KÄYTTÄJÄHALLINNAN TEHOSTAMINEN ULKOISTETUSSA IT-YMPÄRISTÖSSÄ

Case: Identiteetinhallintajärjestelmän käyttöönotto ja salasanan itsepalvelu

LAB-AMMATTIKORKEAKOULU
Insinööri (ylempi AMK)
Digitaaliset teknologiat
Kevät 2020
Mika Romppanen

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Romppanen, Mika	Opinnäytetyö, YAMK	Kevät 2020
	Sivumäärä 62 sivua	

Työn nimi

Käyttäjähallinnan tehostaminen ulkoistetussa IT-ympäristössä
Identiteetinhallintajärjestelmän käyttöönotto ja salasanan itsepalvelu

Tutkinto

Insinööri (ylempi AMK), digitaaliset teknologiat

Organisaatioiden käyttäjillä on käytössään useita eri käyttäjätunnus-salasana -pareja useisiin eri järjestelmiin. Useiden tunnusten ja salasanojen ylläpito on yhä hankalampaa ja työläämpää niin käyttäjälle kuin palveluntuottajille. Identiteetinhallinta sekä salasanan itsepalvelu pyrkivät saamaan sähköisten identiteettien ylläpidon kontrolliin ja tuomaan helpotusta tilanteeseen IT-palvelutoimittajalle sekä loppukäyttäjille.

Opinnäytetyössä tutkittiin identiteetinhallinnan ja salasanan itsepalvelun toiminnallisuuden käyttöönoton hyötyjä ulkoistetussa IT-ympäristössä, sekä käynnistettiin kahdelle asiakkaalle identiteetinhallintajärjestelmän sekä salasanan itsepalvelun suunnittelu- ja käyttöönottoprojektit. Tavoitteena on vähentää IT-palvelutoimittajan käyttötuen työmäärää.

Opinnäytetyössä käytettiin hyödyksi tutkimuspäiväkirjamenetelmää sekä analysoitiin palveluntoimittajan työnohjausjärjestelmän dataa. Työn alkuosa koostuu tutkimuspäiväkirjasta sekä IT-palvelutoimittajan toiminnanohjausjärjestelmän datan pohjalta tehtyyn analyysiin. Työssä on hyödynnetty myös palvelutoimittajan kokemusperäistä tietoa.

IT-palvelutoimittajan työnohjausjärjestelmän raporttien pohjalta tehdyssä analyysissä löydettiin mahdollisuuksia huomattaviin käyttötuen työmäärän säästöihin käyttäjien salasanan vaihtojen sekä manuaalisesti tehtävien käyttäjätunnusten osalta. Lisäksi tunnistettiin tietoturvaa edistäviä hyötyjä identiteetinhallinnan sekä salasanan itsepalvelun osalta. Ottamalla identiteetinhallintajärjestelmä ja salasanan itsepalvelu käyttöön, myös loppukäyttäjille voidaan tuoda säästöä työaikaan käyttöoikeuslomakkeiden ja käyttötukeen puhelimessa jonottamisen vähenemisen muodossa.

Asiasanat

identiteetinhallinta, salasanan itsepalvelu, käyttäjähallinta

Abstract

Author(s)	Type of publication	Published
Romppanen, Mika	Master's Thesis	Spring 2020
	Number of pages 62 pages	

Title of publication

Enhancing user management in an outsourced IT environment
Case: Implementing identity management system and password self-service

Name of Degree

Master of Engineering, Digital Technologies

Users in organizations have access to several different username-password pairs for several different systems. Maintaining multiple IDs and passwords is becoming increasingly difficult for both the users and the service providers. Identity management and password self-service aim to control the maintenance of electronic identities and bring relief to the IT service provider and end users.

The thesis investigated the benefits of implementing an identity management system and password self-service functionality in an outsourced IT environment. Identity management and password self-service design and implementation projects were launched for two customers. The goal was to reduce the workload of the IT service provider.

The beginning of the thesis was based on development diaries and an analysis of the data of the service provider's work management system. The service provider's empirical knowledge has also been utilized in the thesis.

The analysis based on reports from the IT service provider's work management system found opportunities for significant workload savings on user password changes as well as manual user accounts. In addition, security benefits in terms of identity management and password self-service were identified. By implementing an identity management system and password self-service, end-users can also be saved on working time in the form of reduced access queues and user support on the phone.

Keywords

Identity management, password self-service, user management

SISÄLLYS

1 JOHDANTO

Tämä LAB-ammattikorkeakoulun ylemmän ammattikorkeakoulun opinnäytetyön aihe käsittelee käyttäjähallinnan näkökulmasta identiteetinhallinnan hyötyjä sekä seuraa kahden identiteetinhallintaympäristön suunnittelua. Identiteetinhallinnan yhteydessä asiakkaalle jalkautetaan mahdollisuus vaihtaa itsepalvelun kautta organisaation toimialueen käyttäjätunnuksen salasana. Tavoitteena opinnäytetyössä on tunnistaa identiteetinhallinnan ja salasanan itsepalvelun hyödyt kahdessa organisaatiossa sekä saattaa identiteetinhallinnan projekti toteutuskelpoiseksi.

Työ rajataan koskemaan identiteetinhallinnan osalta järjestelmän suunnittelua ja hyötyanalyysiä perustuen palveluntarjoajan työnohjausjärjestelmän dataan. Salasanan vaihdon itsepalveluautomaation osalta työssä suoritetaan suunnittelu, työnohjausjärjestelmän dataan perustuva analyysi sekä käyttöönotto. Työn ulkopuolelle rajataan käyttöönoton jälkeinen säästyneen työajan toteutuman analysointi ja seuranta.

Organisaatioiden käyttäjillä on käytössään useita eri käyttäjätunnus-salasana -pareja useisiin eri järjestelmiin. Osa järjestelmistä tulee perinteisesti tuotettuna organisaation omilta palvelimilta ja osa pilvipalveluna. Useiden tunnusten ja salasanojen ylläpito on yhä hankalampaa niin käyttäjälle kuin organisaatiolle. Identiteetinhallinnasta käytetään myös lyhennettä IDM, joka tulee termin englanninkielisestä sanasta identity management. Identiteetinhallinta, sekä salasanan itsepalvelu pyrkivät saamaan ylläpidon kontrolliin ja tuomaan helpotusta tilanteeseen loppukäyttäjille.

Opinnäytetyö on tutkimuspäiväkirja tyyppinen. Työ pitää sisällään neljä kappaletta kolmen viikon seurantajaksoja ja jokaista jaksoa seuraa arviointi. Jokaiselle jaksolle asetetaan tavoite ja sen etenemistä seurataan seurantaviikkojen yhteenvedoissa sekä jaksoarvioinneissa. Tutkimuspäiväkirjaa pitämällä on tarkoitus oppia omista työtavoista ja kehittää itseään kohti tehokkaampaa ja järjestelmällisempää työskentelytapaa. Työssä on myös analysoitu palveluntarjoajan työnjohtojärjestelmän dataa, etsien mahdollisuuksia työmäärän säästöön.

Opinnäytetyössä haetaan vastauksia seuraaviin tutkimuskysymyksiin:

- Mitkä ovat identiteetinhallinnan hyödyt IT-palvelutoimittajan liiketoiminnalle?
- Mitkä ovat salasanan itsepalvelun hyödyt IT-palvelutoimittajan liiketoiminnalle?

Tutkimuspäiväkirjaa käsitellään luvussa kolme. Luvussa neljä on analysoitu palveluntarjoajan työnohjausjärjestelmän raportteja sekä tuotu esille ennen projektia ja projektin aikana

tunnistettuja hyötyjä identiteetinhallinnasta ja salasanan vaihdon itsepalvelusta. Luvut viisi ja kuusi tarjoavat teoriapohjan opinnäytetyössä käsiteltyihin aiheisiin.

Työn teoriaosuudessa esitellään identiteetinhallinnan perusteita sekä käsitellään käyttäjän tunnistautumista ja siihen liittyviä tietoturva näkökulmia esitellen lukijalle mitä identiteetinhallinta on ja miksi salasanan vaihdon itsepalvelukäytäntö tuo työajan säästön lisäksi parannusta tietoturvaan

2 TOIMINTAYMPÄRISTÖ

2.1 IT-palvelutoimittaja

Työssä mainittu IT-palveluntoimittaja on kansainvälisen IT-palveluntoimittajan suomalainen tytäryhtiö, joka työllistää yli 132 tuhatta työntekijää yli sadassa maassa. Suomessa työntekijöitä on yli 2000 ja liikevaihto viimeisen viiden vuoden aikana on pysynyt reilussa 400 miljoonassa eurossa. Asiakkaat koostuvat pienistä kunnista aina suuriin koko maan kattaviin konserneihin, joille tarjotaan monipuolisia IT- ja huoltopalveluita.

2.2 Asiakasympäristöt

Opinnäytetyön aikana toimitaan kahdessa eri asiakasympäristössä, jotka ovat luonteeltaan ja vaatimuksiltaan erilaisia. Asiakkaista käytetään nimityksiä asiakas a ja asiakas b.

2.3 Projektin vastuut

Työn kirjoittajan työnkuva on toimia palveluntuottajan tuotantopäällikkönä. Tuotantopäällikkö vastaa ja raportoi asiakkaalle tuotettavasta jatkuvasta palvelusta. Lisäksi tuotantopäällikkö osallistuu palvelun kehittämiseen ja edustaa jatkuvaa palvelua kehityshankkeissa.

Raportoinnin ja toiminnan pohjalla ovat asiakkaan kanssa laaditut sopimukset, joissa on määritelty palvelun vaatimustasot. Palvelun mittarit määritellään asiakkaan ja palveluntuottajan välisissä sopimuksissa. Palvelusta voidaan mitata esimerkiksi palvelupyyntöjen vasteaikaa, käyttötuen puheluiden läpimenoa tai palvelinten ja tietoliikennelaitteiden käytettävyyttä.

Asiakkuudessa toimivat tuotanto- ja palvelupäälliköt muodostavat yhdessä asiakkuuden palvelunhallinnan. Palvelunhallinta esittelee yhdessä asiakkaan kanssa sovituin määräajoin raportit palvelusopimuksen mukaisista käytettävyyksistä, poikkeamista palvelussa sekä palvelunlaadussa.

Ennen tuotantopäällikön tehtävänkuvaa työn kirjoittaja on toiminut osana projektiryhmää, jossa otettiin identiteetinhallintajärjestelmä käyttöön. Ennen projektin käynnistystä käyttäjätunnukset luotiin käsin ja lähetettiin esimiehelle sisäisessä postissa suljetussa kirjekuoressa. Projektissa käytiin läpi henkilön palkkaamisen työnkulku ja viilattiin prosessia

identiteetinhallinnan kannalta sujuvammaksi. Projektissa määriteltiin identiteetin yksilöivät avaintiedot, selvitettiin rajapinnat lähde- ja kohdejärjestelmiin sekä suoritettiin järjestelmän toteutus ja käyttöönotto. Projektin suunnittelu- ja toteutustyön suoritti pohjoismainen ohjelmistotalo. Sekä asiakkaalla että ohjelmistotalolla oli omat projektipäälliköt. Lisäksi asiakkaalla oli projektiin kiinnitettyjä organisaation asiantuntijoita käytettävissään. Prosessit suunniteltiin asiakkaan toimesta yhteistyössä ohjelmistotalon asiantuntijoiden kanssa. Käyttöönoton jälkeen työn kirjottaja on toiminut yli kahdeksan vuotta järjestelmän pääkäyttäjänä.

Molemmat asiakkaista ovat nimenneet projektiin tietohallinnostaan edustajat projektiryhmään. Heidän tehtävänään on tuoda projektiin asiakkaan näkökulmaa ja asiantuntemusta organisaatiosta. Asiakas a:n projektissa on käytettävissä myös toiminnanohjausjärjestelmän pääkäyttäjä koska järjestelmä tulee toimimaan identiteetinhallinnan lähdejärjestelmänä. Asiakas b:llä ei muita asiakkaan henkilöitä ole mukana, koska uusi toteutus pohjautuu olemassa olevaan järjestelmään. Molemmat asiakkaista ovat nimenneet keskuudestaan ryhmän pilottikäyttäjiä, joita hyödynnetään salasanan vaihdon itsepalvelun testaus vaiheessa ennen laajamittaista käyttöönottoa.

IT-palvelutoimittajan osalta projektiin on resursoitu projektipäällikkö, työn kirjoittaja sekä kolme arkkitehtia. Yksi arkkitehdeistä toimii salasanan itsepalvelun suunnittelijana ja asiantuntijana. Kaksi muuta ovat identiteetinhallinnan arkkitehtejä, joista toinen hoitaa asiakas a:n identiteetinhallinnan järjestelmän suunnittelun ja toinen asiakas b:n identiteetinhallinnan järjestelmän suunnittelun pohjautuen vanhaan järjestelmään.

