun tarkistin asian ryhmäkäytännöistä, oli kyseinen asetus poistettu käytöstä vanhassa kotihakemistosijainnissa. Tätä ei kuitenkaan ollut huomattu tehdä ennakoivasti uudelle kotihakemistosijainnille. Windows 8 -versiosta lähtien slow-link moden oletuslatenssi on 35 ms, jonka jälkeen tiedostojako siirtyy offline-tilaan (Microsoft 2021f). Tietyissä toimipisteissä internet-yhteys on laadultaan sellainen, että kyseinen raja rikkoutuu rutiininomaisesti joko normaalitilanteessa, tai kun internet-kaistanleveydestä käytetään riittävän suuri osuus, jolloin latenssi nousee internet-yhteyden saturaation kasvaessa. Ongelma saatiin korjattua nopeasti, kun sen juurisyy selvisi, ja käytännössä korjauksena oli poistaa slow-link mode käytöstä, sillä tällaisissa tapauksissa siitä on vain haittaa.

Kolmantena hieman vaativampana asiana minun piti selvittää tiettyjen etätukiohjelman suositeltujen asetusten vaikutusta tietoturvaan, ja sitä voiko kyseisiä käyttöä sujuvoittavia asetuksia muuttaa. Tietoturva-asetusten pohjana on ympäristössä hyödynnetty sekä Microsoftin suosituksia, että tiettyjä STIG-dokumentteja (Security technical implementation guide). Käytetty STIG on Yhdysvaltojen puolustusministeriöltä julkisesti saatavilla oleva määrittely, joka perustuu NIST 800-53-standardiin ja siihen liittyviin dokumentteihin (DISA, 2021). Asetus koskee Windows UAC-ominaisuutta, ja on kyseisessä dokumentissa määritelty olevan tärkeydeltään keskitasoa. Tämän lisäksi Microsoft (2021g) ei suosittele asetusta asetettavan arvoon "Elevate without prompting", sillä se heikentää kyseisen ominaisuuden tietoturvavaikutusta. Tämän seurauksena en tule suosittelemaan nykyisen asetuksen muuttamista, sillä vaikutus käytettävyyteen on suhteellisen pieni, mutta vaikutus tietoturvaan ja ylläpitotunnusten käytön turvallisuuteen on mielestäni merkittävä.

Viikon merkittävin kehittyminen tapahtui prosessisuunnittelussa, sillä siinä joutui pohtimaan tarkasti prosesseja ja niiden vaikutuksia tietoturvaan, tietosuojaan ja muutosten jäljitettävyyteen. Erityisesti muutosten jäljitettävyys oli mielenkiintoinen aihe, sillä käytännössä minkä tahansa käyttöoikeusmuutoksen tulee olla jäljitettävissä valtuutusten ja tekijän

osalta niin, että mahdolliset väärinkäytökset tai virheet voidaan havaita ja korjata. Tähän liittyy osaltaan toimenpiteiden lokituksen kokonaiskuvan hahmottaminen, eli miten lokitusta tehdään tällä hetkellä ja miten sitä pitäisi kehittää kyseisten tavoitteiden tukemiseksi.

3.5 Seurantaviikko 5

Maanantai 14.02.2022

Tälle päivälle olen aamusta varannut itselleni aikaa analysoida tähän mennessä edenneitä datansiirtoja ja katsoa kuinka hyvin ne ovat edenneet. Lupasin myös raportoida tästä sidosryhmille. Päivällä on tämän lisäksi kolme muuta kokousta, joista yksi koskee kulunvalvontajärjestelmän uudistamisprojektia, yksi on ITSM-järjestelmän viikkokokous, ja kolmas on tekninen kokous erään sidosryhmän kanssa liittyen AD-ryhmillä tehtävään käyttöoikeushallintaan. Muulla vapaaksi jäävällä ajalla suunnittelen edistäväni tiettyjä RDS-hallintaympäristöön sekä datansiirtoautomaatioon liittyviä kesken olevia tehtäviä.

Päivä meni suunnilleen odotetun mukaisesti. Aamulla sain tehtyä skriptin, joka analysoi datansiirtoautomaation lokeja, ja luo senhetkisen tilanneraportin siirtojen tilasta. Raportista selvisi sellainen yllätys, että merkittävällä osalla tunnuksia ei ole kirjauduttu verkkoon kohtuullisen pitkään aikaan, joten tästä syntyi myös sidosryhmän suuntaan selvitettävää. On nimittäin mahdollista, että osa kyseisistä tunnuksista ei enää ole aktiivisessa käytössä. Tähän liittyy myös edellisellä viikolla mainitsemani HR- ja AD-järjestelmien välisen käyttäjätunnushallinnan automatisoinnin projektiehdotus, sillä tunnushallinta ja sen elinkaaren seuranta on nykyisellään manuaalinen prosessi. Datasta selvisi myös se, että käyttäjät lykkäävät datansiirtoa kohtuullisen paljon, ja loppuviikon tavoitteena onkin saada viimeisteltyä siirron aloituksen pakotus ja samanaikaisten siirtojen rajoittamisominaisuudet niin, että ne saadaan käyttöön seuraavalla viikolla. Datansiirtoprojektiin liittyen sain myös tehtyä valmistelevia toimenpiteitä kahden muun sidosryhmän osalta, ja heidän pilottinsa tämän osalta alkanee mahdollisesti jo tällä viikolla.

Kulunvalvontajärjestelmän uudistamisprojektikokous oli melko rutiininomainen projektin seurantapalaveri, joten siitä ei syntynyt yllätyksiä. Samaten ITSM-järjestelmän viikkokokouksesta ei syntynyt yllätyksiä, tosin siellä sivuttiin taas toimipisteisiin liittyvän datan ylläpitoa, josta on keskusteltu aiemmin. Tästä syntyi itselleni ylimääräinen työtehtävä niihin liittyvän master datan hallinta- ja ylläpitoprosessin suunnittelusta ITSM-järjestelmässä.

Päivän viimeisessä kokouksessa käytiin läpi uuteen järjestelmään liittyvää käyttöoikeushallintaa AD-ryhmillä, ja sitä miten se käytännössä tapahtuu toimintaympäristössämme.

Sain vastattua alustaviin kysymyksiin, mutta kokonaisuus vaikutti melko monimutkaiselta, joten tästä syntynee vielä lisää teknisiä konsultaatiotarpeita. Tässäkin yhtenä keskeisenä kysymyksenä prosessiin liittyen oli käyttöoikeusryhmien valtuutus ja valtuutusketjut, mikä liittyy suoraan edellisellä viikolla tekemääni ehdotukseen. En saanut juurikaan edistettyä RDS-hallintaympäristöön liittyviä tehtäviä päivän aikana, joten ne jäävät seuraavalle päivälle.

Tiistai 15.02.2022

Tiistaina on taas kohtuullisen monta kokousta, joista kaksi ovat viikoittaisia seurantakokouksia. Kaksi muuta kokousta liittyvät kahden eri sidosryhmän datansiirtojen suunnitteluun, ja viimeinen kokous liittyy tulevan ensimmäisen tason tuen tehtävien ja eskalaatiopolkujen määrittelyyn. Vapaata aikaa on melko vähän, mutta tänään pitää saada RDS-hallintaympäristöä koskevat tietyt tehtävät etenemään, joten loppuaika on varattu sille.

RDS-hallintaympäristön viikkokokouksessa selvisi yksi ongelma, joka oli vaivannut toista RD Gatewaytä. Ongelma liittyi siihen, miten RD Gateway käsittelee älykortin tunnistetietoja, kun käytössä on älykortti, jonka varmenne on linkitetty useampaan käyttäjätunnukseen ja käyttäjänimivihje (user name hint) on käytössä. RD Gateway ei ymmärrä muita kuin älykortilla olevan UPN:ää (user principal name) vastaavan käyttäjätunnuksen, joten käytännössä kirjautuminen tapahtuu kahdella eri tunnuksella. RD Gatewayn eräässä asetuksessa pääsynhallintaan oli kuitenkin määritelty vain toista tunnusta vastaava käyttöoikeusryhmä, mikä esti kyseisen RD Gatewayn käytön. Ongelma ratkaistiin myöntämällä käyttöoikeudet kaikille älykortilla käytettäville tunnuksille. Datansiirtoautomaation kokouksissa saatiin aikataulutettua seuraavien sidosryhmien pilotointiaikataulut ja ne sujuivat rutiininomaisesti.

Ensimmäisen asteen tuen tehtävien ja eskalaatiopolkujen määrittelykokouksessa käsiteltiin tällä kertaa lähinnä toisen yksikön alueelle kuuluvia tehtäviä, joten tällä kertaa olin kokouksessa kuuntelijan roolissa. Kokous ei kuitenkaan ollut osaltani turha, sillä se toimi hyvänä tiedonjakokokouksena, ja siinä käsiteltiin erityisesti erilaisten Azure-ylläpitoroolien tarvetta. Sain päivän aikana tehtyä suunnittelemani RDS-hallintaympäristöprojektiin liittyvät tehtävät, ja joidenkin rutiininomaisten ongelmanselvitysten lisäksi päivän aikana ei tapahtunut muuta merkittävää.

Keskiviikko 16.02.2022

Tänään on kaksi erilaista yksikkökokousta, mutta näiden lisäksi on vain yksi muu kokous, jossa käsitellään uuden HR-järjestelmän tukilomakkeen toteutusta ITSM-järjestelmään. Suunnitelmanani onkin, että saan päivän aikana edistettyä AD-tunnusten ylläpitoon liittyvää skriptiä mahdollisesti valmiiksi asti, sekä paria aiemmin lykkäämääni RDS-hallintaympäristön dokumentointitehtävää.

Päivän tavoitteet toteutuivat osittain. Kokoukset etenivät suunnitellusti, ja niistä ei syntynyt mitään erityistä mainittavaa. Päivän aikana tuli joitakin palvelupyyntöjä, joiden ratkaisemiseen jouduin käyttämään jonkin verran aikaa. Yksi näistä liittyi datansiirtoautomaatioon, jossa eräällä käyttäjällä näyttivät kadonneen tiedostot siirron jälkeen. Tutkimisen jälkeen syyksi paljastui kuitenkin se, että tiedostot olivat aikaisemmin tallentuneet tietokoneen paikalliselle kovalevylle, eivätkä näin sijainneet kotihakemistossa. Kyseinen ongelma liittynee siihen, miten Windows käsittelee paikallisen käyttäjäprofiilia ja uudelleenohjattuja kansioita resurssienhallinnan kirjastonäkymää käytettäessä. Kyseinen näkymä yhdistää nämä kaksi sijaintia yhteen näkymään, jolloin on teoriassa mahdollista, että käyttäjä tallentaa tiedostoja tietämättään paikalliselle levylle. Korjaus oli yksinkertainen, eli käyttäjää ohjeistettiin miten tiedostot saa kopioitua verkossa olevalle levylle. Paikalliseen käyttäjäprofiiliin tiedostoja tallennettaessa on riski tietojen katoamisesta, sillä kyseisestä sijainnista ei synny varmuuskopioita.

Päivän aikana sain myös lähetettyä useampia kokouskutsuja liittyen aiemmin käsittelemiini asioihin, eli juuri HR- ja AD-integraatioon sekä AD:n objektien omistajuuteen kohdistuvaan ehdotukseen liittyen. Sain tehtyä AD-tunnusten ylläpitoskriptin ensimmäisen osan testausvalmiiksi, mutta siihen tarvittavaa palvelutunnusta ei ole vielä luotu, joten sen testaus viivästyy. RDS-hallintaympäristön dokumentointitehtävät jouduin myös siirtämään eteenpäin, ja ne siirtyvät todennäköisesti ensi viikolle.

Torstai 17.02.2022

Torstaille on taas varattuna vain kaksi kokousta. Toinen niistä käsittelee tulevan ensimmäisen asteen tuen tehtävien määrittelyä, ja toinen on tämänhetkiseen ensimmäisen asteen tukeen liittyvä viikkokokous. Yöllä on myös poikkeuksellisesti suurempi VPN-infrastruktuurin muutos, jonka testaamiseen osallistun yön aikana. Muuten jatkan päivän aikana AD-tunnusten ylläpitoskriptin seuraavaa osaa ja datansiirtoautomaation jatkokehitystä.

Kokouksista ei syntynyt taaskaan mitään yllätyksiä ja ne etenivät rutiininomaisesti. AD-tunnusten ylläpitoskriptin toinen osa edistyi, mutta ei tullut vielä valmiiksi. Palvelutunnus ei kuitenkaan ole vieläkään valmis, joten todennäköisesti testaus viivästyy seuraavalle viikolle, mutta tämä ei aiheuta aikataulun lykkääntymistä. Datansiirtoautomaation jatkokehitys jäi myös muiden tehtävien jalkoihin tältä päivältä. Eräällä käyttäjällä esiintyi sama ongelma kuin edellisenä päivänä, eli tiedostot näyttivät kadonneen mutta olivatkin tallentuneena paikalliseen käyttäjäprofiiliin. Ongelman esiintyminen kahteen kertaan ei ole mitenkään hälyttävää ja ei siis aiheutunut suoraan itse datansiirtoautomaatiosta, mutta sen suhteen voi olla aiheellista pyrkiä kartoittamaan ongelman laajuutta myöhemmin, sillä se aiheuttaa lisäriskin datan katoamiselle. Paikallisesta käyttäjäprofiilista ei nimittäin oteta varmuuskopioita.