3 PÄIVÄKIRJA

Opinnäytetyön tutkimuspäiväkirjaa varten pidettiin neljä kappaletta kolmen viikon seurantajaksoja. Jokaisen seurantajakson jälkeen laadittiin jaksoarviointi. Seurantajaksot joudutiin viemään läpi todella tiiviillä aikataululla opinnäytetyön aikataulun takia. Seurantajaksot muodostuivat seuraavasti:

- ensimmäinen seurantajakso viikot 1-3, kokonaisarviointi ja jaksoanalyysi viikko 4
- toinen seurantajakso viikot 5-7, kokonaisarviointi ja jaksoanalyysi viikko 8
- kolmas seurantajakso viikot 9-11 kokonaisarviointi ja jaksoanalyysi viikko 12
- neljäs seurantajakso viikot 13-15, kokonaisarviointi ja jaksoanalyysi viikko 16.

3.1 Ensimmäinen seurantajakso

Ensimmäinen seurantajakso kattaa 31.12.2019 – 19.1.2020 välisen ajan. Keskelle ensimmäisen seurantajakson ensimmäistä viikkoa osuu vuodenvaihde toisen viikon alkaessa loppiaisella. Perinteisesti osa ihmisistä on lomalla joulusta loppiaiseen, joten ensimmäinen puolikas seurantajaksosta on loppukäyttäjien näkökulmasta varmasti hiljaisempaa.

Ensimmäisen seurantajakson alkaessa päiväkirjassa seurattava projekti on ollut käynnissä joitakin viikkoja. Asiakas a:lle on identiteetinhallintajärjestelmän suunnittelua aloitettu ja pidetty ensimmäiset työpajat. Asiakas b:lle identiteetinhallintajärjestelmän suunnittelu mallinnetaan käytössä olevan järjestelmän pohjalta, joten suunnittelu osuus on edennyt vauhdilla projektin käynnistettyä. Salasanan itsepalvelusta on pidetty työpajat molempien asiakkaiden kanssa ennen ensimmäistä seurantajaksoa. Itsepalvelun käyttöönotto ei vaadi suurta suunnittelua vaan kyseessä on suoraviivainen käyttöönotto.

Ensimmäisen seurantajakson tavoitteena on saada päätettyä salasanan vaihdon itsepalvelun osalta toteutusmalli sekä käyttöönoton aikataulu, mikäli salasanan vaihdon itsepalvelun pilotoinnit sujuvat hyvin.

Salasanan vaihdon itsepalvelu käyttää hyväkseen asiakkaan Active Directory toimialueen käyttäjätunnukselle tallennettua matkapuhelinnumeroa. Matkapuhelinnumeroiden muotoilusta toimialueelle pitää saada päätös. Matkapuhelinnumeroita hyödynnetään useissa järjestelmissä salasanan itsepalvelun lisäksi, ja ongelmaksi muodostuu niiden eroavaisuudet muotoilun osalta. Salasanan itsepalvelu vaatii numeron kansainvälisessä formaatissa

yhtenä merkkijonona, kun taas Office 365 conditional access vaatii puhelinnumeroon välilyönnin maakoodin jälkeen. Office 365 conditional access on tietoturvaa lisäävä toiminnallisuus Microsoft Office 365 -pilvipalvelussa. Toiminnallisuudella voidaan määritellä luotettuja päätelaitteita ja verkkoalueita. Näiden pohjalta luodaan säännöstö, jolla rajoitetaan palveluun pääsyä luotettaviksi määritellyistä verkkosijainneista ja päätelaitteista.

Salasanan vaihdon itsepalvelun osalta tavoitteena on myös saada selkeä näkemys käyttötuen tekemistä salasanan vaihtojen määristä. Jokainen puhelu kirjataan työnohjausjärjestelmään, mutta vaatii lisää perehtymistä, että järjestelmästä saadaan ajettua raportit ja jalostettua niistä yhteenveto.

Ensimmäisen seurantajakson aikana identiteetinhallintajärjestelmän osalta tavoitteena on saada asiakas b:lle loppukäyttäjätestaukset sovittua ja pohdittua käyttöönottoa. Asiakas a:n osalta tavoitteena on saada selvä näkemys manuaalisesti luotavien AD-käyttäjätunnusten ja niihin liittyvien käyttöoikeuksien määristä sekä arvio työllistävästä vaikutuksesta.

3.1.1 Viikkoarviointi, viikko 1

Ensimmäiselle seurantaviikolle osuu uudenvuodenaatto, joten oletettavasti asiakkaiden loppukäyttäjiä sekä tuotannon asiantuntijoita on vielä lomalla. Tämä näkynee rauhallisuutena, ainakin kalenteri on tyhjä.

Salasanan itsepalvelutyökalun osalta molemmat asiakkaat ovat määrittäneet keskuudestaan pilottikäyttäjät. Pilottikäyttäjille asennettiin salasanan vaihtotyökalu sekä toimitettiin linkki työkalun web-versioon käyttöohjeineen. Pilotoijien tehtävänä oli simuloida käyttäjän tarvetta vaihtaa salasananansa ilman, että joutuu soittamaan käyttötukeen.

Asiakkaiden pilottikäyttäjien antamien raporttien pohjalta salasanan itsevaihtotyökalun sovellus sekä web-versio todettiin projektiryhmässä toimiviksi. Salasanan itsevaihto työkalu nojaa käyttäjän AD:n, eli Active Directoryn, toimialueen käyttäjätunnuksen attribuutissa olevaan matkapuhelinnumeroon. Loppukäyttäjille päätettiin tuotantoon mennessä viedä sovellusversio. Web-versiota automatiikasta tulee käyttämään lähinnä asiakkaan hallituksen henkilöt. He ovat käyttäjiä, joilla ei ole käytössä asiakkaan standardilaitteita, mutta käyttävät asiakkaan sähköpostia mobiililaitteilla sekä Office 365 -portaalin kautta.

Ennen kuin käyttäjä voi vaihtaa salasanan itsepalvelun kautta, täytyy käyttäjän matkapuhelinnumero olla viety AD:n attribuuttiin. Tällä toimenpiteellä voidaan varmistaa, että salasanan saa vaihdettua vain ennalta määritellystä puhelinnumerosta. Puhelinnumeroiden täytyy olla käyttäjien henkilökohtaisia työnumeroita. Toisella asiakkaalla puhelinnumerot

ovat AD:lla pääosin kunnossa ja kansainvälisessä formaatissa. Heidän osaltansa voidaan lähteä tuotantoon tammikuun aikana.

Toisen asiakkaan osalta AD:n puhelinnumerotiedot koostuvat nelinumeroisista lyhytnumeroista, joihin ei voida soittaa tai lähettää tekstiviestiä asiakkaan puhelinvaihteen ulkopuolelta. Näitä numeroita ollaan korjaamassa projektin ulkopuolisena muutoksena, jossa asiakkaan operaattorin mobiilivaihde integroidaan AD:n kanssa. Integraatio täydentää liittymille käyttäjän laskutus- ja henkilötiedot. AD:lle tuodaan taas vastavuoroisesti käyttäjän puhelinnumero kansainvälisessä muodossa. Avaintietona operaattorin ja AD:n tiedoissa toimii käyttäjän palkanlaskennan henkilönumero. Tämä integraatio oli tarkoituksena ottaa käyttöön jo joulukuussa, mutta operaattori ilmoitti heillä alkaneesta taustajärjestelmien jäädytysajasta, joka kestää tammikuun alkupuolelle asti. Ennen kuin operaattorin jäädytysaika loppuu, ei integraatiota saada tuotantoon. Salasanan vaihdon itsepalvelua ei tälle asiakkaalle taas voi ottaa käyttöön, ennen kun matkapuhelinnumerot ovat AD:lla kansainvälisessä muodossa.

Matkapuhelinnumeroiden osalta tuli ilmi ristiriita muotoilujen osalta. Salasana automaatio ei salli välilyöntiä, jota tarvitaan taas Office 365 -tietoturvaominaisuuksien kanssa. Tähän ei ole saatu vielä valmista päätöstä, vaan asian käsittely jatkuu tulevina viikkoina.

Toiselle asiakkaista ei ensimmäisessä vaiheessa tule IDM-järjestelmään ollenkaan lomakkeita, vaan pelkkä integraatio toiminnanohjausjärjestelmään, joka toimii heidän identiteetin lähdejärjestelmänään. Muut kuin toiminnanohjausjärjestelmän syötteestä tulevat käyttäjät luodaan toistaiseksi vielä käsin asiakasportaalissa olevien lomakkeiden pohjalta. IDM-järjestelmän tuotantoon viennin jälkeen tulee tarkastella jatkokehitystarpeita, joihin edellä mainitut käsin luotavat tunnukset kuuluvat. Lopullisena tavoitteena on rutiiniasioiden mahdollisimman suuri automaatioaste. Mikäli näiden lomakkeella anottavien tunnusten määrät jäävät pieniksi, täytyy automatisoinnin hyödyt miettiä, kun työmääräarvio automaatiosta saadaan.

Kyseiselle asiakkaalle identiteetinhallintajärjestelmän lähdedata tulee toiminnanohjausjärjestelmästä. Selvityksen alla on vielä, mitä kenttiä järjestelmästä tuotaisiin ja tuodaanko ne csv-siirtotiedostona vai reaaliaikaisena web-service rajapintana. Csv-tiedostoa puoltaisi jo olemassa oleva siirtotiedosto, johon joudutaan kyllä tekemään muutoksia joka tapauksessa. Siirtotiedoston huono puoli on taas sen valvomisen hankaluus. Web-service olisi modernimpi siirtomenetelmä, web-serviceä pystyisi valvomaan csv-tiedostoa paremmin ja muutokset tulisivat identiteetinhallintajärjestelmälle välittömästi. Siirtotiedostojen tapauksessa tulee tyypillisesti viiveitä, sillä tiedostoa siirretään ajastetusti seuraaviin kohteisiin.

Toisen asiakkaan osalta lähdejärjestelmänä toimii asiakkaan palkanlaskentajärjestelmä ja siirtomenetelmänä csv-muotoinen siirtotiedosto. Ratkaisu oli ilmeinen, koska siirtotiedosto oli jo olemassa ja käytössä nykyisen korvattavan IDM-järjestelmän kanssa. Heille tulee IDM-järjestelmään lomakkeita, joilla voidaan anoa käyttäjätunnuksia opiskelijoille ja vuorotyöntekijöille. Heidän osaltansa yhden ongelman muodostaa yhteistyökumppaneiden tunnukset, jotka luodaan Active Directory toimialueella ulkopuolisille käyttäjille varattuun organisaatioyksikköön. Aiemmassa järjestelmässä nämä ovat automatisoitu lomakkeella, mutta uuden järjestelmän käyttöönotossa nämä jätettiin jatkokehitysvaiheeseen. Kirjasin lomakkeelle tarvittavat asiat ja työnkulun, ja pyysin niiden pohjalta työmääräarviota. Lisäksi pyysin pohtimaan, olisiko toteutusta mahdollista aloittaa jo ennen uuden IDM-järjestelmän tuotantoon viemistä.

Ennen vuodenvaihdetta saimme tiedon, etteivät kaikki asiakas b:n esimiesasemassa olevat olleet hoitaneet määräaikaisella työsopimuksella työskenteleville alaisilleen uutta työsopimusta ajoissa. Esimiehet olivat aikatauluttaneet sopimuksen laatimisen uudenvuoden jälkeen tehtäväksi. Asia on erittäin ongelmallinen, koska mikäli määräaikainen työsopimus päättyy vuodenvaihteeseen, eikä sille ole luotu jatkoa, katsoo IDM-järjestelmä käyttäjän poistuneeksi ja lukitsee tunnukset. Kun saimme tiedon asiasta, pidimme asiakkaan yhteyshenkilöiden kanssa kriisipalaverin, jossa laadimme käyttötuelle ohjeistuksen millä ehdoilla ilmoittajien tunnukset saa avata. Asiakas laati asiasta tiedotteen intranettiin, mutta viestintä ei ehtinyt asettaa tiedotetta ajoissa näkyviin.

Vuodenvaihteen jälkeen ensimmäinen arkipäivä oli torstai 2.1.2020. Käyttötuki sai heti aamusta asiakas b:n henkilöstöltä paljon puheluita, eikä tilanne rauhoittunut ennen aamupäivää. Puheluruuhkan aiheutti vuodenvaihteessa lukittautuneet käyttäjätunnukset. Tarkemmassa selvityksessä löytyi kolme juurisyytä puhelutulvaan:

- Esimiehet eivät jatkaneet määräaikaisia työsopimuksia ajoissa, joten IDM-järjestelmä tulkitsi työsuhteet päättyneiksi.
- Esimiehet olivat laatineet ajoissa uuden työsopimuksen, mutta työsopimukselta puuttui esimies kiinnitys. Esimiestieto on määritelty IDM-järjestelmässä pakolliseksi tiedoksi, joten nämä työsopimukset jouduttiin hylkäämään.
- Esimiehet eivät olleet jatkaneet lomakkeella anottavia käyttäjätunnuksia.

Kaikki ylläolevat kolme kohtaa, olisi voitu välttää paremmalla tiedottamisella ennen vuodenvaihdetta. IDM-järjestelmä lähettää tunnukselle merkitylle esimiehelle viikkoa ennen voimassaolon päättymistä sähköpostiviestin, jossa muistutetaan tunnuksen vanhenemisesta. Ilmeisesti kaikille esimiehille ei nämä viestit mene perille. Puuttuvat

esimieskiinnitykset voivat johtua esimiesten huolimattomuudesta, osaamattomuudesta palkanlaskentajärjestelmän kanssa tai teknisessä virheestä palkanlaskentajärjestelmässä. Lähetimme palkanlaskentaan listan melkein 300 työsopimuksesta, joista esimiestieto puuttui. Otimme asian esille IDM-projektiryhmässä ja ehdotimme, ettei uudessa järjestelmässä esimiestiedon puuttuminen estä tunnusten luontia tai voimassaolon jatkamista.

Molemmilta asiakkailta puuttuu toimiva käyttäjätunnusten poistoprosessi. Poistoprosessin puuttuminen aiheuttaa Office 365 -lisenssien yliallokointia, josta aiheutuu taas lisenssien siivoustarpeita. Toisella asiakkaista esimiesten kuuluisi tilata tunnuksille poistot lomakkeella, mutta käytäntö osoittaa, etteivät esimiehet hoida tätä asiaa. Asiakas b:llä olemassa oleva IDM-järjestelmä lukitsee tunnukset työsuhteen päätyttyä, mutta varsinainen poistologiikka puuttuu. Otin asian esille projektiryhmässä jo aiemmin, ja uuden IDM-järjestelmän myötä poistot on tarkoitus automatisoida ja huomioida tarvittavien lisenssien vapautukset osana käyttäjän poistoa.

IDM ja salasanan itsepalvelun lisäksi viikkoon kuului paljon pienempiä yksittäisiä tehtäviä. Olen laatinut asiakkaalle ehdotuksen jatkossa noudatettavasta prosessista, kun palveluntarjoajan lähituki ja asiantuntijat tarvitsevat kulkuoikeuksia asiakkaan tiloihin. Lisäksi viikkoon kuului asiakkaille tuotettaviin palvelimiin liittyen huoltokatkoaikojen läpikäyntiä, poistuvien palvelinten saattamista poistoprosessiin ja pois laskutuksesta sekä palvelutasosopimus-laskentaan liittyvien asioiden läpikäyntiä. Valitettavasti vuodenvaihteen tunnusten lukittautumiset aiheuttivat vuoden ensimmäiselle arkiaamulle sellaisen puhelutulvan, ettei käyttötuen tavoitettavuuksissa välttämättä päästä enää tammikuun tavoitteisiin.

Ensimmäisen viikon aikana projektiryhmä sai käytyä asiakas b:n kanssa läpi uuteen IDM-järjestelmään luotavien sähköpostipohjien muotoilut. Asiakas hyväksyi muotoilut.

Tapasin joulukuussa opinnäytetyön ohjaajani ja hän järjesti tapaamisen Neea Similän kanssa. Neea on kirjoittanut syksyllä 2018 YAMK tasoisen opinnäytetyön, jossa hyödynnettiin tutkimuspäiväkirjamenetelmää. Neea suositteli kirjaamaan asiat muistiin sitä mukaa, kun ne tulevat eteen. Hän mainitsee tämän myös opinnäytetyössään. Otin tämän vinkin vakavissani ja pidin Word-tiedostoa koko ajan auki, johon tein jokaiselta päivältä pääotsikon ja kirjasin ranskalaisin viivoin ongelmia, sekä, kehityskohteita palavereita ja asiakokonaisuuksia. Ensimmäisenä päivänä huomasin unohtaneeni kirjaamisen, joten jouduin kirjaamaan päivän tapahtumat työpäivän jälkeen. Kun aloitin viikkoyhteenvedon kirjoittamista, huomasin perjantainpäivän kirjausten puuttuvan. Nämä taisivat kadota käynnistäessäni työkoneen uudelleen. Olen pitänyt tapana tallentaa tiedoston jokaisen muutoksen jälkeen, mutta jatkossa pitää olla huolellisempi välitallennusten kanssa. Jälkikäteen päivän asioiden muisteleminen ei ole optimaalinen tapa.

3.1.2 Viikkoarviointi, viikko 2

Toisen seurantaviikon tiistai on loppiainen, jonka jälkeen viimeisetkin joululoman viettäjät tyypillisesti palaavat töihin.

IDM-lomakkeilta löydettiin määritysvirhe, joka antoi lomakkeen täyttäjälle mahdollisuuden kirjata vastuuyksikkötietoihin mitä tahansa, eikä pakottanut valitsemaan asiakkaalla käytössä olevista vastuuyksiköistä. Tämä aiheuttaa ongelmia laiterekisterin ja laskutusautomaatioiden suhteen, joten tämä on korjattava ennen tuotantoon menemistä. Lisäksi esimieskohta oli mahdollista jättää täyttämättä.

Keskustelimme projektipäällikön kanssa IDM-tuotantoon vientiin liittyvistä yksityiskohdista. Tuotantoon vientiä varten tarvittaisiin tarkistuslista asioista, jotka täytyy huomioida IDM-järjestelmän yliheitossa vanhasta uuteen. Ilmeisesti käyttökelpoista tarkistuslistaa ei ole valmiiksi olemassa, vaan sellainen joudutaan luomaan testien yhteydessä. Selvää on, että ainakin käyttötuelle ja asiantuntijoille täytyy ohjeistaa toimintatavat ennalta määritellyissä ongelmatilanteissa, sekä miten tukipyyntöjä järjestelmään liittyen reititetään toiselle ja kolmannelle tasolle.

Keskustelimme lyhyesti asiakas b:n kanssa mitä asioita loppukäyttäjien näkökulmasta pitää saada valmiiksi ennen IDM-järjestelmä yliheittoa. Itse järjestelmän lomakkeet ovat sen verran yksinkertaisia, ettei varsinaisia koulutuksia tarvitse välttämättä järjestää. Ehkä asiakkaalta voisi kouluttaa järjestelmään muutaman yhdyshenkilön, jotka osaisivat tukea järjestelmän käytössä muita käyttäjiä. Isolle käyttäjämassalle voisimme tehdä videon lomakkeen käytöstä sekä kuvalliset ohjeet.

Vuodenvaihteiden työsopimusongelmien jälkeen pohdin, miten käyttäjän poistoprosessi saadaan toimimaan niin varmasti, ettei vääriä tunnusten poistoja tule. Entä jos esimies ei jatkossa luo työsopimusta ajoissa? Tällöin tunnukselle tehdään poistoprosessin mukaiset toimenpiteet, vaikka käyttäjä olisi oikeasti töissä. Tunnuslukitukset pitää ohjeistaa käyttötuelle huolellisesti ja heille pitää luoda selvä ohjeistus mitkä kaikki toimenpiteet täytyy tehdä, jos havaitaan väärin perustein poistoprosessiin meneviä tunnuksia. Kun tunnus poistuu, vapautuu siihen kytketty Office 365 -lisenssi. Office 365 -lisenssin poistuttua postilaatikko säilytetään kolmekymmentä päivää, tämän jälkeen postilaatikko poistuu palvelusta lopullisesti. Projektiryhmän kanssa täytyy keskustella, tarvitaanko uuteen IDM-järjestelmään jokin poistoprosessin estävä toiminnallisuus. Esimerkiksi boolean tyyppinen attribuutti, jonka kytkemällä true-asentoon poistoprosessia ei suoritettaisi. Tätä voitaisiin käyttää tilanteissa, joissa esimies ilmoittaa etukäteen, ettei työsopimusta saada ajoissa tehtyä.

Asiakas a:n toiminnanohjausjärjestelmästä tuotavien kenttien selvitys ei ole edennyt useista kyselyistä huolimatta. Asiasta on keskusteltu sisäisesti ja päätimme varata asiasta palaverin asiakkaan ja asiantuntijan kanssa. Ennen kyseistä palaveria projektiryhmän pitää kuitenkin pystyä muodostamaan selkeä näkemys tarvittavista kentistä.

Asiakas a:lle uuden IDM-järjestelmän palvelimia ei ole vielä tilattu. En saanut järjestelmäarkkitehdilta selvää vaatimuslistaa, joten tilaan identtisen ympäristön sen pohjalta, mitä asiakas b:lle tilattiin. Palomuuriavauksia ei voida tilata, ennen kuin palvelimille on määritetty IP-osoitteet. Asiakkaalle ei ole vielä pystytetty testiympäristöä, joten tuotantoympäristön puuttuminen ei vaikuta vielä aikatauluun.

Asiakas b on tilannut uudet M365 -lisenssit vuodelle 2020, mutta lisenssit eivät näy Microsoftin portaalissa oikean sopimuksen alla. Vanhat lisenssit ovat käytössä 60 vuorokautta, joten lisenssit on pakko saada helmikuun loppuun mennessä. Asiasta jouduttiin lopulta tekemään vikailmoitus Microsoftille.

Asiakas b:n uudessa IDM-järjestelmässä oli vielä vikakorjaukset käynnissä, mutta loppukäyttäjätestaukset aloitetaan aikataulun mukaisesti maanantaina 13.1. Asiakkaan henkilöstöhallinnon ja heidän palkanlaskennan toimittajan avulla saimme testimateriaalin, jolla lähdejärjestelmän rajapintaa voidaan simuloida. Testimateriaali oli kuitenkin erilaisella formaatilla mitä nykyisen IDM-järjestelmän saama siirtotiedosto, joten saatua testimateriaalia ei voida käyttää. Projektiryhmä päätti edetä varasuunnitelmalla ja generoida itse testimateriaalin oikeassa formaatissa.

Käyttötuki kirjaa työnohjausjärjestelmään jokaisen soiton ja työpyynnön, ja ne kategorisoidaan useampitasoisesti. Kollegan avustuksella löysin Microsoft Business Intelligence -järjestelmästä raportin, jolla saa kaikki palveluntarjoajan työnohjausjärjestelmän tapaukset ulos Excel-formaatissa. Kategorioilta suodattamalla sain ulos salasanan vaihtoa käsittelevät tapausmäärät jokaiselta kuukaudelta. Jokaiselle tapaukselle on merkattu myös käytetty työaika. Jatkan raportin jalostamista ja koostan arvion käytetyöstä työajasta, joka menetetään salasanojen vaihtamisen vuoksi. Raportit vaativat kuitenkin läpikäyntiä, sillä salasanan vaihtokategorian alle on virheellisesti kirjattu myös muunlaisia tapauksia. Lisäksi kirjatuissa työmäärissä on pientä hajontaa. Eniten ihmetyttää pieni joukko tapauksia, joissa käytetty työaika on yli viisin tai jopa yli kymmenkertainen. Jätän nämä tapaukset pois laskuista, sillä niissä on selvästi jouduttu tekemään enemmän kuin vaihtamaan asiakkaan salasana.

Asiakkaan AD:n ja matkapuhelinoperaattorin mobiilivaihteen integraatioprojektin aikataulu ei ole vielä tarkentunut. Odotamme lisätietoja viikon neljä jälkeen. Saimme operaattorilta kuitenkin siirtotiedoston, joka sisältää kaikki matkapuhelinliittymät. Listan perusteella

saamme vietyä numerot AD:lle, mutta ensin data on pystyttävä validoimaan. Numeroiden validointi on tärkeää, jotta voimme varmistua oikealle käyttäjälle vietävän oikean matkapuhelinnumeron. Väärän numeron yhdistäminen väärään käyttäjään aiheuttaisi sekaannuksen lisäksi tietoturvaongelmia, sillä numerotietoa käytetään salasanan itsepalvelussa tunnistautumiseen. Avaintietona on asiakkaan palkanlaskentajärjestelmän uniikki henkilönumero. Sama tieto pitää löytyä sekä operaattorilta numeron tiedoista että AD käyttäjätunnuksen attribuutilta. Vertailin dataa palkanlaskentajärjestelmän työsuhteiden kanssa, ja löysin yli kahdeksankymmentä eroavaisuutta vertaillessani sukunimitietoja vastakkain. Lähetimme datan asiakkaalle läpikäytäväksi. Saimme myös alustavan päätöksen, että numero viedään yhdessä merkkijonossa ilman välilyöntiä. Office 365 -tietoturvaominaisuuksien osalta ei suoriteta numeroiden palveluun ennalta vientiä, vaan asiakasta neuvotaan rekisteröimään käytettävä matkapuhelinnumero manuaalisesti.