Päivän aikana selvitettäväksi tuli kuitenkin vaikea ratkaistava ongelma. Ongelma liittyy siihen, että tietyssä uudessa toimipisteessä työskentelee toisen julkishallinnon organisaation työntekijöitä oman organisaatiomme työntekijöidemme rinnalla. Työnjohdollisesti kaikki henkilöt kuuluvat organisaatioomme, mutta he käyttävät kuitenkin oman organisaationsa tietokoneita, VPN-yhteyksiä sekä muita resursseja. Tämän seurauksena heidän pitäisi pystyä tulostamaan dokumentteja oman organisaationi tulostimiin, mikä aiheuttaa kuitenkin teknisiä haasteita erinäisten reunaehtojen takia. Ongelma tuli ilmi melko myöhään iltapäivällä, joten ratkaisusta ei vielä päätetty, mutta erilaisia ratkaisuehdotuksia käytiin kyllä läpi. Ongelmia aiheuttavat erityisesti toisen organisaation VPN-ratkaisu, pilviratkaisuihin liittyvät GDPR- ja tietosuojavaatimukset salassa pidettävän tiedon osalta, sekä ratkaisun käytettävyys kirjautumisen osalta. Toisen organisaation työntekijöillä on nimittäin lisäksi käytössään kahdet eri tunnukset, ja ratkaisun tulee olla käyttäjien kannalta riittävän käytettävä. Palaan tähän ongelmaan ja sen ratkaisumahdollisuuksiin tarkemmin viikkoanalyysissä, sillä asiaa käydään vielä perjantaina varmasti läpi.

Perjantai 18.02.2022

Tänään kalenteriin on varattu kolme eri kokousta, joista yksi on yksikkökokous, toinen koskee datansiirtoautomaation kotihakemistojen siirtojen statusta, ja kolmas koskee älykorttikirjautumisen käyttöönottamista palvelimille. Näiden kokousten lisäksi suunnitelmissa on edistää datansiirtoautomaation kehityskohteita, sekä saada testattua ratkaisuja torstaiseen organisaatioiden väliseen tulostustarpeeseen.

Kokouksissa ei syntynyt merkittäviä yllätyksiä, paitsi palvelinten älykorttikirjautumisen osalta selvisi se, että käyttöönoton levittäminen ei ole aivan niin yksinkertaista kuin työasemille, sillä ylläpito jakautuu sekä asiakkaina toimiville sidosryhmille, että digitaalisen

perustan konesali- ja kapasiteettipalveluille. Käyttöönotosta pitää siis sopia erikseen kunkin sidosryhmän kanssa, mutta kokouksessa sovittiin pilotoinnista kaupunginkansliassa, johon digitaalinen perusta myös kuuluu.

Datansiirtoautomaation kehitystyö eteni, mutta en saanut sitä viimeisteltyä aivan loppuun aiempien viikon suunnitelmien mukaisesti, sillä tulostusratkaisun testaaminen kulutti aikaa. Testasin dokumentaation perusteella Microsoftin Universal Print -ominaisuutta, ja se näytti toimivan juuri niin kuin pitää. Käyttäjälisensseistä löytyi pieni ongelma, sillä kaikille lisensseille ei ollut aktivoitu tarvittavaa ominaisuutta, joten laitoin tästä kysymyksen eteenpäin. Testauksen onnistuminen ei kuitenkaan tarkoita vielä sitä, että toiminnallisuutta voidaan hyödyntää, sillä vierasorganisaation laitteiden tietoturva-asetukset saattavat estää sen käytön ja lisäksi tulostustyöt voivat sisältää henkilötietoja, joten GDPR:än vaatimukset tulee huomioida. Tekninen testaus tuli kuitenkin tehtyä, ja sain selvitettyä päivän aikana myös GDPR-asiaa pintapuolisesti. Käytännössä eteneminen vaatii yhteydenottoa organisaationi tietosuojavastaaviin, tietosuojan vaikutusten arviointia sekä keskustelua vierasorganisaation IT-henkilöstön kanssa siitä, että voiko ominaisuutta hyödyntää heidän tietoturvavaatimustensa puitteissa.

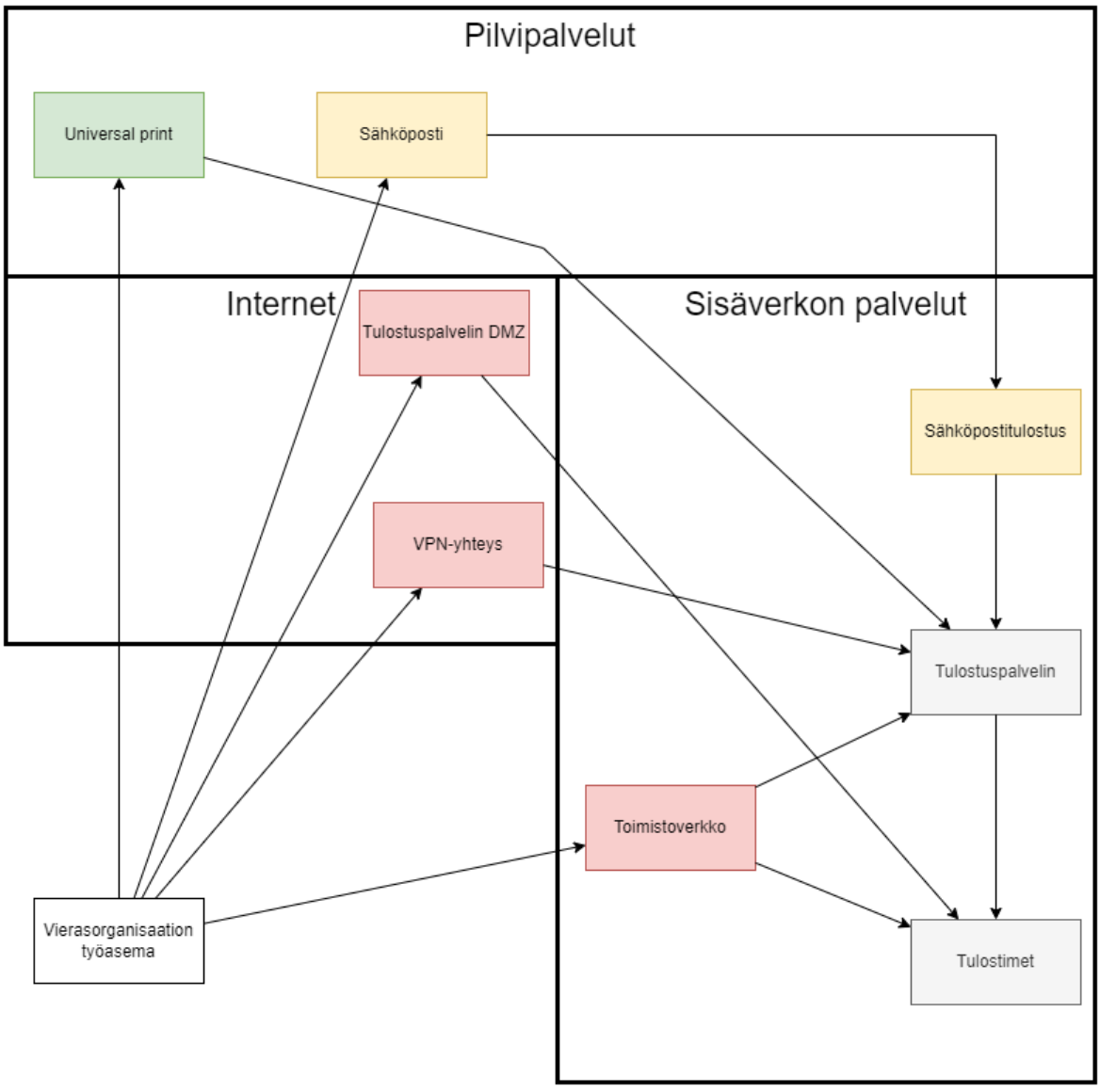
Viikkoanalyysi

Viikon tehtävät olivat pääosin rutiininomaista ongelmanselvitystä. Sekä RDS-hallintaympäristöprojektiin, että datansiirtoautomaatioon liittyi joitakin uudenlaisia ongelmanselvitystarpeita, mutta nekin olivat hyvin rutiininomaisia ja vaativat lähinnä aiemmin hankkimani tiedon mieleen palauttamista. Viikon merkittävin selvitystyö ja osaamisen kehittyminen liittyi vierasorganisaation tulostamistarpeeseen, sekä GDPR-asetuksen pohdintaan.

Kyseisessä tulostamistarpeessa vierasorganisaatio käyttää omia kannettavia tietokoneitaan, ja ne on liitetty heidän organisaationsa IT-infrastruktuuriin. Heidän työpisteensä on kuitenkin oman organisaationi erään yksikön toimipisteessä, missä ei ole muita internetyhteyksiä kuin organisaationi toimistoverkko, sekä vierailijoille tarkoitettu internet-yhteys. Tulostimet ovat verkkotulostimia, ja ne ovat organisaationi toimistoverkkoon yhdistettyjä. Tämän lisäksi organisaationi IT:llä ei ole mitään ylläpito-oikeuksia vierasorganisaation työasemiin.

Kuviossa 3 kuvataan erilaiset harkitsemani ratkaisuvaihtoehdot. Erilaisia ratkaisuvaihtoehtoja kerätessä piti huomioida verkkoyhteydet, palveluiden sijainti, organisaatioiden tietoturvakäytännöt, kuin myös käytettävyys ja hallittavuus. Yksinkertaisimpana ratkaisuna oli kytkeä laitteet suoraan verkkojohdolla toimipisteen sisäverkkoon, jolloin niistä olisi suora

pääsy tulostinpalvelimelle ja tulostimille. Tämä ei kuitenkaan todennäköisesti onnistu, sillä vierasorganisaatiolla näyttäisi olevan käytössä ns. always-on VPN-ratkaisu, joka tarkoittaa siis sitä, että tietokoneet yhdistävät aina VPN-yhteydellä kyseisen organisaation omaan verkkoon, ja reitittävät kaiken liikenteen sitä kautta. Oman organisaationi sisäverkon näkökulmasta liikenne tulisi siis Internetistä (vierasorganisaation verkosta), mistä ei ole sisäverkkoon suoraa pääsyä. Toisena ongelmana olisi tulostinten asentaminen työasemille, sillä se on myös todennäköisesti estetty käyttäjäoikeuksilla ja vaatisi vierasorganisaation tietohallinnon toimenpiteitä.



Kuvio 3. Harkitut tulostusmahdollisuudet eri teknologioita käyttäen. Väreistä punainen = todennäköinen tekninen tai käytettävyyseste, keltainen = mahdollinen hallinnollinen tai käytettävyyseste, vihreä = ei tiedossa olevia esteitä tai esteet todennäköisesti ratkaistavissa.

Toinen ajatus oli erillisen tulostuspalvelimen pystytys DMZ-alueelle. Tähän liittyy kuitenkin erilaisia tietoturvariskejä, sillä Windowsin tulostuspalvelusta on löytynyt vuonna 2021 useita tietoturva-aukkoja (Microsoft 2021i) ja palvelimen tulisi olla käytettävissä internetistä. Tämän lisäksi ratkaisuun liittyy ylläpito-ongelmia, sillä todennäköisesti tulostimien asennus pitäisi tehdä vierasorganisaation tietohallinnon kautta, mikä ei olisi hyväksyttävä ratkaisu ylläpidon kannalta.

VPN-yhteys taas voisi olla muuten toteutettava ratkaisu, mutta siihen liittyy merkittäviä käytettävyysongelmia, sillä VPN-yhteys pitäisi avata aina vain tulostamista varten, minkä lisäksi on todennäköistä, että se ei olisi teknisesti mahdollista johtuen vierasorganisaation VPN-ratkaisusta. Kahden eri VPN-asiakasohjelmiston samanaikainen käyttö ei kokemukseni perusteella ole todennäköisesti tuettua. Käytännössä jäljelle jäävät vain kaksi eri pilvipalvelua.

Ensimmäinen pilvipalveluista, eli tulostaminen pilvisähköpostin kautta lähettämällä viesti liitteineen tiettyyn sähköpostiosoitteeseen, on jo käytännössä olemassa, mutta sen käyttö on hallinnollisesti kiellettyä GDPR-asetuksen takia. Sinänsä GDPR ei itsessään estä palvelun käyttöönottoa, mutta organisaationi tiukan tulkinnan mukaisesti tulosteissa olevia henkilötietoja ei saa käsitellä pilvipalvelussa olevan sähköpostin kautta, vaikka data ei missään vaiheessa poistu EU/ETA-alueelta. Käsittääkseni yhtenä syynä tälle on lähetettyjen viestien jääminen sähköpostiin, jolloin henkilötietoja sisältävää materiaalia voi alkaa kertyä kyseisiin postilaatikoihin muodostaen potentiaalisesti henkilötietoja sisältävän henkilötietorekisterin.

Microsoftin Universal Print-ratkaisu poistaa kyseisen ongelman, sillä siellä tulostustöiden tyypillinen säilytysaika on muutaman päivän, ja enimmäissäilytysaika 10 päivää (Microsoft 2021h). Data on myös kryptattu sekä sen siirtyessä palveluun ja palvelusta, että sen odottaessa tulostusta. Suurena toimijana Microsoft mahdollistaa myös GDPR:ään liittyvien tietopyyntöjen toteuttamisen (Microsoft 2020). Pintapuolisesti kaikki ymmärtämäni GDPR:än vaatimukset siis täyttyvät, kunhan asianmukainen riskianalyysi on tehty. Kyseinen ratkaisu poistaa myös tulostinten asentamisen ongelman, sillä asennus onnistuu ilman tarvetta ylläpitäjän oikeuksille oman testaukseni perusteella, ja käyttäjä voi tehdä sen itsepalveluna ohjeiden pohjalta.