Muuten viikko oli aika rauhallinen. Projektilta yli jäänyt työaika meni jatkuvan palvelun seuraamisessa ja koordinoinnissa. Asiakas b:lle tullaan tekemään Anti-Virus tuotteen vaihto sopimuksellisista ja ylläpidollisista syistä. Tuotteen vaihtoa varten on pohjatöiden tekeminen hyvällä mallilla ja asennuspaketit on saatu vakioitua sekä asiakas on toimittanut käytettävät lisenssit perjantaina.

3.1.3 Viikkoarviointi, viikko 3

Viikko kolme on vuoden 2020 ensimmäinen täysi työviikko. Asiakas b:n loppukäyttäjätestit alkoivat maanantaina testiympäristössä. Itse testit menivät hyvin, mutta korjattavia kohteita löytyi. Testaamisen suorittivat asiakkaan edustajat projektin testausvastaavan laatimien testitapausten pohjalta. Testeistä kirjattiin ylös 15 korjauskohdetta.

Järjestelmän lähettämät sähköpostit eivät menneet kaikissa tapauksissa perille käyttäjälle. Lisäksi viestien muotoiluista löydettiin vikaa.

Itse järjestelmän käyttöliittymän käännöstyöt englannista suomeksi ovat vielä kesken. Käännöstyöt on ehdottomasti saatava valmiiksi ennen käyttöönottoa. Käyttöliittymästä löytyi myös virhe, joka antoi esimiehelle mahdollisuuden muokata kaikkien henkilöiden tietoja, vaikka järjestelmän pitäisi rajata muokkausoikeudet vain omiin alaisiin. Käyttöliittymän lomakkeella käyttäjän on mahdollista kirjata kustannuspaikaksi mitä tahansa. Tämä tuo ongelmia myöhemmin laskutukseen ja raportointiin, joten kenttä on muutettava sellaiseksi, joka pakottaa käyttäjän valitsemaan jonkin olemassa olevista kustannuspaikoista.

Muita virheitä löydettiin kulunvalvontajärjestelmän integraatiosta, josta puuttui tietoja. Lisäksi luodun AD-käyttäjätunnuksen salasanan vaihdon pakotus ei toiminut ja osalla käyttäjätunnuksista oli tunnus luotu väärällä formaatilla.

Asiakkaan kanssa on sovittu järjestettäväksi uusi loppukäyttäjätestaus. Alustavasti käyttöönoton päivämääräksi on arvioitu 10.2. Pidän ajankohtaa henkilökohtaisesti kiirehdittynä.

Aiemmin kävimme asiakas b:n kanssa läpi AD-käyttäjätunnuksen poistoprosessia. Laadimme asiakkaalle ehdotuksen, jonka he tällöin hyväksyivät. Ehdotuksessa käyttäjätunnus lukitaan työsuhteen päätyttyä, ja poistetaan ennalta sovitun viiveen jälkeen. Viive sovittiin riittävän pitkäksi, että mahdolliset virhetilanteet työsopimuksen, eli lähdedatan kanssa saadaan tarvittaessa korjattua jopa loma-aikana. Tähän liittyen pitää miettiä ja sopia asiakkaan kanssa prosessi poikkeustapauksia varten. Poistoprosessia koskeva keskustelu heräsi vuodenvaihteen jälkeen, ja asiakkaan linjaus tunnusten poistosta on muuttunut, tai ainakin se on epäselvä. Tähän tarvitaan jonkinlainen päätös. Jos päätöstä ei saada ennen loppukäyttäjätestejä, pitää poistoprosessista karsia tunnuksen poistava osa pois, kunnes asia on selvä. Vaatimukset käyttäjätunnusten poistoista pitäisi mielestäni liittää asiakkaan sisäisiin ja ulkoisiin auditointivaatimuksiin. Mietittävä on, onko oikeasti tarve keskitetylle lokienhallintajärjestelmälle, mikäli AD-tunnusten säilyttämisen syyt ovat auditointivelvoitteet.

Selvitin työnohjaus järjestelmästä saatujen raporttien pohjalta mahdollisuuksia asiakas a:lle luotujen AD-käyttäjätunnus määrien selvittämiseksi sekä niihin käytetyn työajan arvioimiseksi. Raportilta kategorisointeja suodattamalla saadaan AD-tunnuksiin liittyvät työpyynnöt eroteltua. Ongelmaksi muodostuu kirjausten eli datan laatu. Kategorisoinneilla ei saa suodatettua selvästi pelkästään luotuja tunnuksia, joten työnohjausjärjestelmän datan perusteella on vaikeaa saada tarkkaa määrää luoduista käyttäjätunnuksista. Pyysin asiantuntijaamme ottamaan listauksen suoraan AD:lta. Tämän listauksen osalta sain luotettavat käyttäjätunnusmäärät laskettua, perustuen käyttäjätunnuksen luontipäivämäärän attribuuttiin.

Suodatin työnohjausjärjestelmän raportilta kaikki tapaukset, jotka kohdistuivat uusien käyttäjätunnusten luontia vuoden 2019 aikana. Jokaiselle työpyynnölle kirjataan tapaukseen menevä työaika. Jos työpyyntöä ratkaistaan useassa jaksossa, laskee järjestelmä palvelupyyntöön kohdistuvan kokonaisajan. Selvää keskiarvoa käytetystä työmäärästä on luoduille AD-tunnuksille vaikeaa antaa, sillä käytetty työmäärä heittelee todella paljon eri työpyyntöjen välillä. Haarukka asettuu kuitenkin pääosin 18 ja 40 minuutin väliin.

Asiakas a:n osalta on käyty keskustelua tarvittavista toiminnanohjausjärjestelmän poiminnan kentistä. Olemassa on jo jonkinlainen integraatio, jossa AD:n käyttäjätiedot täydennetään toiminnanohjausjärjestelmästä saatavan csv-tiedoston pohjalta. Siirtotiedosto täydentää kustannuspaikkaan sekä esimieheen liittyviä attribuutteja. IDM:n ja toiminnanohjausjärjestelmän välisessä integraatiossa käytettävät kentät on valittu perustuen olemassa olevaan csv-tiedostoon, ja asiantuntijoidemme mukaan pystymme päättelemään luotavien tunnusten sijainnin AD:n organisaatiorakenteessa sekä käyttöoikeudet riittävän pitkälti nykyisillä kentillä. Ongelmaksi muodostuu toiminnanohjausjärjestelmän datan laatu. Katsoimme dataa läpi yhdessä asiakkaan kanssa ja huomasimme, että ainakin vastuuyksiköitä käsittelevissä kentissä oli osalla käyttäjistä tiedot väärin. Nämä on korjattava asiakkaan toimesta ennen käyttöönottoa. Toiminnanohjausjärjestelmän osalta pohdimme myös, miten saamme tiedon poistuvista käyttäjistä.

Asiakas toivoo myös monityösuhdelogiikan rakentamista. Osalla määräaikaisista käyttäjistä on useampi yhtäaikainen työsuhde. Tämä tarkoittaa, että heillä on useampi esimies ja vastuuyksikkö samaan aikaan. Miten nämä tiedot viedään AD:lle sekä asiakkaan intranetin henkilöhakuun? Jos käyttäjälle viedään vain toisen työsuhteen tiedot AD:hen, mikä työsuhde valitaan?

3.1.4 Ensimmäisen seurantajakson kokonaisarviointi

Ensimmäisen seurantajakson yksi teema oli saada raportoinnin kautta näkymä salasanaitsepalvelun ja identiteetinhallinnan mahdollisuuksiin työmäärän säästön näkökulmasta. Raportoinnissa oli omat ongelmansa, mutta sain luotua näkemyksen käyttäjätunnusten luomiseen ja salasanojen vaihtoon kuluvasta työajasta. Raportointeja tehdessä ja opiskellessa kiinnitin huomiota datan laadun merkitykseen. Jos tapauksia ei kirjata johdonmukaisesti, heijastuu se lopulta raporteille datan heikkona laatuna. Tämä taas voi johtaa virheisiin laskutuksessa ja loppuasiakkaalle suoritettavassa raportoinnissa. Asia vaatii vielä syvällisempää lisätutkimusta sekä keskustelua käyttötuen esimiehen kanssa.

Sain luotua työnohjausjärjestelmän datan perusteella raportin käyttötuen tekemistä salasanan vaihdoista molempien asiakkaiden osalta. Työmäärät näkyvät samalla raportilla, mutta datan laadullisten ongelmien vuoksi salasanan vaihtojen alle on kirjattu myös pidempikestoisia ongelmia. Todennäköisesti tulen tekemään arvion perustuen massaan ja käytän tätä työmäärän arvioinnin pohjana.

Selvitin myös asiakas a:lle luotujen AD-käyttäjätunnusten määriä vuoden 2019 aikana. Työnohjausjärjestelmän raportilta kaikki luodut käyttäjätunnukset pitäisi löytyä, mutta en saanut suodatettua raportista luotettavasti pelkästään palvelupyyntöjä, joissa oli luotu uusi

käyttäjätunnus. Päädyinkin käyttämään AD:sta ajettua raporttia, jonka tunnusten luontipäivämäärän mukaan sain suoraan laskettua tunnusmäärät eri kuukausina. Kävin läpi työnohjausjärjestelmästä käyttäjätunnusten luontiin liittyviä tapauksia yksitellen ja muodostin sen pohjalta raja-arvot normaaliksi luokiteltaville AD-käyttäjätunnuksen luonnille. Selvää on, että tällä hetkellä käyttäjätunnuksen luomisessa menee sen verran paljon työaikaa, että vähäiselläkin palvelupyyntöjen määrällä käytetty kokonaistyöaika nousee korkeaksi.

Asiakas b:n osalta en laskenut luotujen käyttäjätunnusten määriä, koska ne luodaan jo nyt vanhalla IDM-järjestelmällä automaattisesti. Seuraavalla seurantajaksolla otan tavoitteeksi tehdä arvion asiakas b:lle luotavista ulkopuolisista käyttäjistä.

Työnohjausjärjestelmän kategorisointien ja eri lisäkenttien ristiinkäyttö hankaloittaa raportointia. Optimaalisessa tilanteessa samoja kategorisointeja käyttämällä saisi luotettavan raportin tehdyistä salasanan vaihdoista tai luoduista AD-tunnuksista. Nyt mielestäni dataan ei voi täysin luottaa. Ensisijaisesti tämä olisi mielestäni ohjeistus ja lisäkoulutusasia. Tutkittava on myös, onko nykyiset kategorisoinnit asiakkuutta palvelevia, vai onko siellä selviä puutteita tai käyttöpalveluiden henkilöillä näkemyseroja. Hyvin suuri osa palvelupyynnöistä kulkee käyttötuen kautta. Datan laatuun voisi saada parannusta jo pelkästään käyttötuen sisäisen keskustelun lisäämisellä kirjaamiseen liittyen. Käyttötuella on käytössään jonkinlaisia valmiita pohjia eri tilanteita varten. Näissä valmiissa pohjissa on kategorisoinnit ja mahdolliset asiantuntija jonot asetettu valmiiksi. Kategorisoinnit on katsottu käyttötuen työnjohdon ja palveluvastaavien kanssa yhdessä, joten niiden pitäisi olla kunnossa. Eri pohjien käyttöä eri tilanteissa pitäisi kuitenkin täsmentää jatkoa ajatellen datan laadun parantamiseksi.