Teknisesti ratkaisu on käytännössä jo toteutettu tekemäni testauksen yhteydessä, mutta sen saattaminen tuotantokäyttöön vaatii lisäselvityksiä. Ensimmäisenä on GDPR-asetuksen tulkinta, sillä se ei kuulu omalle osaamisalueelleni. Oman näkemykseni mukaan riskienhallinnan näkökulmasta Universal Print -ratkaisun voisi rinnastaa internet-

palveluntarjoajien suorittamaan internet-liikenteen reititykseen. Merkittävimpänä erona on se, että palveluntarjoajana Microsoftilla on kryptatun datan salausavaimet omassa hallinnassaan, mutta tämän palvelun osalta Microsoft ei kuitenkaan käsittele tulostustyötä. Mikäli olen ymmärtänyt teknologian oikein, tulostustyö muodostuu tulostavan henkilön koneella, ja se ainoastaan siirtyy Microsoft-infrastruktuuria hyödyntäen muuttumattomana ja ilman sisällön lukemista lähdetyöasemalta kohdetulostimelle, kuten internet-liikenteen reititys.

Toisaalta GDPR-tietoa hakiessani päädyin myös kuntaliiton näkemykseen reilun vuoden vanhasta Schrems II -päätöksestä. Kuntaliiton (2021) tulkinnan mukaan "... henkilötietojen käsittelyllä EU/ETA –alueen ulkopuolella tarkoitetaan tilannetta, jossa tiedot on tallennettu EU/ETA –alueen ulkopuolelle ja lisäksi tilannetta, jossa EU/ETA –alueen sisälle tallennettuun tietoon pääsee etäyhteydellä EU/ETA –alueen ulkopuolelta." Kyseinen tulkinta tarkoittaisi sitä, että minkä tahansa etäyhteysratkaisun olemassaolo sisäverkon palveluihin tarkoittaisi sitä, että datan sijainti rinnastettaisiin EU/ETA-alueen ulkopuolella olevaksi. Etäyhteysratkaisut eivät nimittäin kokemukseni perusteella tyypillisesti ota kantaa siihen, mistä maasta etäyhteys otetaan. Kyseinen tulkinta on siis mielestäni tietotekniikan realiteetit huomioon ottaen naiivi ja ylivarovainen, sillä se poistaisi merkityksellisen eron datan säilyttämisestä EU/ETA-maiden sisä- ja ulkopuolella, kun otetaan huomioon etäyhteysratkaisujen yleisyys.

Tekninen ratkaisu vaatii siis vielä sen käyttöönoton läpikäyntiä organisaationi tietosuoja-asiantuntijoiden, sekä vierasorganisaation tietohallinnon kanssa. Jos mainitsemiani pilvipalveluita ei ole mahdollista käyttää, on hyvin mahdollista, että käytettävyyden kannalta hyvää ratkaisua ei voida toteuttaa ja vierasorganisaation työntekijöiden tulee aina tulostettaessa käyttää oman organisaationi konetta (joita heillä ei tällä hetkellä ole), tai yhdistää tietokone aina tulostettaessa suoraan tulostimeen USB-kaapelilla, mikä on kuulemieni kommenttien perusteella käytettävyydeltään erittäin huono ja työntekoa haittaava ratkaisu.

Universal Print voisi myös ratkaista Microsoftin (2021i) haavoittuvuuteen liittyviä ongelmia. Haavoittuvuuden ratkaisemiseksi on jouduttu tekemään epätäydellisiä ratkaisuja, ja haavoittuvuuden riskien täysi hallitseminen vaatii todennäköisesti merkittäviä ylläpidollisia toimenpiteitä ja niihin liittyvää ajankäyttöä tulevaisuudessa. Niiden toteuttaminen voi myös aiheuttaa käytettävyysongelmia organisaation sisällä. Tämän takia otan asian esille myös kyseisen haavoittuvuuden korjauksien toteutuksesta vastaavan yksikön kanssa lähiaikoina.

3.6 Seurantaviikko 6

Maanantai 21.02.2022

Tänään päivän tavoitteena on saada datansiirtoautomaation muutokset testauskuntoon, ja mahdollisesti jopa suoritettua uusiin ominaisuuksiin liittyvä testaus loppuun. Päivän aikana on toisaalta useampia kokouksia, joten suuri osa päivästä kuluu niihin sekä niihin valmistautumiseen. Kaksi kokouksista liittyvät automaatioihin, toinen niistä AD- ja uuden HR-järjestelmän väliseen integraatioon, ja toinen AD:n objektien omistajuuteen liittyvään prosessiin ja automaatioon.

Päivä eteni kokousten osalta odotusten mukaisesti, mutta datansiirtoautomaatiossa tuli yllättäviä ongelmia eräiden käyttöliittymämuutosten kanssa, ja ne vaativat lisäselvittelyä. Tältä osin en siis saavuttanut päivän tavoitteitani. Kokouksissa päätettiin lähteä edistämään niissä esiteltyjä projekteja, ja niihin sovittiin seurantakokouksia etenemisen seuraamiseksi. Päivän aikana autoin myös useampia kollegoitani eräissä teknisissä kysymyksissä (offline-tiedostojen ja haun indeksoinnin toiminta sekä AD-tunnusten attribuutteihin liittyviä kysymyksiä).

Tiistai 22.02.2022

Tiistaille on taas varattuna useita kokouksia, joista yksi koskee edellisen viikon viikkoanalyysissä kuvaamaani Universal Print -ominaisuuden käyttöönottoa. Toinen kokous koskee uuteen HR-järjestelmään liittyvää tietoturvakysymystä, joka pitää ratkaista ennen sen käyttöönottoa, ja kolmas on salasanojen nollaamiseen liittyvä ongelmanselvityskokous. Tämän lisäksi päivän aikana on myös yksi rutiininomainen viikkokokous. Suuresta kokousmäärästä huolimatta datansiirtoautomaatioon liittyvät muutokset tulisi saada tänään valmiiksi testaus mukaan lukien.

Päivän tehtävät etenivät suunnilleen suunnitelmien mukaisesti. Datansiirtoautomaation muutokset tulivat valmiiksi, mutta en saanut sitä testattua aivan tarpeeksi, että se olisi valmis tuotantoon viemiseksi. Universal Print -käyttöönottoon liittyvässä kokouksessa varsinaisia teknisiä esteitä ei ilmennyt ja sen laajempi käyttöönotto voisi myös olla mahdollista, eli kyseinen asia on riippuvainen organisaation tietosuojaohjeistuksen täyttymisestä. Kyseisen asian edistäminen jää kuitenkin seuraavalle viikolle hiihtolomaviikon takia, sillä tietyt avainhenkilöt ovat lomalla.

HR-järjestelmän tietoturvakysymys saatiin myös ratkaistua niin, että se ei aiheuta ongelmia ennen käyttöönottoa. Tämä liittyi uniikin tunnisteen itsepalvelurekisteröintiin, joka pitää vain käytännössä poistaa käytöstä ennen käyttöönottoa. Salasanojen nollaamiseen liittyvässä kokouksessa löytyi Azuressa olevan salasanan itsepalvelunollauksen osalta puute, joka koskee tiettyjä tunnuksia. Tämän selvittäminen piti ohjata asiantuntijoille, sillä en itse ylläpidä kyseistä toiminnallisuuden osaa, mutta virheilmoitusten perusteella kyseessä näyttäisi olevan puutteellinen palvelutunnuksen käyttöoikeusdelegaatio.

Keskiviikko 23.02.2022

Tänään on myös jonkin verran kokouksia, joista kaksi ovat rutiininomaisia viikkokokouksia. Tämän lisäksi päivän aikana on RDS-hallintaympäristön käyttöönottokokous, jossa sovittaneen sille lopullinen aikataulu. HR- ja AD-automaatioon liittyen on myös kokous erään asiakkaisiin kuuluvan sidosryhmän kanssa. Muita päivän työtehtäviä ovat datansiirtoautomaatioon liittyvän raportoinnin teko projektin etenemisen seurantaa varten, sekä edellisenä päivänä jääneen testauksen saattaminen loppuun.

RDS-hallintaympäristön käyttöönottokokouksessa saatiin sovittua lopullinen aikataulu käyttöönottoon liittyvälle pysyvien ylläpito-oikeuksien poistamiselle, kuin myös siihen liittyvien koulutusten ajankohta. HR- ja AD-automaation kokouksessa käytiin läpi erilaisia vaihtoehtoja ja sidosryhmän tarpeita, ja ratkaisun soveltuvuudesta päästiin näkemykseni mukaan yhteisymmärrykseen. Vaihtoehtoisena ratkaisuna oli eräällä toisella sidosryhmällä olevan IAM-järjestelmän (Identity and Access Management) laajentaminen tälle sidosryhmälle käyttöön, mutta ratkaisu vaatisi paljon räätälöintiä ja sen käyttöönotossa kestäisi todennäköisesti pidempään.

Datansiirtoautomaation raportointiskripti tuli valmiiksi, ja se käytännössä tutkii siirtolokeista, että kuinka paljon siirtoja on tehty, epäonnistunut ja kuinka paljon niitä on vielä tekemättä ja kerää tiedot soveltuvassa muodossa Excel-taulukkoon. Sain myös testauksen suoritettua loppuun, ja muutokset siirrettäneen tuotantoon huomenna. Päivän suunnitellut työtehtävät tulivat siis valmiiksi, vaikka pidin hieman lyhyemmän työpäivän.

Torstai 24.02.2022

Torstai on käytännössä kokousvapaa, joten suunnitelmana on saada työlistaa edistettyä. Tähän liittyvät RDS-hallintaympäristön käyttöönoton valmistelutehtävät, kuten dokumentointi ja käyttöoikeuksien ajantasaisuuden varmistaminen, tietyn tukipalveluiden ohjelmaasennuksia auttavan skriptin laajemman käytön mahdollistaminen, ja jos aikaa jää yli,

alkaa valmistella HR- ja AD-automaation tarkempaa teknistä määrittelyä. Sain myös palvelutunnuksen edellisinä viikkoina mainitsemaani toista HR-automaatiota varten, ja pyrin saamaan sen pilottikäyttöön tämän päivän aikana.

Sain päivän aikana edistettyä RDS-ympäristöön liittyviä tehtäviä, kuin myös edistämään mainitsemaani ohjelma-asennuksissa auttavaa skriptiä. Kyseinen skripti on päivitys toiseen vuosia vanhaan samankaltaiseen skriptiin, ja sen päivitys ei ole aivan niin suoraviivaista kuin muistin. Sillä voi käytännössä asentaa ohjelmiston etäkoneelle ilman, että siitä aiheutuu koneen käyttäjälle käyttökatkoa tai tarvetta sopia ohjelman asennusajankohtaa etukäteen, kunhan ohjelman asentaminen ei vaadi asennuksen aikaisia syötteitä. Tämä vähentää huomattavasti manuaalista työtä, kuin myös asennusten sopimiseen kuluvaa aikaa.

HR-automaatiota varten luodun palvelutunnuksen käyttöönotto jäi vielä tekemättä, sillä päivän aikana asiaa pohtiessani jäi vielä hieman epäselväksi, että mikä olisi paras palvelin sen alustaksi. Tämä voi myös vaatia keskustelua tiettyjen asiantuntijoiden kanssa, jotka ovat tämän viikon lomalla.

Perjantai 25.02.2022

Perjantaina ajattelin pitää lyhyemmän työpäivän, ja edistää samoja työjonoon jääneitä tehtäviä kuin torstaina. Päivä oli kokousten osalta myös täysin tyhjä.

Kärsin päivän aikana hieman keskittymisvaikeuksista liian monen samanaikaisen tehtävän takia, ja tämän takia päivän tuotokset jäivät ajankäytön huomioon ottaen vähäisiksi, vaikka huomioon ottaisi lyhyemmän työpäivän. Tätä tapahtuu silloin tällöin, ja tyypillisesti kokonaisuuden näkökulmasta se ei ole omaa työtehoani liiallisesti haittaavaa. Päivän aikana sain kuitenkin työstettyä ohjelmien asennusautomaatiota, sekä tehtyä RDS-hallintaympäristöön liittyviä tehtäviä.

Viikkoanalyysi

Viikon aikana tapahtui edistystä useammassa projektissa, joista merkittävimmät olivat datansiirtoautomaatioskripti sekä RDS-hallintaympäristön käyttöönotto. Datansiirtoautomaatioprojekti sinällään jatkuu vielä pitkälle kesään, mutta viimeisimpien muutosten jälkeen en usko, että itse automaation toiminnallisuuteen tarvitsee enää käyttää kehitysaikaa. Projektin vetovastuu on toisella projektipäälliköllä ja itselläni on vain tekniseen toteutukseen liittyvä vastuu. Kotihakemistojen siirtämistä tulee kuitenkin tapahtumaan myös jatkossa, ja

sen takia skripti on toteutettu niin, että sitä on mahdollista hyödyntää myös muihin tarkoituksiin.

Viikkoanalyyseistä on saattanut jo näkyä, että työhöni liittyy melko paljon erilaista automatisointia ohjelmoinnin ja skriptauksen kautta. Näihin liittyy jatkuvasti tiettyjä pohdittavia asioita, jotka ajattelin ottaa esille tässä viikkoanalyysissä. Ensimmäisenä huomioitavana asiana on ylläpidettävyys ja skripteihin liittyvän tiedon jakaminen. Datansiirtoautomaation yhtenä tärkeänä osana oli tehdä dokumentaatio, jota seuraamalla täysin ulkopuolinen ohjelmoija pääsee kiinni automaation perusajatukseen. Sinänsä automaatio ei ole koodin määrältä kovin pitkä (noin 1000 koodiriviä), mutta sen ymmärtämiseksi on hyvä olla dokumentoituna syyt, miksi jotkin asiat on tehty tietyllä tavalla. Koodissa on tietenkin jonkin verran kommentteja ja automaatioon liittyvä lokitus auttaa myös koodin ymmärtämisessä, mutta olen havainnut sen, että lisäksi on hyvä olla erilaisia prosessikuvauksia (kuten serantaviikon 1 kuvassa 4), että kokonaisuus hahmottuu. Tämä on huomioitava erityisesti kriittisemmissä skripteissä, kuten tulevassa HR- ja AD-automaatioskriptissä. Kyseinen ylläpidosta huolehtiminen onkin näkemykseni mukaan yksi syy, miksi ainakin omassa organisaatiossani järjestelmiä hankitaan mieluummin palveluna kuin itse asennettuina ja ylläpidettyinä.

Toinen skriptaukseen liittyvä itseäni jatkuvasti häiritsevä asia on versionhallinta. En ole niin tottunut ohjelmoija, että versionhallinnan käyttäminen olisi luonnollista osana normaalia toimintaa, vaan tyypillisesti versioin tiedostot käsin ja pidän edellisiä versioita tallessa tietyin kriteerein. Tämä menetelmä toimii kohtuullisesti, kun kukaan muu ei tee niihin muokkauksia, mutta organisaatiossa on myös muita osaavia skriptaajia ja ilman versionhallintaa tai selkeää prosessia skriptien muokkaus on aina niiden tekijän vastuulla. Olenkin jo pidempään pohtinut sitä, olisiko mahdollista saada otettua käyttöön jokin versionhallintajärjestelmä erilaisten skriptien ylläpitämiseksi. Tässä kuitenkin ongelmaksi on aina muodostunut se, että skriptaajat eivät oman kokemukseni mukaan ole pääsääntöisiä koodaajia. Täten versionhallinnan käyttö vaatisi sekä koulutusta, että toimintatapojen muutosta, ja tämä voisi olla hankalampaa erityisesti sellaiselle henkilöille, jotka käyttävät skriptaamista työkaluna harvemmin. Laajempien skriptien teon tarve on kuitenkin melko harvinaista, tyypillisemmin skriptit ovat kokemukseni mukaan lyhyitä ja tekevät yhden hyvin rajatun toimenpiteen, jolloin niiden versionhallinnalle ei ole samanlaista tarvetta. Jos kuitenkin jossain vaiheessa olisi hieman enemmän aikaa, voisin haastatella organisaation täysverisiä koodareita, jotka hyödyntävät versionhallintaa jatkuvasti, ja selvittää miten sen saisi mahdollisesti osaksi myös tätä ns. kevyempää ohjelmointia.

Viikon toisena teemana nousi esille ajanhallinta, ja erityisesti erilaisten töiden priorisoiminen. Käytännössä minulla on jatkuvasti enemmän tehtäviä kuin aikaa niiden tekemiselle, mutta aiemmin tämä ei ole aiheuttanut ongelmia, vaan saan varattua tehtäville sopivat määrät aikaa ja tehtyä ne aikataulujen puitteissa. Omalta kannaltani suurin ongelma muodostuu kuitenkin silloin, jos välittömästi valmistumista vaativat tehtävät on tehty, mutta työlistalla on kuitenkin edelleen paljon tehtäviä, joiden prioriteeteissä on epäselvyyttä. Tällaisissa tapauksissa saatan aloittaa yhtä tehtävää, mutta toinen tehtävä jää pyörimään päässä, jolloin yksittäiseen tehtävään keskittymisestä tulee erittäin vaikeaa. Tämä tapahtui esimerkiksi kuluneen viikon perjantaina, mutta en ole nähnyt ongelman olevan niin merkittävä, että sen osalta tarvitsisi ryhtyä toimenpiteisiin. Yksi parannettava asia on kuitenkin pitää selkeää kesken olevien tehtävien listaa ja priorisoida ne asianmukaisesti, sillä olen huomannut myös sen, että silloin tällöin jokin tehtävä saattaa jäädä pidemmäksi aikaa tekemättä unohtumisen takia.

Viikon ongelmanratkaisutehtävät olivat melko rutiininomaisia, ja pohjautuivat aiemmin hankkimaani tietoon. Tämä ei kuitenkaan tarkoita sitä, että tiesin valmiiksi ratkaisun jokaiseen ongelmaan, vaan ongelman syy oli helppo selvittää, ja ratkaisun toteuttamiseksi piti korkeintaan tutustua tekniseen referenssimateriaaliin. Esimerkiksi Azuren salasanan itsepalvelunollauksen ongelman selvittämiseksi tiesin yleisellä tasolla, miten ratkaisu toimii teknisesti, mutta jouduin kuitenkin tutustumaan Microsoftin (2022) tekniseen dokumentaatioon tämän toiminnallisuuden osalta. Kyseisen teknisen dokumentaation avulla pystyin myös varmistamaan, että korjauksen suorittaminen ei kuulunut omalle vastuualueelleni, ja siten ohjaamaan sen oikealle taholle.

3.7 Seurantaviikko 7

Maanantai 28.02.2022

Maanantai on jo valmiiksi täynnä kokouksia, jotka koskevat ensimmäisen asteen tuen vastuutaulukkoa, ITSM-järjestelmän kehityskohteiden edistymistä, datansiirtojen edistymistä ja ITSM-järjestelmän tilannetta yleisesti. Päivän aikana sovittaneen datansiirtojen uusien ominaisuuksien käyttöönotosta, sekä tietyn ITSM-järjestelmän lomakkeen kehityksestä, mutta muilta osin pyrin edistämään erityisesti RDS-ympäristöön liittyviä työtehtäviä, jos aikaa jää.

Päivän aikana ei syntynyt yllättäviä ongelmanselvitystehtäviä, ja kokoukset etenivät odotetusti. Datansiirtoautomaation ominaisuuksien tuotantoon vienti sovittiin seuraavalle päivälle, eli käytännössä tein muutokset illalla, että ne ovat seuraavana päivänä voimassa.

Muutokset koskivat datansiirtojen pakottamista tiettyjen lykkäyskertojen ja päivämäärän jälkeen, sillä nykyisellään käyttäjät ovat voineet halutessaan lykätä sitä ikuisesti.

ITSM-lomakkeen kehityksestä saatiin myös sovittua. Kyseisen lomakkeen tarkoituksena on mahdollistaa käyttäjille itsepalveluna tiettyjen tietojen ylläpito, ilman että IT-henkilöstöltä vaaditaan manuaalisia toimenpiteitä. Automaation toteuttamisesta on myöhemmin tällä viikolla aloitus/määrittelypalaveri, ja sen tekninen toteutus hankitaan eräältä palveluntarjoajalta. RDS-ympäristöön liittyvien tehtävien edistäminen ei mahtunut tämän päivän aikatauluun.

Tiistai 01.03.2022

Aamun aikana minun pitää seurata datansiirtoautomaation muutosten toimivuutta, minkä lisäksi päivän aikana on kaksi viikkokokousta. Muuten päivän aikana pitää edistää RDS-ympäristön käyttöönottoon liittyviä valmistelutoimenpiteitä, mihin liittyy ylläpitotunnusten läpikäymistä, sekä tiettyjen ominaisuuksien viimeistä testaamista.

Päivän aikana havaitsin yhden datansiirtoautomaatiossa olleen virheen, mutta se ei aiheuttanut näkyvää haittaa. Kyseinen bugi aiheutti ongelman samanaikaisia siirtoja rajoittavaan toiminnallisuuteen, mutta käytännössä samanaikaisia siirtoja on vielä parin päivän verran odotettavissa verrattain vähän, eli toiminnallisuus ei ollut vielä tarpeellinen. Bugi johtui yksinkertaisesta kirjoitusvirheestä, jonka virhe oli ns. try/catch-blokin sisällä, minkä takia en havainnut sitä testeissä. Tässä on myös hyvä esimerkki siitä, että try/catch-toiminnallisuutta kannattaa käyttää harkiten ja kohdistetusti, koska muuten se voi peittää oikeista ongelmatilanteista tulevat virheet alleen. Korjaus oli yksinkertainen, kun virhe löytyi.

Muuten päivän aikana tuli joitakin ongelmanselvitystilanteita, tai ehkä enemmän niiden ohjaamista asianmukaisille tahoille. Ensimmäinen ongelma liittyy Azuren vierastilien sähköpostien muuttamiseen, ja miten sen voisi tehdä mahdollisimman pienellä vaivalla sekä tietohallinnolle, että käyttäjälle itselleen. Tästä saatiin alustava testi tehtyä mutta on epäselvää, että onko ratkaisu toimiva. Muutoksen näkymisessä voi mennä jokin päivä, joten tilannetta pitää seurata.

Toinen ongelma liittyi sähköpostipalveluun ja yhteiskäyttöisten postilaatikoiden viestinlähetysoikeuksien delegointiin. Lyhykäisyydessään jos yhteiskäyttöinen postilaatikko on paikallisessa ympäristössä, kun taas sen käyttäjän postilaatikko on pilvisähköpostissa, ei normaaleja powershell-komentoja käyttäen voi delegoida lähetysoikeuksia kyseiseen paikallisessa ympäristössä olevaan yhteiskäyttöiseen postilaatikkoon. Tähän löytyi ratkaisu,

mutta se vaatii tiettyjen automaattitoiminnallisuuksien muuttamista niin, että oikeudet lisätään suoraan AD:ssa olevaan postilaatikon käyttäjätiliin, sen sijaan että käytetään Exchange Onlinen powershell-komentoja.

RDS-ympäristön käyttöönottoon liittyvistä työtehtävistä sain tärkeimmät tehtyä, mutta seuraavalle päivälle jäi vielä hieman tekemistä. Tärkein asia oli saada seuraavan viikon koulutusten kokouskutsut lähetettyä, sekä varmistaa että kaikilla tarvittavilla henkilöillä on ympäristöön käyttöoikeus. Tekemättä jäi vielä parin uuden ominaisuuden testaus, sekä käyttäjäkokemuksen parantaminen ympäristöön yhdistämisen osalta.

Keskiviikko 02.03.2022

Tänään yhtenä tavoitteena on saada kaikki loput RDS-hallintaympäristöön liittyvät valmistelutehtävät valmiiksi, sillä siihen liittyvät koulutukset ovat seuraavalla viikolla, jolloin se tulee täysimääräisesti tuotantokäyttöön. Tämän lisäksi päivän aikana on kaksi eri yksikkökokousta, salasanojen nollaamiseen ja siihen liittyvään käyttäjän tunnistamiseen kohdistuva kokous, kuin myös erään ITSM-järjestelmän lomakkeen toteutuksen lyhyt esittely, jossa olen sen tarkistavana osapuolena.

Sain käytännössä tehtyä kaikki suunnittelemani tehtävät loppuun, ja näistä merkittävin oli saada yhdistämiseen käytettävä RDP-tiedosto digitaalisesti allekirjoitettua ja lisättyä luotetuksi, ettei yhdistettäessä tarvitse aina reagoida varoitusikkunaan. Yleisemmin kyseisenlaiset varoitusikkunat olisi aina hyvä saada pois, sillä jos ohjeistuksen yhtenä osana on tietyn varoituksen ohittaminen, voi se kouluttaa jopa IT-ammattilaisia kyseisten varoitusten automaattiseen ohittamiseen kaikissa tilanteissa, mikä voi taas aiheuttaa myöhemmin tietoturvariskin. Tässä tapauksessa kyse oli siis varoituksesta, jossa pyydettiin tarkistamaan varmenteen oikeellisuus ja sen myöntäjä, mutta sen saa poistettua käytöstä määrittämällä varmenteen luotetuksi ryhmäkäytännöllä.

Yksikkökokouksissa ei tullut esille odottamattomia asioita, ja ITSM-järjestelmän lomakkeen esittely sujui hyvin. Lomakkeen kehittäjän pitää tehdä lomakkeeseen enää joitakin pieniä korjauksia, ja se on valmis. Tässä tuli myös taas esille se, että vaatimusten kommunikointi voi olla hyvin haastavaa. Eri henkilöt tulkitsevat vaatimuksia eri tavalla kuin myös eri olettamuksin, sillä ihmisten kieli on oman kokemukseni mukaan hyvin epätarkkaa. Väärinkäsitykset saatiin kuitenkin sujuvasti selvitettyä, vaikka asiointikielenä oli englanti kahdella eri aksentilla, ja seuraavassa esittelyssä lomakkeen voi odottaa olevan toiminnallisuuksiltaan valmiina.

Salasanojen nollaamiseen liittyvässä kokouksessa käsiteltiin puhelimitse tapahtuvan tunnistamisen ongelmia, eli miten voidaan todentaa IT-tukeen soittavan henkilön henkilöllisyys sellaisella varmuudella, että tunnuksen salasanan voi nollata. Tässä keskustelussa huomioitiin erilaisia uhkia, ja päädyttiin mielestäni ainoaan toimivaan ratkaisuun, jos kyseistä palvelua halutaan puhelimitse antaa. Käytännössä pitää löytää jokin sellainen tieto tai tietojen yhdistelmä, jotka eivät ole muiden tiedossa tai helposti selvitettävissä, jotka ovat kuitenkin IT-tuen tarkistettavissa soittajasta riippumattomasti. Yhtenä osana tätä voi olla soittajan puhelinnumeron vertailu nollattavan tunnuksen puhelinnumeroon, huomioiden kuitenkin mahdollisuus soittavan numeron väärentämiseen (spooffaus). Päivän aikana kulunvalvontajärjestelmän uusimisprojektiin liittyen piti myös selvittää joitakin tietoliikenneasioita, mutta ne olivat rutiininomaista tekemistä.