Toinen seurantajakson teema oli saada asiakas b:n IDM projektin loppukäyttäjä testejä eteenpäin sekä miettiä hieman käyttöönoton asioita. Salasana itsepalvelun osalta alkuperäinen ajatus oli päästä tammikuussa tuotantoon. Ensimmäisen seurantajakson aikana ei tuotantoon kuitenkaan päästy kummankaan asiakkaan kohdalla. Asiakas b:n osalta ongelmana on matkapuhelinnumeroiden saaminen käyttäjien AD-tunnuksen attribuuttiin. Numeroiden vienti on kohtuullisen yksinkertainen toimenpide, mutta sitä varten tarvittaisiin asiakkaan operaattorilta poiminta matkapuhelinnumeroista ja niihin liitetyistä henkilönumeroista. Yksi versio listasta jo saatiin, mutta se jouduttiin hylkäämään valmiiksi vanhana. Operaattorilla on kestänyt useita viikkoja uuden listan toimittamisen kanssa. Toiveena on, että numerot saataisiin vietyä AD:lle helmikuun alun aikana. Saimme viikon neljä aikana operaattorilta viestin lisäviivästyksistä integraation kanssa.

Asiakas a:n osalta syy jäi viime palaverissa epäselväksi. Jouduin olemaan edellisistä seuranta kokouksista pois, joten yritän selvittää tilanteen viimeistään viikon viisi aikana.

Matkapuhelinnumeroiden osalta saimme päätettyä käyttäjän AD-tunnuksen attribuutille kirjoitettavan formaatin, joka palvelee sekä salasanan vaihdon itsepalvelua että Office 365 vahvan tunnistautumisen tarpeita.

Asiakas b:n osalta IDM:n loppukäyttäjätestit saatiin vietyä testiympäristöä vasten läpi. Testit menivät itsessään onnistuneesti, mutta korjattavaa jäi. Näistä jätinkin seuraavalle seurantajaksolle yhden tavoitteen. Uudet loppukäyttäjätestit kuitenkin tarvitaan. Projektiryhmälle oli jo aiemmin varattu aika käyttöönoton asioiden miettimiseen, mutta aika peruuntui. Pidän asiaa harmillisena, sillä käyttötuen että asiantuntijoiden ohjeistukset pitää saada selväksi palveluntarjoajan puolella. Asiakkaan puolella riittävä koulutus ja opastus on hoidettava riittävällä tasolla. Näiden asioiden pohjalta aiemmin ehdotettu 10.2.2020 käyttöönotto huolestuttaa minua.

IDM-järjestelmän käyttöliittymän lopullinen toteutus kirjautumisineen, siirtymineen ja valikoineen näyttelee isoa osaa lopullisen järjestelmän jalkauttamisessa asiakkaan käyttäjille sekä heille järjestettävän koulutuksen tarpeeseen. Mitä yksinkertaisemmaksi prosessi ja käyttöliittymä saadaan hiottua loppukäyttäjän näkökulmasta, sitä helpommalla projektiryhmä ja asiakkaan edustajat pääsevät järjestelmän jalkauttamisessa sekä tulevaisuudessa uusien esimiesten kirjautuessa ensimmäistä kertaa. Tavoitteena olisi saada järjestelmästä niin yksinkertainen, ettei perustoiminnallisuuksia varten tarvitsisi lukea käyttöohjeita. Valitettavasti projektissa ei ole mahdollisuutta suorittaa kunnollista käyttöliittymätutkimusta.

Asiakas b:n uuden IDM-järjestelmän käyttöönottoon liittyen muutamat prosessit vaativat lisää työstämistä. Oikeastaan käyttöönoton hetkellä kaikki järjestelmään liittyvät käyttötapaukset kuuluisivat olla kuvattuna prosessikaaviona. Tämän lisäksi vanhaan IDM-järjestelmään peilaten, tunnistan muutamia sovittavia prosessiasioita, joissa IDM-järjestelmää käytetään välillisesti aputyökaluna. Esimerkiksi ulkopuolisen henkilön tunnistamiseen tai työsuhteen varmistamiseen joissain tilanteissa.

Asiakas a:n osalta projektiryhmällä on jonkinlainen näkemys toiminnanohjausjärjestelmästä tarvittavista kentistä, mutta asiaa pitää varmasti tarkentaa vielä. Tuotantoympäristön palvelinten tilaaminen on viivästynyt, mutta tässä kohtaa projektia tuotanto ympäristöä ei tarvita vielä, joten viivästys ei vaikuta projektin aikatauluun.

Ensimmäisen seurantajakson aikana päiväkirjan ylläpito haki hieman malliaan, varsinkin ensimmäisen viikon aikana. Alkuunsa päiväkohtaiset kirjaamiset unohtuivat tehtävien ja palavereiden ohessa. Muutamaan otteeseen jouduinkin muistelemaan työpäivän jälkeen läpikäytyjä asioita, sekä palaamaan päivän sähköposteihin. Muutaman päivän jälkeen

rytmi päiväkirjan pitämiseen alkoikin muodostua. Koen asioiden saman tien kirjaamisen ylös helpoimmaksi vaihtoehdoksi.

Ensimmäisen seurantajakson kohdalla koen päiväkirjan tuovan suoran hyödyn asioiden jälkikäteen tutkiskelun ja mietiskelyn työkaluna. Tyypillisesti hektisinä työpäivinä ei asioita ehdi tai osaa miettiä syvällisesti. Päiväkirjaa viikkoraportiksi purkaessa tuntuukin, että viikolla käsiteltyyn asiaan löytää enemmän näkökulmia, kun antaa aivojen levätä asian osalta ja palaa myöhemmin asiaan. Päiväkirja toimii hyvänä muisti- ja tehtävälistana, johon on helppo palata ja siitä käy heti ilmi omat silloiset ajatukset asian tiimoilta. Kun alan purkamaan viikon merkintöjä tekstiksi, minut pakotetaan käsittelemään asiaa uudelleen ja pohtimaan sitä useasta eri näkökulmasta.

Pohdinkin, miten implementoisin päiväkirjan ylläpitämisen normaaleihin työskentelymenetelmiini. Päiväkirja voisi toimia ikään kuin suttupaperina ja sieltä virallinen tuotos olisi palvelu-, muutos- ja selvityspyynnöt sekä sähköpostiohjelman tehtävämerkinnät.

3.2 Toinen seurantajakso

Toinen seurantajakso käsittää 27.1.2020 – 16.2.2020 välisen ajan. Asiakas b:n osalta seurantajakson tavoitteena on salasanan vaihdon itsepalvelun käyttöönotto. Identiteetinhallinnan osalta tavoitteena on käyttöönottaa IDM-järjestelmä sekä ajaa vanha järjestelmä alas. Samassa yhteydessä pitää saada ratkaisu kolmansien osapuolten käyttäjätunnusten luomiseen.

Asiakas a:n osalta tavoitteena on saada salasanan vaihdon itsepalvelu itsepalvelun tuotantoon. IDM:n osalta projektissa pitää saada lyötyä lukkoon lähdejärjestelmänä toimivan toiminnanohjausjärjestelmän tietokentät sekä tiedonsiirtoformaatti.

3.2.1 Viikkoarviointi, viikko 5

Toisen seurantajakson ensimmäinen viikko oli molempien projektien osalta varsin hiljainen. Ensimmäinen projektin sisäinen tilannepäivityspalaveri peruuntui ja jälkimmäisen kanssa minulla oli toinen asiakaspalaveri samaan aikaan, jonka jouduin priorisoimaan projektipalaverin ylitse.

Projektin varsinainen projektipäällikkö on ollut useita viikkoja sairaslomalla, mutta viikolla kuusi projektin varsinaisen projektipäällikön pitäisi palata töihin. Tämän pitäisi hieman helpottaa asioiden edistämistä. Projektipäällikön tuuraaja on tehnyt hyvää työtä projektin osalta. Uskon asioiden etenevän hieman selkeämmin varsinaisen projektipäällikön palattua, sillä hänellä on mahdollisuus käyttää enemmän aikaa projektin vaatimiin tehtäviin, kuin oman työn ohessa häntä tuuraavalla.

Asiakas a:n kanssa pidetyssä palaverissa keskustelimme salasanan vaihdon itsepalvelun käyttöönotosta ja sitä pidättelevistä asioista. Asiaan ei minun mielestäni tullut vieläkään selkeyttä, enkä osaa sanoa mikä pidättelee tuotantoon vientiä. Keskustelimme samassa yhteydessä AD-käyttäjätunnusten matkapuhelinnumerotiedoista, mutta niiden pitäisi olla kohtalaisessa kunnossa asiakkaan osalta.

Kyselin uudelleen projektiryhmältä työmääräarviota ulkopuolisten käyttäjien lomakkeen luomisesta asiakas b:n uuteen IDM-järjestelmään. Työnkulku ja tarvittavat tiedot ovat valmiiksi tiedossa, joten suunnittelussa pitäisi päästä helpolla. En ole saanut kuitenkaan minkäänlaista vastausta työmäärä- ja kustannusarviosta lomakkeen osalta. Kun uusi IDM-järjestelmä otetaan käyttöön, suljetaan vanha IDM-järjestelmä ja samalla poistuu käytössä ollut ulkopuolisten käyttäjien lomake, ja mahdollisuus luoda ulkopuolisia käyttäjiä automatisoidusti. Uuden lomakkeen osalta tärkein tieto olisi mahdollinen aikataulutus. Aikataulu ohjaa ulkopuolisten tunnusten väliaikaista toteutusta.

Jos väliaika vanhan IDM-järjestelmän sulkemisen ja uuden IDM-järjestelmän lomakkeen väliin jää pieneksi, voidaan väliaika varmasti mennä Word-lomakkeiden avulla. Asiakkaan yhteyshenkilöille toimitettaisiin Word-lomakkeet, jotka asiakas liittäisi palvelupyynnön lisäksi. Tätä varten vaaditaan käyttötuelle ohjeet tunnusten luomisesta. Ennakoin tätä jo viimevuoden puolella ja pyysin asiantuntijaamme tekemään ohjeet valmiiksi.

Toinen vaihtoehto on tilata selainkäyttöinen lomake asiakasportaaliin. Lomake voi olla puoli- tai täysautomaattinen. Mikäli lomake luodaan täysautomaattisena, ei sitä kannata enää tehdä uudelleen IDM-järjestelmään. Mikäli osa käyttäjätunnuksiin liittyvistä toiminnallisuuksista on IDM-järjestelmän puolella ja osa asiakasportaalissa, aiheuttaa se loppukäyttäjissä hämmennystä ja sekaannusta.

Selvitin päätöksen tueksi ulkopuolisten käyttäjätunnusten luontimääriä asiakas b:llä viimeisen viiden vuoden aikana. Lukumäärät on esitetty kuviossa 1. Luotujen ulkopuolisten käyttäjientunnusten määrä on kasvanut vahvana trendinä vuodesta 2015 vuoteen 2018. Noiden neljän vuoden aikana tunnusmäärät ovat karkeasti kaksinkertaistuneet vuosittain. Vuoden 2019 aikana tunnuksia luotiin kuitenkin enää puolet edelliseen vuoteen nähden.

Uskon, että vuosien 2018 ja 2019 eroavaisuutta selvittää asiakkaan ostopalveluissa tapahtuneet muutokset sekä palveluiden ulkoistukset.

KUVIO 1. Asiakas b:n ulkopuolisten AD-tunnusten määrät viimeisen viiden vuoden aikana

Palvelutoimittajan kokemukseen perustuen asiakas b:n toimintaympäristössä yhden luodun ulkopuolisen käyttäjätunnuksen luomiseen ja tunnusten toimittamiseen kuluu aikaa noin kymmenen minuuttia. Aika pitää sisällään tapauksen kirjaamiseen kuluvan työajan. kymmenen minuutin arvion mukaan vuonna 2019 olisi kulunut arviolta noin kahdeksan henkilötyöpäivää ulkopuolisten käyttäjätunnusten tekemiseen manuaalisesti. Vuonna 2018 ulkopuolisten käyttäjätunnusten määrä oli suurimmillaan määrän ollessa reilut 700 kappaletta. Henkilötyöpäiviksi muutettuna käyttäjätunnusten manuaalisesti luominen veisi arviolta 16 henkilötyöpäivää.

Käytin tällä viikolla myös hieman aikaa taustamateriaalin etsimiseen. Löysinkin kolme opinnäytetyötä, jotka liittyvät tämän työn aiheeseen läheisesti.

3.2.2 Viikkoarviointi, viikko 6

Projektipäällikön paluu töihin toi odottamaani vauhtia projektiin. Heti viikon alussa asiakas a:n salasanan vaihdon itsepalvelun osalta saatiin asiakkaalta lupa käyttöönottoon. Tällä hetkellä asiakkaan työntekijöistä matkapuhelinnumero on AD:lla kolmasosalla käyttäjistä.