Torstai 03.03.2022

Torstaille on kalenterissa joitakin kokouksia, joista yksi käsittelee aiemmin esiin tuomani Universal Print -ominaisuuden käyttöönottoa, toinen tiettyjen vakiomuutosten käsittelyprosessia, kolmas eräiden palvelinten siirtoa palveluntuottajalta toiselle, ja vielä lisäksi on yksi viikoittainen seurantakokous. Näiden lisäksi päivän tavoitteina on tarkkailla datansiirtoautomaation etenemistä, koska pakotettuja siirtoja voi ensimmäistä kertaa alkaa tänään lykkäyskertojen tullessa täyteen. Alan myös valmistella maanantaista RDS-hallintaympäristön koulutusta varten materiaalia niin, että saan sen viimeisteltyä perjantaina. Työjonossa on myös yksi palvelupyyntö, joka pitäisi saada viimeisteltyä tänään.

Universal Print -kokouksessa saatiin sovittua ominaisuuden käyttöönoton edistämisestä, mihin kuuluu sivun pituisen esityksen tekeminen siihen liittyvistä tietosuoja- ja muista käytännön asioista. Tämän lupasin saada valmiiksi perjantaina, niin asiaa saadaan edistettyä. Käytännössä tätä varten tulee vain saada tarvittavat tietosuojan arvioinnit ja käyttöönottopäätökset tehtyä, itse tekninen toteutus on pilotin jäljiltä käytännössä valmis. Datansiirtoautomaation seuraamisesta ei syntynyt yllätyksiä, ja kaikki näytti toimivan kuten piti. Samanaikaisten siirtojen määrät pysyivät kohtuullisina, ja sain seurattua uusien ominaisuuksien toimintaa niin, että uusia bugeja ei esiintynyt.

Koulutusmateriaalista sain rungon luonnosteltua, ja saan sen tehtyä loppuun kuin myös varmistettua demojen toimivuuden huomenna. Sain myös mainitsemani palvelupyynnön tehtyä loppuun, se liittyi suuren AD-ryhmäjoukon luomiseen, mitä varten kannatti tehdä skripti. Päivän aikana tuli myös asiakkaalta pyyntö saada lista erään sähköpostin jakelulistan henkilöiden sähköpostiosoitteista. Pyyntöön liittyy myös kyseisen listan saamisen kuukausittain, joten teen tätä varten skriptin, jonka asiakas voi suorittaa aina halutessaan

kyseisen listan tuottamiseksi. Hieman haasteellisemmaksi tämän tekee se, että asiakkaan tietokoneella ei ole tiettyjä ylläpitotyökaluja asennettuna, joten toteutusta ei voi tehdä aivan samoin kuten normaalisti, vaan se vaatii hieman monimutkaisemman lähestymistavan.

Perjantai 04.03.2022

Päivä on lähes kokonaan kokoukseton, päivän aikana on ainoastaan yksi HR- ja AD-automaatioon liittyvä lyhyt suunnittelukokous. Päivän aikana tavoitteina on saada RDS-hallintaympäristön koulutusmateriaali valmiiksi, varmistaa että kaikki siihen liittyvä ohjeistus on ajan tasalla, sekä saada kirjoitettua eilen mainitsemani dokumentti Universal print-toiminnallisuuteen liittyen. Jos tämän lisäksi jää vielä aikaa, käytän sen HR- ja AD-automaation teknisen suunnitteludokumentaation työstämiseen.

Päivän työtehtävät toteutuivat melko hyvin suunnitelmien mukaisesti, ja mitään merkittäviä yllätyksiä ei tapahtunut. Suunnittelukokouksessa käytiin läpi mm. automaatiota sivuavan toisen projektin resurssointia, sekä teknisiä vaatimuksia. RDS-hallintaympäristön koulutusmateriaali tuli valmiiksi, ja Universal print-toiminnallisuuden dokumentti tuli miltei valmiiksi. Pidin taas normaalia lyhyemmän päivän kertyneiden saldotuntien poispitämiseksi, minkä takia en saanut aivan kaikkea suunniteltua valmiiksi.

Viikkoanalyysi

Viikon aikana osaamiseni kehittyi taas ensisijaisesti kertauksen kautta, sillä merkittäviä uusia ongelmia ei esiintynyt. Jouduin kuitenkin, kuten useimpina muina viikkoina, hakemaan ja kertaamaan tietoa erinäisistä teknisistä dokumenteista. Yhtenä esimerkkinä on Azure AD:n vierastilien sähköpostiosoitteen muuttaminen. Tämä tilanne tapahtuu, kun vierasorganisaation henkilö on kutsuttu vieraaksi esimerkiksi Microsoft Teamsiin, ja henkilön sähköpostiosoite muuttuu. Tällöin kirjautuminen ei enää onnistu ilman, että vierastiliin tehdään muutos (Microsoft 2022b).

Microsoft (2022b) mainitsee myös sen, että aikaisemmin tili on pitänyt poistaa ja kutsua uudelleen. Tämä oli myös oma tietoni asiasta asian tultua esille myös aiemmin viime vuoden puolella. Dokumentaation lukeminen uudelleen kuitenkin toi esille myös tämän uuden vaihtoehdon, joka on huomattavasti käyttäjäystävällisempi ja vähemmän vaivaa kuin aiempi toimintatapa. Päiväkirjamerkinnän aikaan en vielä ollut ehtinyt tutustua kyseiseen dokumentaatioon uudestaan, minkä takia siinä ei viitata suoraan tähän menetelmään, vaan juuri aiempaan toimintatapaan.

Viikon aikana työtehtävät keskittyivät myös RDS-hallintaympäristöprojektin edistämiseen, sillä toimin siihen liittyvänä kouluttajana projektin teknisenä projektipäällikkönä toimimisen lisäksi. Kyseiseen ympäristöön liittyi kuitenkin viikon aikana lähinnä käyttöönottoon valmistelevia toimenpiteitä, eikä suoranaisten teknisten ongelmien ratkaisua. Käyttöönotosta syntyy kuitenkin muutos ylläpito-oikeuksien toimintatapaan, mistä odotan aiheutuvan alkuun haittaa, sillä kokemuksieni perusteella toimintamallien muutoksista syntyy aina alkuun hieman hämmennystä ja totuttelua. Tämän takia valmistelu on erityisen tärkeää, sillä kaikki ylimääräiset huomioimattomat ongelmatilanteet lisäävät tästä aiheutuvaa kuormitusta tarpeettomasti.

Muutos vaikuttaa erityisesti oman yksikköni toimintaan, sillä siihen liittyy pysyvien ylläpito-oikeuksien poistaminen työasemien ylläpitotunnuksilta, että kyseiset oikeudet saadaan monivaiheisen tunnistautumisen taakse suojaan. Tietoturvan kannalta tällä saavutetaan merkittävä hyöty, sillä tällöin ylläpitotunnuksen joutuminen vääriin käsiin ei vaaranna heti koko työasemaympäristöä. Tämä estää esimerkiksi sivuttaisen liikkumisen verkossa, koska ilman mahdollisuutta lisätä ylläpitäjän oikeuksia ilman monivaiheista tunnistautumista, ei ylläpitotunnuksella ole oikeutta esimerkiksi etäkirjautumiseen. Sivuttaisen liikkumisen riskin vähentämiseen on useita toimintatapoja ja tekniikoita, kuten esimerkiksi juuri monivaiheinen tunnistautuminen, minimioikeuksien periaate, sekä ylläpito-oikeuksien eriyttäminen eri ylläpitotunnuksille (NCSC 2018). Näistä useimmat ovat jo käytössä omassa organisaatiossani, mutta tämä muutos on mielestäni merkittävä parannus ylläpitotunnusten tietoturvaan.

Datansiirtoautomaatiossa jouduin perehtymään tarkemmin siihen, miten WPF (Windows Presentation Framework) ja käyttöliittymiin liittyvä säikeistys toimii Powershellin kanssa. Käytännössä lykkäystoiminnon toteuttamiseksi skriptiä suoritettaessa yksinkertaisin tapa saada käyttäjälle hyvä käyttäjäkokemus oli simuloida ohjelmallisesti napinpainallus, jolloin käyttöliittymä käyttäytyy kuten käyttäjä olisi itse painanut nappia. Tässä jouduin kuitenkin käyttämään hieman yrityksen ja erehdyksen menetelmää, sillä vaikka olen rakentanut käyttöliittymiä ja monisäikeisiä ohjelmia muilla kielillä en ollut varma, miten se käytännössä toimii Powershellin kanssa. Tässä tapauksessa Powershell käytännössä käyttää C#-kieltä ja WPF:ää taustalla, mutta sen säikeistys ei toimi suoraan käyttöliittymän kanssa, jos käyttöliittymälle yrittää lähettää tapahtumia (event) toisista säikeistä. Käytännössä kun yritin saada käyttöliittymän napinpainallusta simuloitua, jäi käyttöliittymä jumiin ikään kuin ns. tapahtumia tuottava säie (event dispatching thread) olisi jäänyt jumiin. Tähän löytyi kuitenkin suoraan ratkaisu eräästä blogista, missä kehotettiin käyttämään tiettyjä Windows formsin toiminnallisuuksia ApplicationContext-luokan kautta (LeMaire 2016).

Ratkaisua piti tietenkin vielä soveltaa jonkin verran, koska kirjoittaja yritti ratkaista hieman erilaista ongelmaa, mutta se antoi suoraan vastauksen siihen, miksi aiemmat yritykseni eivät olleet toimineet. Sain tästä myös hyvän pohjan tulevaisuuden Powershell-käyttöliittymien tekoa varten.

Viikon aikana jouduin myös tutustumaan hieman tarkemmin organisaationi GDPR- ja tietosuojaohjeistukseen Universal Print-ominaisuuden takia. Tätä tulen tarvitsemaan myös muissa projekteissa, sillä käytännössä organisaatiossani tulee tehdä kaikista uusista henkilötietoja käsittelevistä prosesseista ja järjestelmähankinnoista tietosuojan vaikutusten arviointi, jolla voidaan arvioida siihen liittyvät riskit ja varmistaa henkilötietojen käsittelyn olevan GDPR-säädösten mukaisia. Muilta osin viikon työtehtävistä tai ongelmista ei ole syvällisempää raportoitavaa.

3.8 Seurantaviikko 8

Maanantai 07.03.2022

Päivä on taas melko täynnä kokouksia, minkä lisäksi tänään on RDS-hallintaympäristöön liittyvä koulutus, jossa toimin kouluttajana. Kaksi kokousta liittyy HR- ja AD-järjestelmien integraatioon, joista toisessa on osallistujia HR-järjestelmän puolelta, ja toisessa käydään oman organisaationi asiantuntijoiden kanssa sisäisesti läpi alustavaa määrittelyä ja projektin etenemistä. Tavoitteina näistä kokouksista on saada selvä kuva siitä, mitä dataa HR-järjestelmästä on mahdollista tuoda, sekä saada tarkemmin selville, miten se teknisesti tapahtuu. Tämän lisäksi päivän aikana on kulunvalvonnan uusimisprojektin seurantapalaveri. Päivän kokousten ulkopuolisen ajan suunnittelen käyttäväni koulutukseen valmistautumiseen, sekä HR-järjestelmän integraation määrittelydokumentin työstämiseen.

Päivän aikana ei syntynyt yllätyksiä ja se sujui suunnitelmien mukaisesti. HR- ja AD-järjestelmien integraatiokokouksesta selvisi tarvittavat tiedot, ja niiden perusteella sovittiin siirrettävään dataan liittyvistä lisäyksistä. Tämän lisäksi datan siirtämisen tekninen toteutus selvisi, ja se erosi hieman olettamastani. Muutos ei ole kuitenkaan olennaisesti merkittävä, käytännössä data siirtyy erään toisen automaatiopalvelimen kautta.

Päivän aikana tein vielä viimeistelytoimenpiteitä koulutusmateriaaliin ja varmistin demojen toimivuuden. Sain myös kirjoitettua HR- ja AD-järjestelmien integraatiodokumenttia eteenpäin, ja sen suhteen ei ollut toisessa kokouksessa suurta mainittavaa. Siellä tuli kuitenkin jo esille huomioitavia asioita, ja kyseinen kokous pidetään joka toinen viikko projektin etenemisen seuraamiseksi ja eri näkökulmien esille tuomiseksi.

Koulutus sujui suunnitelmien mukaisesti, ja siellä tuli hyviä kommentteja, joista yksi liittyi RDS-hallintaympäristön kehittämiseen. Muutoshallinnan läpinäkyvyyden ja tiedottamisen näkökulmasta eräs koulutuksen osallistuja pyysi ylläpitämään ympäristöön tehtävistä parannuksista ja muutoksista muutoslokia. Tämä oli erinomainen ehdotus ja looginen paikka muutoslokille on muun dokumentaation kanssa tietämyskannassa (knowledge base). Koulutukseen valmistautuessani havaitsin myös tarpeen siihen liittyvien käyttöoikeuksien tilauslomakkeelle, joka pitää myös saada työn alle. Näin lomakkeesta saadaan määrämuotoinen kaikkien tarvittavien tietojen osalta sen sijaan, että tarvitsee tehdä vapaamuotoinen tukipyyntö.

Tiistai 08.03.2022

Tänään kalenterissa on taas joitakin kokouksia, mutta aikaa on myös muille työtehtäville. Aamusta minun pitää testata joitakin RDS-ympäristön ominaisuuksia ja loppuajan suunnittelen käyttäväni dokumentointiin. Minun täytyy myös tehdä erään tilauslomakkeen testausta, jonka olin alustavasti suunnitellut tälle päivälle aiemmin. Päivän kokouksista kaksi on viikoittaisia seurantakokouksia, yksi on ITSM-järjestelmän uusien ominaisuuksien esittelytilaisuus, ja viimeisessä käydään läpi uudesta HR-järjestelmästä tapahtuvaa datansiirtoa.

Päivän aikana en saanut edistettyä dokumentaatiota täysin haluamallani tavalla, sillä jouduin vaihtelemaan hieman liian usein eri työtehtävien välillä. Näihin kuului tietty ongelmanratkaisu, joka liittyi päivämäärämerkkijonon muotoon. Syytä ei löytynyt suoraan dokumentaatiosta, mutta google-haulla löytyi selitys, ja syynä oli /-merkin erikoismerkitys, jossa se korvataan järjestelmän päivämääräerottimella. Yhdysvaltojen päivämäärissä esimerkiksi päivämääräerotin on /-merkki, kun taas Suomessa se on piste. Eri tietokoneiden vaihtelevat kieliasetukset siis loivat erilaisia merkkijonoja, mikä vaikeutti erään toiminnallisuuden automaatiota. Tämä saatiin kuitenkin korjattua muuttamalla /-merkki pisteeksi, jolloin sillä ei enää ole erikoismerkitystä.

HR-järjestelmän datansiirtoon liittyvät käytännön asiat tuli myös sovittua, ja siirtoprosessi saataneen käyntiin järjestelmän käyttöönoton yhteydessä, vaikka varsinainen automaatio ei olisikaan vielä valmis. Kyseistä dataa voidaan kuitenkin hyödyntää erilaisissa manuaalisissa prosesseissa, kuten nykyisen HR-järjestelmän dataa on hyödynnetty.

Keskiviikko 09.03.2022

Edistän taas päivän aikana samoja työtehtäviä, mitä aiemminkin tällä viikolla, sillä olen aiempina päivinä aliarvioinut dokumentointiin menevän ajan. Minun täytyy RDS-hallintaympäristön dokumentaation päivittämisen lisäksi päivittää datansiirtoautomaation dokumentaatio muutosten osalta ajan tasalla. Päivän aikana on kolme erilaista toistuvaa kokousta, joista yhdessä käsitellään ensimmäisen asteen tuen toimittajan muutosta, toinen liittyy HR-järjestelmiin ja erityisesti uuden järjestelmän käyttöönottoon liittyviin asioihin, ja kolmas on tiedonvaihtokokous pienen asiantuntijajoukon välillä.

Päivän aikana sain dokumentaation työstettyä muilta osin valmiiksi, mutta RDS-hallintaympäristön tekninen Powershell-dokumentaatio ja muutosloki jäivät vielä kesken. Tavoitteena onkin saada tämä dokumentaatiotehtävä huomisen aikana valmiiksi, vaikka kalenteri näyttää sen suhteen jo hyvin täydeltä. Dokumentaation valmistumiselle on kuitenkin aikaraja tämän viikon perjantaina, jolloin dokumentaation tulee olla täysin tarkasteltavissa.

Päivälle osui myös yksi ylimääräinen kokous, jossa käsiteltiin kertakirjautumisen määrittämistä ITSM-järjestelmään toisesta Azure AD -ympäristöstä. Tätä varten mukana on ulkoisen palveluntarjoajan konsultti, ja kokouksessa olivat kaikki tarvittavat sidosryhmät mukana. Kokouksessa saatiin käytyä läpi tarvittavat oikeudet ja määritykset, ja varsinaista konfiguraatiota varten varattiin seuraavalle päivälle uusi kokousaika pienemmälle joukolle. Muutos voi kuitenkin vaatia lisäselvittelyjä, mutta sen saaminen valmiiksi nopeasti on kriittistä sujuvan toiminnan takaamiseksi.

Uuteen HR-järjestelmään liittyvässä kokouksessa selvisi HR-järjestelmässä olevia mahdollisia prosessiongelmia, jotka saattavat joissain tapauksissa hidastaa datan saamista HR- ja AD-järjestelmien automaatiolle. Käytännössä tämä voi siis tarkoittaa, että tunnusten luonti viivästyy, jolloin uusi työntekijä ei saa heti käyttäjätunnuksia käyttöönsä, mikä hyvin monessa työtehtävässä estää töiden tekemisen. Tämä pitää huomioida automaation suunnittelussa niin, että tämänkaltaisissa tapauksissa tunnukset on mahdollista luoda myös HR-järjestelmästä riippumattomasti ja myöhemmin varmistaa uniikkien tunnisteiden vastaavuus eri järjestelmien välillä. Tämä ei kuitenkaan poista automaation hyötyjä, sillä jos tunnusten manuaalista saadaan vähennettyä edes 75 prosenttia, on ajansäästö edelleen merkittävä. Tässä vaiheessa on vielä kuitenkin vaikeaa arvioida, että kuinka suuresta ongelmasta on kysymys, mutta se on huomioitava prosessissa.

Torstai 10.03.2022

Torstai on käytännössä täynnä kokouksia, joten muiden työtehtävien edistämiselle ei ole juurikaan aikaa. Niiltä osin kuin aikaa on, jatkan RDS-ympäristön powershell-dokumentaation työstämistä. Päivän kokoukset käsittelevät AD:n ja ITSM-järjestelmän integraatiota, yhteistyötä erään sidosryhmän kanssa, sekä toisen Azure AD -ympäristön kertakirjautumisen mahdollistamista ITSM-järjestelmään. Tämän lisäksi päivän aikana on ITSM-järjestelmän kehityssprintin demokokous, sekä RDS-hallintaympäristön ohjausryhmä.

Kokoukset etenivät pääosin odotetusti päivän aikana. Aamun AD:n ja ITSM-järjestelmän integraatiokokouksesta sain tehtäväksi dokumentoida siihen liittyvät eri ympäristön osat, sillä kokouksen osallistujista minulla on paras kokonaiskuva eri tietolähteistä ja niiden suhteista. Yhteistyökokouksesta ei vielä tullut itselleni tehtäviä, mutta siihen liittyen sovittiin toinen kokous, jossa tullaan käymään läpi sidosryhmän uusien henkilöiden IT-oikeuksien tilaus- ja toimittamisprosessia. RDS-hallintaympäristön ohjausryhmässä saatiin tarvittavat päätökset ympäristön käyttöönotosta ja jatkokehityksestä kesää kohti mentäessä.

Päivän mielenkiintoisin tehtävä liittyi kertakirjautumisen (SSO) määrittämistä ITSM-järjestelmään. Kyseisessä kokouksessa oli mukana kyseisen toiminnallisuuden ulkoinen asiantuntija, sekä kertakirjautumisen lähdeympäristön ylläpitäjiä. Toiminnallisuus saatiin valmiiksi kokousajan puitteissa, ja omana roolinani oli toimia olemassa olevan ympäristön teknisenä asiantuntijana. Kokouksessa oli siis kaikki tarvittava asiantuntemus paikalla, minkä takia ratkaisemattomia ongelmia ei syntynyt. Kyseessä oli myös erittäin aikakriittinen tehtävä, sillä kyseistä ominaisuutta tarvitaan jo seuraavalla viikolla.

Tämän lisäksi sain edistettyä dokumentaatiota jonkin verran, ja saan sen seuraavana päivänä valmiiksi.

Perjantai 11.03.2022

Perjantaina kalenterissani on RDS-hallintaympäristön koulutus, jossa toimin kouluttajana. Lisäksi päivään mahtuu seuraavan ITSM-järjestelmän kehityssprintin suunnittelukokous, mutta muita ennalta sovittuja kokouksia ei päivän aikana ole. Päivän muihin työtehtäviin kuuluvat RDS-hallintaympäristön dokumentaation viimeistely ja julkaisu, ITSM- ja AD-integraatioon liittyvä tietovirtakuvauksen tekeminen, eri organisaatiotasojen selvitys HR-datasta, sekä HR- ja AD-integraation teknisen dokumentaation työstäminen. Näistä viimeisen valmistumiseen tulee menemään pidempään aikaa, mutta tavoitteena on saada muut mainitsemistani tehtävistä valmiiksi.

Aamun koulutus meni pääpiirteittäin suunnitellusti, mutta siinä tapahtui eräs ongelma liittyen RDS-hallintaympäristöön kirjautumiseen. Tämä ei kuitenkaan vaikuttanut merkittävästi koulutuksen sisältöön, mutta nousi ylimääräiseksi selvitettävien asioiden listalle ja vaati hieman improvisointia. Koulutuksen jälkeen asiaa tutkiessani ongelmaan liittyvää tietoa löytyi hyvin niukanlaisesti ja ohjasin ongelman selvityksen ympäristön ylläpitäjille, jotka voivat tutkia lokeista mahdollisia syitä ongelmalle. Ongelma ei kuitenkaan näyttäisi olevan tarpeeksi vakava, että se lykkäisi ympäristön seuraavalla viikolla tapahtuvaa käyttöönottoa, sillä se ei estä ympäristön käyttöä ja näyttää hetkelliseltä satunnaiselta ongelmalta. Ongelma poistui itseltäni heti koulutuksen jälkeen, ja se liittyi älykortin käyttämiseen kirjautumisessa.

Muutoin sain päivän aikana edistettyä työtehtäviä odotetusti. RDS-hallintaympäristön dokumentaatio tuli viimeisteltyä ja sain sen julkaistua ohjekirjastoon, ja sain ITSM- ja AD-integraatioon liittyvän tietovirtakuvauksen tehtyä ja lähetettyä tarvittaville sidosryhmien henkilöille. Organisaatiotasojen selvitys HR-datasta oli hyvin nopea toimenpide lyhyellä Powershell-skriptillä, ja sain senkin toimitettua eteenpäin. Sain myös valmisteltua HR- ja AD-integraation teknistä määrittelyä eteenpäin tietomallitasolle.

Viikkoanalyysi

Kohtuullisen suuri osa viikosta kului RDS-hallintaympäristön käyttöönoton valmisteleviin toimenpiteisiin, johon kuuluivat viikolla järjestetyt kaksi koulutusta, joissa toimin kouluttajana. Toisessa näistä RDS-hallintaympäristössä esiintyi ongelma, josta seurasi jonkin verran ongelmanselvitystä. Viikon aikana juurisyytä ei kuitenkaan vielä löytynyt. Yksi erään kollegani esittämä idea ongelman syylle oli virustorjuntatuotteen vaihto, sillä sen laajempi käyttöönottopilotointi alkoi juuri tällä viikolla, ja sen aiemmissa testeissä on löytynyt erilaisia hyvin odottamattomia ongelmia. Kyseinen ongelmanratkaisu jatkuu kuitenkin seuraavalla viikolla, sillä ongelmanratkaisua hankaloittaa ongelman satunnaisuus.

Viikon toisena merkittävänä tehtävänä edistymisen osalta oli HR- ja AD-järjestelmien välinen integraatio, ja erityisesti määrittelyn edistyminen. Erilaisia tietovirtoja on kuvattu aiemmassa viikon 5 viikkoanalyysissä, mutta nyt määrittelyn kautta yhteydet erilaisiin tietojärjestelmiin ja myös sidosryhmien tarpeet alkavat olla selkeämpiä. Käytännössä integraatiossa tulee huomioida eri sidosryhmien ja niiden organisaatiorakenteiden tarpeet, että integraation kautta luotavat ja päivitettävät tunnukset saadaan mahdollisimman valmiiksi. Tunnusten luonnissa tulee myös huomioida erilaisista virhetilanteista viestittäminen, sekä tunnusten tietojen ilmoittaminen oikealle taholle, joka on yleensä työntekijän esimies.

Näiden lisäksi on huomioitava toimenpiteiden jäljitettävyys lokitiedostojen kautta, että voidaan jälkikäteen selvittää millä perusteella automaatio on tehnyt jonkin toimenpiteen. Valtuutusketjussa hyväksyttävä peruste ei koskaan ole se, että automaatti teki jonkin asian, vaan sille pitää aina löytyä valtuutus, esimerkiksi asianmukaisesti valtuutetun henkilön tekemien tai hyväksymien asetusmäärittelyjen kautta.

Kun määrittely saadaan valmiiksi, ei järjestelmän varsinainen ohjelmointi ole aiemman ohjelmointikokemukseni perusteella erityisen monimutkainen asia. Toteutuksessa tulee kuitenkin huomioida järjestelmän ylläpidettävyys, sillä olen kohdannut useita sellaisia järjestelmiä, joiden tekijä on vaihtanut työpaikkaa, ja järjestelmä ei ole käytännössä enää kehitettävissä tai ylläpidettävissä. Tämän takia olen usein kallistunut jonkin toiminnallisuuden hankkimiseen palveluna sen sijaan, että se kehitetään itse, mutta tässä tapauksessa aikataulupaine automaation saamiselle käyttöön on suuri, ja tämän takia olen poikkeuksellisesti itsetehdyn järjestelmän kannalla. Tämä mahdollistaa myös nopean reagoinnin järjestelmän muuttuviin tarpeisiin ja määrittelyn tarkentamisen. Taulukossa 2 on kuvattu pohtimiani riskejä ja mahdollisuuksia näiden kahden eri hankintamallin välillä omien kokemuksieni perusteella.

Taulukko 2. HR- ja AD-integraatiojärjestelmän mahdollisuuksia ja riskejä. (+) tarkoittaa mahdollisuutta, (-) tarkoittaa riskiä.