Kun AD:n ja asiakkaan operaattorin välinen integraatio saadaan tuotantoon, saadaan salasanan vaihdon itsepalvelu kattamaan kaikki loppukäyttäjät. Käyttöönotto vaatii vielä huolellisen asiakastiedottamisen sekä läpikäynnin käyttötuen kanssa. Mietimme mahdollisuutta tiedottaa käyttäjiä tekstiviestillä, tällöin ongelmatilanteessa olisi ohjeet puhelimessa valmiiksi. Lisäksi asiakas lupasi hoitaa sisäisen käyttäjätiedotuksen. Käyttötuen osalta pitää huolehtia, että he ovat ajan tasalla tilanteesta sekä ohjeistaa miten he toimivat ongelmatapauksissa. Ongelma voi koskea puuttuvaa matkapuhelinnumeroa tai salasanan vaihdon toteuttavaa ohjelmistoa. Lisäksi samalla pitää päivittää toimintaohjeet tapauksia varten, joissa käyttäjä pyytää salasanan vaihtoa puhelimitse.

Pidimme asiakas a:n edustajien kanssa työpajan, jossa mietimme heille tulevan IDM-järjestelmän tulevaisuutta. Ensimmäisessä vaiheessa IDM-järjestelmä tulisi luomaan käyttäjätunnukset AD:hen ja käyttäjätilin asiakkaan Office 365 -ympäristöön. Oletuksena tulevat AD-ryhmät ja niillä saatavat oikeudet on peilattu nykyiseen manuaalisesti tehtävään ohjeistukseen. Kun ensimmäisen vaiheen kanssa päästään tuotantoon, on tarkoitus kasata kehityspaketteja yhdessä asiakkaan kanssa. Järjestelmät joihin kirjautuminen tapahtuu asiakkaan AD-tunnuksilla, ovat varmasti ensimmäisissä kehityspaketeissa mukana, sillä niiden käyttöoikeuksien automatisointi on teknisesti helppoa. Suurempi haaste tulee määrittelytyöstä. Voidaanko käyttöoikeudet päätellä automaattisesti toiminnanohjausjärjestelmästä tulevan lähdedatan perusteella vai viedäänkö ne lomakkeille anottavaksi? Lomakkeelle viedyistä toiminnallisuuksista pitää sopia ketkä niitä saa anoa ja tuleeko niihin hyväksyntäkiertoa.

Asiakas b:n uuden IDM-järjestelmän aikataulu selveni hieman. Edellisessä loppukäyttäjätestauksessa löydetyt ongelmat on kohta saatu korjattua ja sisäinen testaus on tarkoitus pitää viikon kahdeksan aikana. Tämän jälkeen varataan aika asiakkaan kanssa uuteen loppukäyttäjätestaukseen. Jos testaukset menevät hyvin, voidaan tuotantoon mennä maaliskuun puolivälissä.

Asiakas b:n osalta saatiin vihdoin selvyys mitä ulkopuolisten käyttäjien luomisen kanssa tehdään jatkossa. Saimme sisäisen työmääräarvion lomakkeen luomisesta asiakasportaaliin. Työmääräarvion mukaan lomake olisi mahdollista toteuttaa automatisoidusti. Käytännössä asiakas täyttää lomakkeelle tiedot, ja tämän jälkeen järjestelmä luo ja lähettää tunnukset automaattisesti. Asiakkaan kanssa onkin päätettävä, lähetetäänkö tunnukset asiakkaan edustajalle vai suoraan henkilölle jolle tunnuksia anotaan. Jos tunnukset lähtevät suoraan henkilölle, jolle ne anotaan, pitää miettiä miten etäyhteyden ohjeet toimitetaan. Yksi mahdollisuus olisi viedä ohjeet nettisivuille, ja laittaa käyttäjätunnus viestiin linkki ohjeisiin. Asiakkaan täytyy määritellä käyttäjät, jotka lomakkeelle sallitaan. Aiemmin

asiakkaan kanssa on keskusteltu, ettei lomakkeelle tulisi hyväksyntäkiertoa vaan rajataan tiukasti käyttäjät, joille lomake sallitaan. Käyttäjät tulisivat olemaan tietohallinnon edustajia sekä liiketoiminnan yhteyshenkilöitä, jotka toimivat asiakkaan ostopalvelurajapinnassa.

3.2.3 Viikkoarviointi, viikko 7

Asiakas b:n matkapuhelinnumerot vietiin kertaluontoisesti käyttäjien AD-tunnuksien puhelinnumeroattribuuttiin, mutta vanha IDM-järjestelmä yliajoi tiedon metadatasta. Vanhan IDM-järjestelmän integraatio vanhaan puhelinvaihteeseen on sammutettu, mutta IDM pitää edelleen vanhaa järjestelmää lähdetietona, joten huomatessaan AD:lla tapahtuneen muutoksen, IDM tuo omasta tietokannastaan tässä tapauksessa vanhan tiedon päälle. Pyysin sovellustoimittajaa muuttamaan vanhan IDM:n AD integraatiota niin, ettei IDM päivitä enää puhelinnumero tietoa. Vanhan IDM-järjestelmän AD-ajurista estettiin muutokset AD:n puhelinnumero kenttiin, ja numerot ajettiin uudelleen. Operaattorin toimittamasta materiaalista saatiin numerot noin 2700 käyttäjälle. Huomioiden asiakkaan käyttäjä- sekä liittymämäärän, on tuo liian vähän. Käytännössä tämä tarkoittaa, että salasana vaihdon itsepalvelu saadaan käyttöön vain kyseisille käyttäjille, ja loput liittyvät palveluun sitä mukaa kun, heidän osaltansa saadaan matkapuhelinnumero AD-käyttäjätunnuksen tietoihin.

Lisäksi selvisi, että asiakas b:n asiakkaan yhteyshenkilö lomailee maaliskuun alusta kolme ja puoli viikkoa, eli käytännössä koko maaliskuun. Tilalle ei saada toista henkilöä, joten uudet loppukäyttäjätestit on pakko saada käytyä helmikuun aikana. Viikon loppupuolella näyttäisi lupaavalta, että vikoja on saatu hyvin korjattua ja sisäiset testit menevät läpi testiympäristössä. Myös uudet loppukäyttäjätestit on varattu helmikuun loppuun. Jos ne saadaan vietyä onnistuneesti läpi, voi projektiryhmä alkaa valmistelemaan käyttöönoton asioita. Kun asiakkaan yhteyshenkilö tulee lomalta, kaiken olisi hyvä olla valmista käyttöönottoa varten.

Asiakas a:n osalta salasanan vaihdon itsepalvelu käyttöönotosta on lähtenyt asiakastiedotteet. Myös käyttötukeen on toimitettu ohjeistukset ja tiedot, miten toimia tapauksissa, joissa tarvitaan korkeampaa tukitasoa.

Asiakas a:n IDM-järjestelmän palvelimet on vihdoin saatu asennettua ja järjestelmän käyttöliittymän tarvitseva julkinen varmenne saatu hankittua. Tilasin loppuviikosta palomuuriavaukset järjestelmää varten. Asiakkaan kanssa päätettiin käyttää nykyistä toiminnanohjausjärjestelmän siirtotiedostoa samoilla tietokentillä. Lisäksi formaatti tulisi pysymään csv-tiedostona.

3.2.4 Toisen seurantajakson kokonaisarviointi

Toisen seurantajakson aikana asiakas a:n salasanan vaihdon itsepalvelu otettiin käyttöön osalle henkilökunnasta. Asiakas b:n osalta AD:lle on saatu vietyä matkapuhelinnumerot ja salasana itsepalvelun työasemasovellus. Asennuksien osalta odotetaan asiakkaan lupaa. Sovelluksen asennusten jälkeen on käyttöönottovalmius.

Käyttäjätunnuspoistoprosessiin ei saatu vielä selkeää vastausta asiakkaalta. Prosessista on käyty asiakkaan kanssa keskustelua ja IDM-projektissa on tehty ehdotus, miten voitaisiin toimia, mutta projekti odottaa vielä lupaa asiakkaalta.

Kummallekaan asiakkaalle IDM-järjestelmää ei otettu käyttöön.

Asiakas b:n kanssa teimme päätöksen viedä kolmannen osapuolen käyttäjätunnushakemukset asiakassivuston lomakkeelle. Lomakkeen toiminnallisuus saadaan automatisoitua, ja määrittelyt voivat alkaa maaliskuun alkupuolella. Samalla täytyy tarkentaa käyttäjätunnuksen hakuprosessi asiakkaan kanssa. Vanhassa lomakkeessa on ollut erillinen hyväksyntäkierto, josta halutaan tässä yhteydessä eroon. Samalla nähdäkseni vastuu kolmansien osapuolten käyttäjätunnusten luomisesta pitää saada siirrettyä asiakkaan vastuulle. Myös kolmansien osapuolten käyttäjätunnusongelmien osalta pitää saada sovittua prosessi. Samalla on käytävät läpi, kuka on heidän yhteyshenkilönsä sekä miltä käyttäjä- tai sidosryhmältä toimittaja saa ottaa vastaan kolmansien osapuolten käyttäjätunnus aktivointeja ja salasanojen vaihtoja. Kun näihin asioihin saadaan vastaukset, tulee ne dokumentoida ja jalkauttaa käyttötukeen sekä asiakkaalle. Dokumentoinnissa on syytä miettiä mahdolliset asiakkaalle tehtävät auditoinnit, joten dokumentaation pitää pystyä vastaamaan mahdollisiin kysymyksiin prosesseista ja vastuutahoista.

Toisella seurantajaksolla isoksi haasteeksi muodostui henkilöresurssit. Automaatiopuolen asiantuntijoiden prioriteetti oli siirretty toiseen asiakkuuteen, joka aiheutti kolmen viikon tauon molempien asiakkaiden IDM-toteutuksissa. Asiantuntijoiden ja projektin arkkitehtien prioriteeteista tuntuu olevan talon sisällä kova kilpailu, joka tuo projektin aikatauluttamiseen isoja haasteita kaikissa asiakkuuksissa. Asiasta keskusteltiin yrityksemme korkeassa asemassa olevan johtoportaan edustan kanssa, joka yritti auttaa asian korjaamisessa, mutta valitettavasti isommat asiakkuudet pystyvät menemään prioriteeteissa ohitse.

Tämän lisäksi asiakkaan edustajat ja pilottihenkilöt ovat olleet poissa, tai tulevat olemaan lopputalven ja kevään aikana pitkiä aikoja lomalla. Pyysimme asiakas b:ltä korvaavaa

yhteyshenkilöä, mutta pyyntöön ei suostuttu. Käytännössä asiantuntijoiden priorisoinnin muutokset ja asiakkaan yhteyshenkilön pitkä loma viivästyttää IDM-järjestelmän käyttöönottoa huhtikuulle. Asiakas b:n tietohallinnon edustajien mukaan kuukaudenvaihteet eivät ole hyvä aika muutokselle, koska kuukauden vaihteessa on paljon muutoksia työsuhteissa. Tämä aiheuttaa heille työkuormituksessa piikin. Käytännössä realistista on saada tuotantoon vienti aikataulutettua viikoille 15 – 17.

Myös projektipäällikkö joutui olemaan sivussa melkein kuukauden. Hänellä oli kyllä hyvä sijainen, mutta asiat eivät edenneet samalla vauhdilla, koska hänellä ei ollut mahdollisuutta käyttää projektille aikaa yhtä paljon. Seurantajakson aikana keskustelimme moneen otteeseen projektipäällikön kanssa tilanteesta. Molemmat kokivat ajan todella tuskaisena, koska projektia ei saatu eteenpäin, eikä asiaan näyttänyt löytyvän tapaa tai henkilöä, jonka avulla tilannetta olisi voitu korjata.

Toisen seurantajakson aikana päiväkirjan pitäminen tuli selvästi paremmin selkärangasta. Mutta koska projekti ei edistynyt, ei päiväkirjamerkintöjäkään tullut samaan, tapaan kuin ensimmäisellä seurantajaksolla. Olen huomannut muistavani asiat paremmin, mikäli kirjaan ne ylös, vaikka vain itselleni. Koska nykyinen työnkuva käsittää paljon palavereita, olen ollut monesti vapaaehtoinen muistionpitäjä. Kun asiat kirjaa ylös, se pakottaa keskittymään itse asiaan. Tähän asti olen kirjannut muistioita sähköpostiin, mutta mietin parempaa tapaa ylläpitää tietoa. Asioita olisi helpompi käsitellä, jos tieto olisi koottu jotenkin helpompaan ja rakenteellisempaan muotoon, kuin sähköpostin arkistointi kansioittain. Yksi vaihtoehto olisi Microsoftin One Note -muistikirja. Muistikirjoissa voisi olla eri aihealueet ja ilmeisesti Outlook sähköpostiohjelmasta voi viedä suoraan sähköposteja osaksi muistikirjaa. Olen kokeillut merkitä osan sähköposteista itselleni tehtäviksi Outlookissa. Tämä helpottaa merkittävästi avoimien asioiden löytämistä, kunhan vain ymmärtää merkitä viestit tehtäväksi. Ongelmaksi on muodostunut oma rutiini, en ole löytänyt vielä luontaista rytmiä käydä Outlookin tehtäviä läpi päivittäin. Parasta varmasti olisikin varata tehtävien läpikäynnille 15 minuuttia joka aamulle päivän aluksi. Haaste tässä on palaverit, jotka alkavat pyörimään heti aamu kahdeksasta eteenpäin.