Itse kehitetty järjestelmä	**Palveluna hankittu järjestelmä**
(+) Helppo räätälöidä, teoriassa kaikki on mahdollista	(-) Räätälöinti voi vaatia raskaan kehitysprosessin, ei välttämättä aina mahdollista
(+) Nopea toteuttaa	(-) Hankintaprosessi julkishallinnossa voi kestää pitkään
(+) Hyvin tehtyä määrittelyä voi hyödyntää tulevaisuuden palveluhankinnassa ja täydentää kokemusten perusteella	(-) Määrittely tulee tehdä täysin valmiiksi ennen hankinnan aloittamista
(-) Järjestelmän ylläpito ja valvonta on omalla vastuulla	(+) Järjestelmän ylläpito ja valvonta kuuluvat tyypillisesti palveluun
(-) Ohjelmointivirheet voivat aiheuttaa toiminnalle tai tietoturvalle riskejä.	(+) Palveluna hankituilla järjestelmillä on usein pitkä kehityshistoria ja niille voidaan asettaa auditointivaatimuksia.
(-) Järjestelmän kehitys ja ylläpito saattaa henkilöityä	(+) Yleensä laaja kehittäjä- ja ylläpitohenkilökunta

Tässä tapauksessa havaitut riskit ovat mielestäni hallittavissa, erityisesti kun määrittelyyn ja dokumentaatioon kiinnitetään huomiota. Tämän takia pidän myös yhteyttä moniin

sisäisiin ja ulkoisiin sidosryhmiin, että määrittelyssä huomioidaan sekä toiminnalliset että ei-toiminnalliset vaatimukset. Jälkimmäisillä viittaan esimerkiksi GDPR:ään, kuin myös organisaation omiin toimenpiteiden jäljitettävyydelle asettamiin sääntöihin.

Viikon aikana oli myös mielenkiintoinen toinen ongelmanratkaisutehtävä, jossa ITSM-järjestelmään piti saada lisättyä kertakirjautuminen toiselta identiteetintarjoajalta (identity provider), että siihen voidaan kirjautua kahden eri ympäristön tunnuksilla. Tähän oli hankittu ulkoinen konsultti, jolla on kokemusta useamman identiteetintarjoajan kertakirjautumisen määrittämisestä käytössämme olevaan ITSM-järjestelmään. Itselläni taas on hyvä tietämys aiempaan kertakirjautumiseen ja identiteettien tuomiseen liittyvistä määrityksistä. Ominaisuus saatiin käyttöön alle kahdessa tunnissa, ja tuona aikana ilmenneet ongelmat ja niiden ratkaiseminen lisäsivät omaa ymmärrystäni kertakirjautumisen määrittelystä yleisemmin, sillä se tehtiin yleistä SAML-protokollaa käyttäen. ITSM-järjestelmänä on Servicenow, ja identiteetintarjoajana oli Azure AD. Molempien järjestelmien osalta on olemassa kattava yleinen järjestelmädokumentaatio toiminnallisuuden määrittämisestä, Azure AD:ssa Microsoft (2021j) ja Servicenow:ssa Servicenow (2022). Uskonkin, että määritys olisi onnistunut myös itseltäni kyseisten ohjeiden perusteella. Tässä tapauksessa ongelmaksi muodostui kuitenkin se, että testiympäristöön ei ollut määritelty kertakirjautumista päälle, joten muutos piti tehdä huolellisesti suoraan tuotantoympäristöön. Erityisesti tässä konsultin asiantuntemuksesta ja kokemuksesta oli apua, sillä tällä pystyttiin välttämään mahdolliset tuotantojärjestelmän käyttöä haittaavat virhetilanteet.

Muutoksessa tuli kuitenkin huomioida myös näkyvyys käyttäjille ja siihen liittyvä viestittämistarve, minkä takia konfiguraatiota ei tehty aivan loppuun asti, vaan ainoastaan minimitasolle, että sitä voidaan hyödyntää nopeasti. Useampaa identiteetintarjoajaa käytettäessä järjestelmän pitää pystyä jollakin tapaa selvittämään, että mille identiteetintarjoajalle järjestelmän käyttäjä ohjataan. Tämä kuitenkin vaatii sen, että käyttäjä kertoo järjestelmään mennessä jonkin tiedon, jolla ohjaus voidaan tehdä. Yhden identiteetintarjoajan tapauksessa tätä tietoa ei tarvita, vaan ohjaus voidaan aina tehdä samaan paikkaan. Tämän takia myöhemmin tehtäväksi asiaksi jäi käyttäjän kirjautumiskokemuksen muuttaminen niin, että käyttäjältä kysytään esimerkiksi sähköpostiosoite, jonka perusteella järjestelmä osaa tehdä ohjauksen oikein. Kyseinen menetelmä kuitenkin aiheuttaa käyttäjälle näkyvän muutoksen, mistä pitää tiedottaa etukäteen. Tämän takia väliaikaisena ratkaisuna uutta identiteetintarjoajaa käyttävät käyttäjät avaavat järjestelmän erityisellä linkillä, mikä ohjaa heidät oikeaan identiteetintarjoajaan. Pitkäaikaisena ratkaisuna tämä voi kuitenkin aiheuttaa hämmennystä, koska järjestelmän eri käyttäjillä on tässä tapauksessa erilaiset ohjeet sinne kirjautumiseen. Muut työtehtävät ja ongelmanselvitykset olivat viikon aikana hyvin rutiininomaisia.

4 Pohdinta ja päätelmät

Päiväkirjaraportoinnin aikana pääsin käytännön kautta tutustumaan useampaan uuteen teknologiaan. Näitä olivat erityisesti Microsoftin Universal Print -tulostusratkaisu, sekä kertakirjautumisen määrittäminen Azure AD:n ja Servicenow:n välille. Tämän lisäksi tehtäviini kuului useamman erilaisen prosessin automatisoinnin suunnittelu, joista merkittävin oli HR- ja AD-järjestelmien välinen prosessi. Suunnitteluun kuului HR-prosessin ymmärtämisen lisäksi eri sidosryhmien tarpeiden huomioiminen, kuin myös organisaation yleiseen ohjeistukseen tutustuminen. Näistä erityisen merkittävä oli tietosuojaohjeistukseen ja -käytäntöihin tutustuminen. Aiemmin en ole joutunut tekemään organisaatiossani määriteltyä tietosuojan vaikutusten arviointia, mutta tämän automaation yhteydessä sekin tuli tutuksi. Tämä auttanee myös tulevaisuudessa erilaisten järjestelmien ja prosessien tietosuojan ja niiden käyttöönottomahdollisuuksien arvioinnissa.

Tästä huolimatta en välttämättä koe kehittyneeni teknisesti merkittävästi, sillä osaamistasoni oli jo ennen opinnäytetyön aloittamista hyvin korkealla. Kehittyminen on siis lähinnä ollut tiedon lisäämistä, mutta se on joka tapauksessa jatkuva työtehtäviini kohdistuva vaatimus uusien ratkaisujen löytämiseksi. Eräs sivuprojekti, mihin en opinnäytetyön aikana kuitenkaan saanut juurikaan käytettyä aikaa, on ylläpitotyökalujen kehittäminen ja erityisesti yhdistäminen osaksi RDS-hallintaympäristöä. Merkittävänä osana tätä sivuprojektia on ymmärtää erilaisia kollegoiden tarpeita, ja luoda erilaisia automaatioita vähentämään rutiininomaisiin tehtäviin kuluvaa aikaa. Tätä varten pitää kuitenkin sekä haastatella organisaatiossani toimivia henkilöitä automatisoitavien rutiinitehtävien havaitsemiseksi, sekä pyrkiä luomaan sellainen toiminnallisuus, mikä on helposti myös muiden päivitettävissä. Tästä päästään myös yhteen havaitsemistani ongelmista työssäni, eli liian monen samanaikaisen projektin haalimiseen työlistalle.

Sivusin oman ajankäyttöni ongelmia päiväkirjamerkinnöissä, mutta mielestäni niihin on syytä tässä pohdintaosiossa vielä palata. Työni on hyvin itsenäistä ja osana siihen liittyy erilaisten kehitystarpeiden havainnointi. Kehitystarpeita on kuitenkin merkittävästi enemmän kuin aikaa niiden toteuttamiselle, joten niitä pitäisi priorisoida jotenkin. Olenkin mielestäni kehittynyt tämänkaltaisessa priorisoinnissa jonkin verran, mutta monen kehityskohteen prioriteetteja voi olla hankalaa arvioida. Esimerkiksi juuri edellisessä kappaleessa mainitsemieni rutiininomaisten työtehtävien automatisointi on hankala arvioinnin kohde, sillä tiedän että kollegoillani on jo hyvin optimoituja manuaalisia ja osittain automaattisia prosesseja erilaisten tehtävien hoitamiseksi. Tämän seurauksena automatisoinnista ei

välttämättä synny sellaista hyötyä mitä kuvittelen, jolloin se pitäisi priorisoida alemmalle tasolle kuin muut tehtävät.

Toisaalta kyseisenlaisen automaation tekeminen voisi antaa ylimääräisiä ideoita kollegoille työn tehostamisesta, sillä aiemman kokemukseni perusteella suuren osan rutiinitehtävistä voi automatisoida, ja näin säästää työaikaa. Tämä voi myös herättää osalla innokkuutta lähteä kehittämään työkaluja itsenäisesti, mistä on hyötyä koko työyhteisölle. Tästä näkökulmasta automaation toteuttamisen prioriteetti olisi taas melko korkea. Tämänkaltainen prioriteettien ristiriitaisuus aiheuttaa taas itselleni helposti tilanteen, jossa saatan käyttää aikaa johonkin tehtävään, mutta sitten arvioin sen prioriteetin matalammalle, jolloin taas lykkään sen suorittamisen myöhemmälle ajankohdalle. Tässä toimintamallissa ei sinänsä ole ongelmaa, paitsi että olen huomannut tekeväni uudelleenpriorisointia liian usein, jolloin työtehokkuus kärsii liian usein tapahtuvan keskittymiskohteen vaihtelun takia.

Tätä on myös tutkittu psykologian tieteenalalla, ja esimerkiksi APA (2006) kuvaa tästä aiheutuvaa tehokkuuden laskua, joka voi olla jopa 40 prosenttia sekä lisätä virheiden todennäköisyyttä. Tämän lisäksi esimerkiksi Software (s.a.) kuvaa ongelmaa myös ohjelmistokehittäjän näkökulmasta. Olen työssäni törmännyt molempiin ilmiöihin, ja erityisesti Softwaren (s.a.) mainitsemaan ns. "flow":hin, jonka voisi suomentaa syväksi keskittymisen tilaksi, ja kuinka sen katoamisesta on itselleni aiheutunut jopa kymmenien minuuttien viive ennen saman keskittymistilan ja tuottavuuden palautumista.

En vielä opinnäytetyön aikana toteuttanut ajankäyttöön liittyviin ongelmiin suoraa ratkaisua, mutta ajattelin kokeilla tehdä priorisoinnista itselleni muodollisempaa kirjanpitoa, jota voin tarkastella esimerkiksi kerran tai pari viikossa, ja myös hyödyntää esimieheni kanssa asioista keskusteltaessa. ITSM-kehityksessä hyödynnetään juuri ketterää kehitysmallia, jossa kehityssykli on noin kaksi viikkoa. Ajattelin, että voisin hyödyntää tästä saatuja hyviä kokemuksia ehkä myös omassa ajankäytön suunnittelussa ja tehtävien priorisoinnissa. Tämä vaatii kuitenkin osaltani vielä pohdintaa.

Päiväkirjamuotoinen opinnäytetyö ja erityisesti päiväkirjan kirjoittaminen toi myös hyvin esille sen, että tietyissä tehtävissä ajankäytön arvioinnissani on vielä kehittämistä. Näistä keskeisimmät ovat ohjelmointi (skriptaus) sekä dokumentaatio. Pystyn arvioimaan päässäni hyvin selkeästi erilaisten komponenttien tarpeen, sekä sen mitä pitää dokumentoida tai on vielä ohjelmoitavana. Tämä selkeys ei kuitenkaan yllättävän usein auta ajankäytön arvioinnissa, sillä esimerkiksi dokumentoinnissa on usein tarvetta erilaisten kuvien tai muiden visuaalisten apuvälineiden käyttöön, ja en ole niiden osalta graafisesti kovin lahjakas. Ohjelmoinnissa taas lokitus ja virheidenkäsittely ovat havaintojeni mukaan sellaisia osa-

alueita, joiden toteutus on vienyt huomattavasti enemmän aikaa kuin olen kuvitellut. Tämä johtuu osittain siitä, että suuri osa skriptauskokemuksestani on ollut skriptien tekeminen omaan tai pienen ryhmän käyttöön, jolloin lokitus tai virheidenkäsittely eivät ole niin merkittävässä asemassa ja niitä voi kompensoida ohjeistuksella virhetilanteiden välttämiseksi.

Päiväkirjan viikkoanalyysejä käytettäessä tutustuin myös enemmän tieteelliseen kirjallisuuteen kuin on työssäni tavallisesti tarpeellista. Normaalitilanteissa työtehtävät keskittyvät operatiiviseen puoleen, eivätkä niinkään tutkimuksellisen tiedon hankkimiseen tieteellisestä kirjallisuudesta, tai sen tuottamiseen. Tässä opinnäytetyössä tämä näkyi lähinnä master dataan liittyvien prosessien suunnittelussa, johon pyrin hakemaan laajemmin tietoa myös tieteellisen kirjallisuuden puolelta sopivan toimintamallin löytämiseksi. Normaalitilanteessa olisin todennäköisesti tukeutunut enemmän muiden organisaatioiden pintapuolisiin esimerkkitapauksiin, mikä on yleensä riittävä lähestymistapa. Useimmat ongelmat ovat sellaisia, joita on jo kohdattu muualla, ja niihin löytyy joko suoraan ratkaisu tai sellaista lisätietoa, mikä auttaa ratkaisemaan ongelman nopeasti. Jossakin tulevaisuuden työssä painopiste voi kuitenkin siirtyä vielä enemmän reaktiivisesta ongelmienselvityksestä ehkäisevään prosessisuunnitteluun, missä tieteellinen lähestymistapa ja tuoreen tieteellisen kirjallisuuden seuraaminen on todennäköisesti paljon merkityksellisempää. Nykyisessä ympäristössä ja työtehtävissäni työhöni kuuluu kuitenkin edelleen paljon ongelmien ratkaisemista ja ehkäisemistä, missä tieteellisen kirjallisuuden merkityksellisyys jää Internetin ns. kollektiivisen tiedon löytämisen ja soveltamistaitojen taakse hyödyllisyydessä.