3.3 Kolmas seurantajakso

Kolmas seurantajakso kattaa 24.2.2020 – 15.3.2020 välisen ajan. Seurantajakson tavoitteena asiakas b:n osalta on saada aloitettua kolmansien osapuolten käyttäjätunnuslomakkeen suunnittelu ja hahmotella prosesseista ehdotus asiakkaalle. Lisäksi tavoitteena on

käyttöönottaa asiakas b:lle salasanan itsepalvelu sekä valmistella uusi IDM-järjestelmä käyttöönotto valmiiksi.

Asiakas a:n osalta seurantajakson tavoitteena on saattaa IDM-projekti tuotekehitysvaiheeseen ja saattaa salasanan vaihdon itsepalvelu tuotantoon.

3.3.1 Viikkoarviointi, viikko 9

Asiakas b:n kolmansien osapuolten käyttäjätunnuslomakkeen suunnittelusta pidettiin pari työpajaa ja ideoitiin sisäisesti. Lomakkeesta saatiin ensimmäinen hahmotelma lomaketyökaluilla toteutettuna. Alkuperäinen työmääräarvio oli laskettu täydelle automaatiolle, mutta tekninen toteutus on vielä hieman epäselvä. Todennäköisesti lomakkeesta tulee puoliautomaatio, jossa tunnus luodaan automaattisesti ja käyttöoikeudet määritellään lomakkeen avaaman tapauksen pohjalta manuaalisesti. Käyttäjältä kysytään tarvittavat käyttöoikeudet lomakkeella. Lomakkeen kentät tulevat suomeksi, mutta osa toiminnoista näyttäisi pysyvän englannin kielisinä, vaikka kielen vaihtaisikin suomeksi.

Asiakas b:llä IDM-projektia tai salasanan itsepalvelua ei päästä viemään tuotantoon ennen kuin asiakkaan yhteyshenkilö tulee lomalta viikolla 13. Ennen sitä on saatava korjattua viimeiset loppuasiakastestauksessa löydetyt virheet, saatava muodostettua pohjaa käyttöohjeille sekä valmisteltava käyttöönoton tarkastuslista.

Asiakas a:n tietohallinnon edustajan sekä toiminnanohjausjärjestelmän pääkäyttäjän kanssa on jatkettu IDM-järjestelmän tulevaisuuden kehityskohteiden miettimistä. Samaa pitäisi alkaa käymään läpi myös asiakas b:n puolella, mutta varmasti parasta ottaa ensimmäiset istunnot asiakkaan kanssa, kun ovat saaneet hetken tutustua uuteen järjestelmään.

3.3.2 Viikkoarviointi, viikko 10

Asiakas a:n IDM-projekti odottaa tällä hetkellä asiakkaan toiminnanohjausjärjestelmän toiminnanohjausjärjestelmän SaaS-toimittajalta hyväksyntää datalle tehtävistä poimintojen muutoksista. Tähän saakka toiminnanohjausjärjestelmästä on saatu vain muuttuneet tiedot kerran viikossa, jatkossa haluttaisiin tiheämmällä tahdilla kaikki työsuhteet. Kentät pysyvät ennallaan. IDM-projektiryhmän mukaan loppukäyttäjätestauksen valmius on kuusi viikkoa toiminnanohjausjärjestelmän poimintadatan saamisesta, eli itse kehitystä ei päästä

tekemään ennen kuin toimittaja hyväksyy poiminnan ja poiminta saadaan suoritettua niin, että lopputulos on sovittu.

Asiakas b:n IDM-projektissa pidettiin toinen loppukäyttäjätestaus, jossa keskityttiin testaamaan toiminnallisuudet, joista löydettiin ensimmäisellä kerralla virheitä. Testeissä löydettiin viisi korjattavaa virhettä, jotka liittyivät pääosin esimiehille lähetettäviin sähköposteihin. Yksi virheistä liittyi kulunvalvonnan automaation poimintaan. Nämä pyritään korjaamaan lähiviikkojen aikana.

Asiakas b:n osalta teimme analyysiä tulevasta IDM-järjestelmän käyttäjämäärästä. Käyttäjämäärä lasketaan laskemalla palkanlaskentajärjestelmän poiminnasta saatavat yksilölliset työsopimukset, sekä arvioidaan aiempien vuosien käyttäjämäärät opiskelijoiden ja ostohenkilöiden osalta. Työsopimusten perusteella asiakkaalla oli analyysinhetkellä hieman alle 6700 käyttäjää, joista reilulla 200 oli useampi työsuhde. Taulukossa 1 on esitetty asiakas b:n opiskelija ja ostohenkilö käyttäjämäärät vuosittain viimeisen viiden vuoden ajalta. Määrät perustuvat nykyisen IDM-järjestelmästä haettuihin käyttäjätunnuksiin.

TAULUKKO 1. Asiakas b:n opiskelija ja ostohenkilö käyttäjämäärät vuosittain

Vuosi	Opiskelija	Ostohenkilö
2019	655	474
2018	305	592
2017	324	272
2016	333	284
2015	312	207

Asiakas a:n salasanan itsepalvelun osalta keskusteltiin laskutusperiaatteista. Normaalisti salasanan vaihdon itsepalvelu kuuluu IDM-tuotteen hintaan, mutta koska salasanaosuus tulee ensin tuotantoon, on siitä sovittu erillinen väliajan veloitus. Veloitus pohjautuu käyttäjämäärään, nyt on keskusteltu asiakkaan kanssa lähinnä periaatteista. Käytännössä asiakasta voi veloittaa vain käyttäjistä, joilla on uniikki +358 -alkuinen matkapuhelinnumero AD-käyttäjätunnuksella. Raportin mukaan heitä olisi tällä hetkellä noin 1700 käyttäjää.

3.3.3 Viikkoarviointi, viikko 11

Asiakas a:n kanssa pidetyssä palaverissa päästiin yhteisymmärrykseen salasanaitsepalvelun käyttäjämäärästä ja käyttöönoton loput toimenpiteet sovittiin hoidettavan viikolla 12.

Käytännössä asiakas tiedottaa käyttäjiään ja projektipäällikkö käyttötukea ja palvelutuotantoa. Lisäksi sisäiset ohjeistukset ja loppukäyttäjän ohjeet pitää viedä paikoilleen sekä laittaa työasemalle asennettava sovellus jakeluun.

Asiakas a:n IDM-projekti pääsi hieman eteenpäin, sillä toiminnanohjausjärjestelmän SaaS-palvelutoimittaja hyväksyi tehtävät muutokset poimintaan. Projektiryhmän mukaan testausvalmius lähdedatan saamisesta on kuusi viikkoa, joten ensimmäisiä testauksia sisäisesti ja asiakkaan kanssa päästään näillä näkymin tekemään huhti-toukokuun vaihteessa.

Asiakas b:n osalta odotetaan asiakkaalta vahvistusta, koska voimme lähteä liikenteeseen salasanan vaihdon itsepalvelun osalta. Tällä hetkellä AD:lla on yksilöllinen matkapuhelinnumero +358 -formaatissa noin 2700 käyttäjällä.

Kuluvalla viikolla on ollut huolestuttavia uutisia korona viruksesta. Maan hallituksen esityksestä on tapahtumia ja tilaisuuksia peruttu. Paikallisuutisten mukaan myös molempien asiakkaiden toiminta-alueelta on löytynyt tartuntoja. Kuluvilla viikoilla varmasti selviää, vaikuttaako koronavirus projektin etenemiseen. Mahdollinen vaikutus voisi olla esimerkiksi, että asiakkaan edustajat alkavat priorisoimaan oman liiketoiminnan koordinointia projektin tehtävien ja kokousten edelle.

3.3.4 Kolmannen seurantajakson kokonaisarviointi

Kolmas jakso oli kahta edellistä seurantajaksoa hiljaisempi ja tämä näkyi myös vähäisinä päiväkirjamerkintöinä. Koska asiat etenivät verkkaisesti ja joiltakin osilta projekti on odotustilassa, sujui asioiden kirjaaminen helposti ja asiat oli helpompi myös tarkistaa sähköpostista. Projektien alussa olen perustanut molemmille asiakkaille sähköpostiin omat arkistot projekteja varten, joka helpottaa asioihin palaamista jälkeenpäin.

Asiakas a:n IDM-projekti odotti lähdedatan poiminnan hyväksyntää toiminnanohjausjärjestelmän SaaS-palveluntarjoajalta. Hyväksyntä saatiin lopulta asiakkaan kiirehtiessä hyväksyntää palveluntarjoajan suuntaan. Salasanan itsepalvelun tiedote ja jakelu saatiin vihdoinkin lähtemään viikon kaksitoista alussa, joten käytännössä sitä voidaan pitää vihdoinkin käyttöönotettuna.

Asiakas b:n osalta seurantajakson aikana projekti on ollut tyhjäkäynnillä tehden valmistelevia töitä asiakkaan edustajan lomaltapaluuta odotellessa. Tuotannolle, käyttötuelle ja asiakkaalle täytyy ennen käyttöönottoa dokumentoida ja ohjeistaa eri käyttäjätunnusten luomisen kanavat. Käytännössä käyttäjätunnukset jakaantuvat kolmeen eri kanavaan:

- lähdedatan perusteella automaattisesti muodostuvat
- IDM-lomakkeella luotavat käyttäjät, niin kutsutut ostohenkilöt ja opiskelijat
- kolmannen osapuolen tukitunnukset, asiakassivuston lomake.

Kolmannen osapuolen käyttäjätunnuslomakkeen osalta olemme pitäneet muutamia suunnittelupalavereja ja sen ulkoasu ja toiminnallisuudet alkavat olla aika pitkällä, joskin vielä demomuodossa. Odotamme asiakkaan edustajaa palaavaksi lomalta, jonka jälkeen asiasta varataan läpikäynti hänen kanssaan.

Salasanan itsepalvelu on käyttöönottovalmis molemmille asiakkaille. Aikataulutimme ohjelmistojakeluiden käynnistämisen ja loppukäyttäjien tiedotuksen viikolle 13. Uskon, että lähiviikkoina tätä tullaan hyödyntämään, sillä koronaviruksen vuoksi etätyöläisten määrä on rajussa kasvussa kaikkialla, myös meidän asiakkaiden keskuudessa.

Kuluneella viikolla koronaviruksella ei ollut projektiin suoraa vaikutusta, mutta pidän sitä suurena riskinä molemmille IDM-projekteille, sillä pitkittynyt poikkeustilanne syö asiakkaiden resurssia ja siirtää heidän keskittymistään heidän ydinliiketoiminnan tukemisen koordinointiin. Koronaepidemian pahentuessa on riskinä huomioitava myös mahdolliset sairastapaukset organisaatiossa. Lisäksi tilanteen pahentuessa on mahdollista, että kaikki ei-välttämätön -kehitys keskeytetään. Koronavirus on aiheuttanut myös käyttötukeen suuren määrän puheluita ja IDM-järjestelmän käyttöönottoa ei mielestäni voi suorittaa, jos käyttötuki on käyttöönoton hetkellä ruuhkautunut. Samalla täytyy varmistaa, ettei välittömässä näköpiirissä ole muita isoja muutoksia tai projektien käyttöönottoja.

Kolmannella seurantajaksolla päiväkirjamerkintöjä tuli huomattavasti vähemmän edellisiin jaksoihin nähden projektin seesteisen vaiheen vuoksi.

3.4 Neljäs seurantajakso

Neljäs seurantajakso kattaa 23.3.2020 – 12.4.2020 välisen ajan. Viimeisen seurantaviikon perjantai on pitkäperjantai. Seurantajakson tavoitteena asiakas a:n osalta on saada IDM-ratkaisu tuotekehitykseen ja käyttöönotettua salasanan itsepalvelu.

Asiakas b:n osalta tavoitteena on suorittaa käyttöönotto uudelle IDM-järjestelmälle sekä salasanan itsepalvelulle.