Työssä löytyi myös eräs mahdollinen tutkimuskohde, mikä liittyy organisaation käyttäjien ongelmatilanteiden painottumiseen eri ajanjaksoilla. Muutoshallinnan kannalta voisi olla hyödyllistä selvittää esimerkiksi se, että milloin IT-tuessa on suurin kuormitus käyttäjien tukipyyntöjen osalta esimerkiksi viikonpäivien, kuukausien ja kausien tasolla. Tällöin ajallisesti joustavia muutos- ja käyttöönottoprojekteja voisi pyrkiä ajoittamaan sellaisiin kohtiin, joissa on tilastollisesti pienin IT-tuen kuormitus. Omien kokemuksieni perusteella itselleni on tullut esimerkiksi sellainen näkemys, että torstait ovat keskimäärin rauhallisimpia päiviä, kun taas alkuviikosta on yleensä kiireisempää. Tämän lisäksi kesälomien jälkeen on usein huippu unohtuneisiin salasanoihin liittyvien pyyntöjen osalta. Tämänkaltaisesta datasta voisi kuitenkin löytyä tilastollisia trendejä, joita voisi mahdollisesti hyödyntää palvelutuotannon parantamisessa.

Opinnäytetyön aikana aloitin myös huomattavan tietojärjestelmäprojektin suunnittelun. Tämä oli HR- ja AD-järjestelmien välinen integraatio. Aluksi integraation oli tarkoitus olla hyvin yksinkertainen ja kohdistua vanhaan järjestelmään, mutta uuden järjestelmän

tuomat prosessimuutokset mahdollistivat datan hyödyntämisen huomattavasti laajemmin. Tämän seurauksena projekti laajeni käytännössä identiteetinhallintajärjestelmäksi, jossa HR-data toimii työntekijöiden tunnusten master datana, ja tunnustenluontiprosessi pyritään automatisoimaan. Lisäksi uuden järjestelmän käyttöönottaminen toi lisäpaineita pitää järjestelmien väliset tiedot ajan tasalla, mikä aiheuttaisi huomattavia ongelmia ilman kyseisenlaista integraatiota. Tässä havaitsin myös sen, että kaikki tarvittava tieto ei välttämättä liiku edes kokouksissa riittävällä tavalla, sillä tietoa on sen verran paljon ja asiantuntemus voi olla sen verran siiloutunutta, että jokin tärkeä tiedonjyvä jää välittymättä. Kyseisenlaisessa tilanteessa nousee esille IT-generalistin kokonaisuuksien ymmärryksen hyöty, sillä osaamiseen liittyy vahvana osana erilaisten prosessien ja tietojärjestelmien kytkösten ja niiden riippuvuuksien kerääminen eräänlaiseksi tiedonjyvien työkalupakiksi. Tämä auttaa myös havaitsemaan kuvaamani kaltaisia tietokatkoksia ja esittämään niihin liittyviä kysymyksiä etukäteen, jolloin odottamattomia yllätyksiä on helpompi välttää.

Lähteet

APA 2006. Multitasking: Switching costs. Luettavissa: https://www.apa.org/topics/research/multitasking. Luettu: 9.4.2022.

DISA 2021. Microsoft Windows 10 Security Technical Implementation Guide, version 2, release 3.

Google 2022. Chrome platform status, Feature: TLS 1.0 and TLS 1.1 (removed). Luettavissa: https://chromestatus.com/feature/5759116003770368. Luettu: 12.2.2022.

Kuntaliitto 2021. EU-tuomioistuimen Schrems II- tuomio ja EDPB:n ohjeistus tietojensiirrosta julkisella sektorilla. Luettavissa: https://www.kuntaliitto.fi/laki/tietosuoja/schrems-ii-ja-mita-tulisi-tehda. Luettu: 19.2.2022

LeMaire, C. 2016. ShowDialog() Sucks: Use ApplicationContext and Run Instead. Luettavissa https://blog.netnerds.net/2016/01/showdialog-sucks-use-applicationcontexts-instead/. Luettu 6.3.2022.

Microsoft 2019. Understand the Effect of Fast Logon Optimization and Fast Startup on Group Policy. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj573586(v=ws.11). Luettu: 22.1.2022.

Microsoft 2020. Privacy & Personal Data. Luettavissa: https://docs.microsoft.com/en-us/universal-print/fundamentals/user-privacy-personal-data. Luettu: 18.2.2022.

Microsoft 2021a. Enable optimized moves of redirected folders. Luettavissa: https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/enable-optimized-moving. Luettu: 22.1.2022.

Microsoft 2021b. Enterprise access model. Luettavissa: https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model. Luettu: 22.1.2022.

Microsoft 2021c. Managing privileges in a file system. Luettavissa: https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/privileges. Luettu 28.1.2022.

Microsoft 2021d. JEA Role Capabilities. Luettavissa: https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/role-capabilities?view=powershell-7.2. Luettu 26.1.2022.

Microsoft 2021e. Folder Redirection, Offline Files, and Roaming User Profiles overview. Luettavissa: https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview. Luettu 5.2.2022.

Microsoft 2021f. Configure slow-link mode. Luettavissa: https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.OfflineFiles::Pol_SlowLinkSettings. Luettu 13.2.2022.

Microsoft 2021g. User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode. Luettavissa: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-behavior-of-the-elevation-prompt-for-administrators-in-admin-approval-mode. Luettu 13.2.2022.

Microsoft 2021h. Universal Print - frequently asked questions (FAQ). Luettavissa: https://docs.microsoft.com/en-us/universal-print/fundamentals/universal-print-faqs. Luettu 18.2.2022.

Microsoft 2021i. Windows Print Spooler Remote Code Execution Vulnerability, CVE-2021-34527. Luettavissa: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527. Luettu: 19.2.2022.

Microsoft 2021j. Tutorial: Azure Active Directory single sign-on (SSO) integration with ServiceNow. Luettavissa: https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/servicenow-tutorial. Luettu: 13.3.2022.

Microsoft 2022. Tutorial: Enable Azure Active Directory self-service password reset writeback to an on-premises environment. Luettavissa: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr-writeback. Luettu: 27.02.2022.

Microsoft 2022b. Reset redemption status for a guest user (Preview). Luettavissa: https://docs.microsoft.com/en-us/azure/active-directory/external-identities/reset-redemption-status. Luettu: 5.3.2022.

NCSC 2018. Preventing Lateral Movement: Guidance for preventing lateral movement in enterprise networks. Luettavissa: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement. Luettu: 5.3.2022.

NIST 2017. NIST Special Publication 800-63B: Digital Identity Guidelines, Authentication and Lifecycle Management. Luettavissa: https://doi.org/10.6028/NIST.SP.800-63b. Luettu: 22.1.2022.

Otto, B. 2012. How to design the master data architecture: Findings from a case study at Bosch. International Journal of Information Management, 32(4), 337–346. doi:10.1016/j.ijinfomgt.2011.11.018

Servicenow 2022. Set up Multi-Provider SSO (San Diego). Luettavissa: https://docs.servicenow.com/bundle/sandiego-platform-administration/page/integrate/single-sign-on/task/t_SettingUpMultiProviderSSO.html. Luettu: 13.3.2022.

Software s.a. Context Switching is Killing Your Productivity. Luettavissa: https://www.software.com/devops-guides/context-switching. Luettu: 9.4.2022.

Spruit, M., & Pietzka, K. (2015). MD3M: The master data management maturity model. Computers in Human Behavior, 51, 1068–1076. doi:10.1016/j.chb.2014.09.030

Liitteet

Liite 1. Opinnäytetyössä käytettyä ammattitermistöä

ACL	Access Control List. Pääsynhallinnassa käytettävä lista käyttöoikeuksista
AD	Active Directory. Microsoftin teknologia käyttäjähakemiston hallintaan.
ADFS	Active Directory Federation Services. Windowsin palvelinkäyttöjärjestelmissä oleva kertakirjautumispalvelu.
API	Application Programming Interface. Ohjelmoinnissa käytettävä sovelluksen rajapinta.
Applocker	Microsoftin Windows-käyttöjärjestelmän tietoturvateknologia, jolla voidaan estää tai sallia sovellusten käynnistäminen niiden digitaalisen allekirjoituksen, tiivisteen tai sijainnin perusteella.
CSE	Client Side Extension. Ryhmäkäytäntöjen komponentti, jolla ryhmäkäytäntöasetuksia suoritetaan Windows-työasemilla.
DMZ-alue	Erillinen verkkoalue organisaation sisäisen verkon ja Internetin välillä, johon on pääsy molemmilta verkkoalueilta. DMZ tulee sanoista Demilitarized Zone.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa verkko-osoitteet IP-osoitteiksi.
Exchange	Microsoftin sähköpostipalvelinohjelmisto.
GDPR	General Data Protection Regulation. EU:n yleinen tietosuoja-asetus.
Group policy	Windowsin ryhmäkäytäntötoiminnallisuus, jolla on mahdollista määrittää asetuksia toimialueen jäseninä oleville tietokoneille.
HR	Human Resources eli henkilöstöhallinto.
IAM	Identity and Access Management. Järjestelmä, joka hallitsee identiteettejä (käyttäjätunnuksia) ja niihin liittyviä käyttöoikeuksia.
Intune	Microsoftin laitteisiin kohdistuvan etähallinnan pilvipalvelu, jolla voidaan tehdä palveluun liitetyille laitteille etähallintaa ja ylläpitoa.

ITIL	Information Technology Infrastructure Library. ITIL on viitekehys IT-palveluhallintaan ja -johtamiseen.
ITSM	Information Technology Service Management. IT-palvelunhallinta.
JEA	Just Enough Administration. Microsoftin tietoturvateknologia ja toimintamalli, jossa ylläpito-oikeuksia delegoidaaan vain juuri sen verran kuin on tarvetta.
JIT	Just In Time access. Microsoftin tietoturvateknologia, jossa tarvittavat käyttöoikeudet aktivoidaan vain juuri ennen niiden tarvetta, jolloin esimerkiksi ylläpito-oikeudet eivät ole jatkuvasti aktiivisena.
Kerberos	Todennusprotokolla, joka perustuu julkisen avaimen salausmenetelmään, ja on Windows-toimialueiden käyttämä oletustodennusprotokolla.
L2/L3	Viittaa OSI-viitemallin tasoihin 2 (siirtokerros/data link layer) ja 3 (verkkokerros/network layer)
M365	Microsoft 365. Microsoftin lyhenne tiettyjä perussovelluksia sisältävälle ohjelmistopaketille. Sisältää esimerkiksi Microsoft Teams ja Office-tuoteperheen ohjelmistoja.
MECM	Microsoft Endpoint Configuration Manager. Microsoftin ohjelmisto, joka mahdollistaa tietokoneiden etähallinnan ja ylläpidon.
MFA	Multi-Factor Authentication. Monivaiheinen tunnistautuminen.
NLA	Network Level Authentication. RDP-protokollaan liittyvä verkkotason todennus, jolla voidaan varmistaa kohdepalvelimen identiteetti, ja jolla palvelin voi varmistua asiakkaan identiteetistä ennen etätyöpöytäresurssien varaamista.
NTLM	NT Lan Manager. Todennusprotokollakokoelma, joista uusin on NTLMv2. Protokolla on Windows-toimialueilla tyypillisesti käytössä toissijaisena todennusprotokollana Kerberoksen jälkeen.
PKI	Public Key Infrastructure. Julkisen avaimen salausmenetelmän toteuttamiseen liittyvä infrastruktuuri.
RDP	Remote Desktop Protocol. Tiedonsiirtoprotokolla Windowsin etätyöpöydän käyttämiseen.
RDS	Remote Desktop Services. Yleistermi Windowsin etätyöpöytään liittyviin palvelinkomponentteihin.

SAML	Security Assertion Markup Language. Esimerkiksi kertakirjautumisessa käytettävä protokolla käyttäjän tietojen ja käyttöoikeuksien välittämiseen vastaanottavalle palvelulle.
Servicenow	Organisaatiossani käytössä oleva IT-palvelunhallintajärjestelmä.
SMB	Server Message Block. Verkkoprotokolla tiedostojen ja palveluiden jakamiseksi. Käytetään Windowsissa esimerkiksi tiedostojen ja tulostinten jakamiseen.
SSO	Single Sign-on. Kertakirjautuminen.
STIG	Security Technical Implementation Guide. Ohjeistus tiettyjen tietoturvastandardien mukaisten asetusten käyttöönottoon.
TLS	Transport Layer Security. Salausprotokolla, jota käytetään esimerkiksi HTTPS-liikenteen salaamiseen.
UAC	User Account Control. Windows-käyttöjärjestelmän tietoturvaominaisuus, joka vahvistaa erikseen ylläpito-oikeuksien aktivoinnin sen sijaan, että ne ovat koko ajan aktiivisena.
VPN	Virtual Private Network. Virtuaalinen erillisverkko, jota voidaan käyttää esimerkiksi organisaation sisäiseen verkkoon yhdistämiseksi sen ulkopuolelta.
WMI	Windows Management Instrumentation. Windows-hallintaan liittyvä rajapinta.
WPF	Windows Presentation Foundation. Viitekehys ja rajapinta Windowsin graafisten käyttöliittymien tekemistä varten.