3.4.1 Viikkoarviointi, viikko 13

Projektille resursoitu IDM-arkkitehti vaihtui. Minulle selvisi vasta äskettäin, että projektiin alun perin resursoidulle arkkitehdille kyseinen projekti oli ensimmäinen nykyisillä tuotteilla tehtävä toteutus. Saimme onneksi tilalle erittäin kokeneen arkkitehdin, joka on työskennellyt vastaavien projektien ja tuotteiden kanssa vuosia. Sovimme, että uusi arkkitehti käyttää viikon 13 asiakas a:n toteutuksen läpikäyntiin ja seuraavan viikon asiakas b:n toteutuksen läpikäymiseen.

Asiakas b:n IDM-projektin käyttöönoton aikataulua jouduttiin siirtämään asiakkaan ilmoituksesta elokuulle koronaviruksen takia. Uutta aikataulua ei ole tarkennettu tai vahvistettu. Virusepidemian vuoksi asiakas keskittyy ylläpitämään nykyiset palvelut ja heidän tietohallintonsa on priorisoitu tukemaan epidemian vuoksi vaadittavia erityistoimia. Projektiryhmä miettii, miten lisäaika saadaan käytettyä hyödyksi. Tarkoituksena on valmistella ohjeet, prosessit ja tiedotus sellaiseen kuntoon, että ne ovat valmiina, kun asiakkaalta saadaan taas lupa jatkaa projektin käyttöönottoa. Yksi ehdotus on myös ollut kerätä kasaan ensimmäinen kehityspaketti, ja tuoda alun perin projektista kehitysvaiheeseen jätetyt toiminnallisuudet järjestelmään jo nyt, ennen varsinaista käyttöönottoa.

Asiakas a:n salasanan itsepalvelulle on suoritettu käyttöönotto, ja asiakas tiedottanut loppukäyttäjiään.

3.4.2 Viikkoarviointi, viikko 14

Asiakas b:n salasanan itsepalvelulla on täysi käyttöönottovalmius, mutta projekti odottaa asiakkaan kanssa käytävien laskutusasioiden hyväksyntää. Tämän jälkeen annetaan työasemalle tehtävälle sovellukselle asennuslupa ja tiedotetaan loppukäyttäjiä.

Asiakas a:n salasanan itsepalvelu on otettu käyttöön edellisellä viikolla. Asiakkaan kanssa käydään vielä läpi sopimusteknisiä asioita palvelun osalta. Olemme myös pohtineet mahdollisuutta tuottaa salasanan itsepalvelua kaupungin konserniyhtiöille. Ratkaisu olisi teknisesti valmis jo levitettäväksi, mutta vaatii ensin neuvottelut asiakkaiden ja palvelun tuottavan tiimin kesken. Tyypillisesti salasanan vaihdon itsepalvelu on paketoitu samaan pakettiin IDM-tuotteen kanssa, joten palvelua tuottavan tiimin pitää saada hinnoiteltua salasana palvelu irrallisena. Ainakin osalla olisi selvä tarve palvelulle, mikäli se saadaan hinnoiteltua järkevälle tasolle.

Asiakas a:n IDM-projektin osalta arkkitehti ja asiakas ovat käyneet läpi toiminnanohjausjärjestelmän tulevaa lähdeaineistoa, ja tunnistettiin tarve saada poissaolotiedot samaan

materiaaliin. Poissaolotiedot ilmeisesti tulevat jo poiminnasta, mutta eivät samaan siirtotiedostoon, joten oletuksemme on, että muutos toiminnanohjausjärjestelmän SaaS-palveluntuottajan päässä on nopea eikä vaadi enää erillistä hyväksyntäkiertoa.

Asiakas b:n IDM-projektissa uusi arkkitehti on tutustunut ratkaisukuvaukseen ja olemme käyneet sisäisesti hänen kanssaan läpi eri käyttäjätunnustarpeita sekä niiden luomisen prosessia ja mahdollisia virhetilanteita. Olemme käyneet myös keskustelua tuplatunnuksiin liittyvästä toiminnallisuudesta. Nykyisessä ratkaisukuvauksessa ei ole suunniteltu estoa luoda järjestelmällä samalle käyttäjälle useita voimassa olevia käyttäjätunnuksia. Käytössä olevassa vanhassa IDM-järjestelmässä tuplatunnusten muodostuminen on tehty vertaamalla järjestelmän metadataan tallennettua henkilötunnustietoa.

3.4.3 Viikkoarviointi, viikko 15

Asiakas a:n IDM-projektiin tehdään muutosehdotus projektin muutoshallintamallin mukaisesti. Projektin muutoshallintamallin mukaisesti projektipäällikkö laatii projektista muutosehdotuksen, jonka asiakkaan ja projektin johtoryhmän tulee hyväksyä. Muutosehdotuksessa ehdotetaan poissaolotietojen hyödyntämistä sekä monityösuhdelogiikan toteutusta. Nämä eivät kuuluneet projektin alkuperäiseen ratkaisukuvaukseen, jota vasten tekninen toteutus suunnitelma ja hyväksymistestauksen testitapaukset tehdään.

Asiakas a:n toiminnanohjausjärjestelmästä on saatu aiemmin muuttuneiden tietojen osalta poiminta kerran viikossa, jonka perusteella päivittyneet työsuhdetiedot on päivitetty käyttäjien AD-tunnuksille. Yhdistävänä avaimena on käytetty toiminnanohjausjärjestelmän henkilönumeroa. Menneellä viikolla selvisi, että IDM-projektia varten tehdyt poiminnan muutokset ovat rikkoneet aiemman siirron. Tämä aiheuttaa sen, ettei kustannuspaikkatiedot sekä esimiestiedot päivity käyttäjien AD-tunnuksille. Näitä tietoja käytetään hyväksi asiakasportaalin lomakkeilla ja automaatioissa.

Asiakas b:n osalta IDM-projektissa keskusteltiin lähinnä sisäisesti, miten aikaa tulisi hyödyntää sekä käytiin toteutusta läpi uuden arkkitehdin kanssa.

Koska asiakas b:n IDM-projektin tuotantoon vienti siirtyi aikaisintaan elokuulle, pudotettiin heille suunnitellun kolmannen osapuolen käyttöoikeuslomakkeen toteutuksen prioriteettia. Lomakkeesta ollaan tekemässä vastaavaa versiota asiakas a:lle, ja heidän lomakettansa on vastavuoroisesti priorisoitu korkeammalle. Päätös tehtiin koska asiakkaalla on käytössä oleva toimiva lomake, kun taas toisella asiakkaalla työnkulku on vielä manuaalinen.

3.4.4 Neljännen seurantajakson kokonaisarviointi

Asiakas a:n osalta seurantajakson aikana saatiin salasanan itsepalvelu käyttöön viivästyksistä huolimatta. Tulevaksi haasteeksi vielä jää toiminnallisuuden jalkauttaminen käyttäjille. Lähitulevaisuuden seurattavaksi asiaksi otetaan käyttötuen tekemien salasanan vaihtojen määrä, jonka perusteella voidaan karkeasti arvioida jalkautuksen onnistuneisuutta. Jotta jalkautuksessa onnistutaan, täytyy uudesta käytännöstä viestiä moneen otteeseen ja ohjeiden olla käyttäjien helposti löydettävissä. Lisäksi käyttötuen pitää osata tarjota vaihtoehtoa käyttäjälle, ennen kuin se tehdään käyttäjän puolesta. Toisena haasteena on saada kaikki käyttäjät rekisteröitymään palveluun, jotta käyttäjillä olisi oikeasti valmius vaihtaa salasananansa palvelun kautta.

IDM-projektin osalta seurantajakson aikana päästiin yksimielisyyteen toiminnanohjausjärjestelmän aineistoon tarvittavista muutoksista, sekä tehtiin projektiin muutosehdotus projektipäällikön toimesta. Muutosehdotukset tunnistettiin asiakkaan kanssa käytyjen keskusteluiden pohjalta.

Edellisen seurantajakson lopussa projektiin resursoitu IDM-arkkitehti vaihtui, jonka vuoksi molempien asiakkaiden toteutuksia on käyty uudelleen lävitse alusta asti. Keskusteluissa on selvinnyt, ettei projektiin aiemmin resursoitu arkkitehti ollut kokenut, eikä ollut tunnistanut asiakkaan sekä toimittajan puolelta kaikkia oleellisia tarpeita. Tämä johti asiakas a:n osalta projektin muutosehdotukseen. Asiakas b:n osalta voi muutosehdotus syntyä myös, mikäli tuplatunnusten muodostuminen halutaan estää.

Meneillään oleva koronaepidemia aiheutti asiakas b:n IDM-projektin käyttöönoton siirtymisen ja projektin pitkittymisen kesälomien jälkeiseen aikaan. Koska epidemian kestoa ei vielä pystytä arvioimaan, on mahdotonta sanoa koska järjestelmälle saadaan lupa viedä tuotantoon. Asiakas a:n projektiin epidemialla ei ole ollut vaikutusta.

Kaikkiaan neljäs seurantajakso oli projektin tuotosten osalta hiljainen, ja ainoastaan asiakas a:n salasanan itsepalvelu oli ainoa konkreettinen valmistunut toimenpide, sekin valmisteltu teknisesti jo aiemmin. Seurantajakso on ollut haastava arkkitehdin vaihtumisen ja koronaepidemian takia. Epidemian tuloa ei kukaan voinut tietää, joten sitä voidaan pitää ylivoimaisena esteenä.

Pohdiskelin tutkimuspäiväkirjamallia uudelleen oman työni kannalta ja sen soveltamista itse työhön. Opinnäytetyön pohjalta koen tutkimuspäiväkirjan sopivan metodeiltaan erinomaisesti kehittämis- ja tutkimushankkeisiin, sekä käyttöönottoihin. Näkisin että tutkimuspäiväkirjalla olisi suurin hyöty projektimaisessa työskentelyssä. Tutkimuspäiväkirjan ylläpito voisi olla projektipäällikön vastuulla, hänen ollessa projektissa se taho, jonka täytyy

olla aina perillä tilanteesta. Projektin lopuksi puhtaaksikirjoitettu tutkimuspäiväkirja toimisi osana loppuraporttia tai olisi sen liite. Tällöin projektin etenemisestä, päätöksistä ja ongelmista jäisi aikajana, johon on helppo palata myöhemmin. Jatkuvan palvelun, eli olemassa olevan palvelun tuottamisen ja ongelman selvityksen osalta, en koe tutkimuspäiväkirjasta lisähyötyä oman työni kannalta.

4 AUTOMATISOINNIN HYÖDYT LIIKETOIMINNALLE

Asiakkaille tehdyn identiteetinhallinnan suunnittelun sekä salasanan vaihdon itsepalvelun käyttöönoton yhteydessä suoritettiin tutkimustyötä palveluntarjoajan työnohjausjärjestelmästä ajetun raportin pohjalta. Molempien asiakkaiden osalta puhelimessa tehtävät salasanan vaihdot ovat prosessiltaan ja taustajärjestelmiltään identtiset. Raporttia tutkittaessa tuli selvästi ilmi tutkittavan datan heikko laatu. Heikko laatu kävi ilmi esimerkiksi isoina vaihteluina kirjatussa työajassa, kun raportilta suodatettiin salasanan vaihtoja tai uusien käyttäjätunnusten luonteja koskevat tapaukset. Kävi myös ilmi, että joitakin ongelmatapauksia oli kategorisoitu salasanan vaihdoksi, vaikka tapausta tarkemmin tutkiessa ei tästä ollut kyse. Vaikka määrällisesti väärin kategorisoinnit olivat hyvin pieni osa kaikista saman kategorisoinnin tapauksista, näille kirjattu työaika nosti laskennallista keskiarvoa. Tapauksia läpikäydessä ja alapuolella esitettyjä taulukoita koostettaessa on pyritty tunnistamaan ja poistamaan laskelmista väärin kategorisoidut tapaukset. Kirjattavien tapausten tietojen laadun parantamiseen tähtäävät toimet on aloitettu.

Alla on tuotu ilmi projektiryhmän sekä palvelutoimittajan havaintoja identiteetinhallinnan sekä salasanan vaihdon itsepalvelun hyödyistä. Salasanan vaihdon itsepalvelu tuotiin molemmille seurattaville asiakkaille uutena toiminnallisuutena. Identiteetinhallinta on toisella asiakkaalla ollut käytössä vuodesta 2011 kun taas toisella prosessi on manuaalinen. Tämä toiminnallinen eroavaisuus on antanut mahdollisuuden tarkastella identiteetinhallinnan tuomia hyötyjä jatkuvassa palvelussa jo ennen projektin käynnistämistä.

4.1 Identiteetinhallinnan hyödyt liiketoiminnalle

Identiteetinhallinnalla saavutetaan monia hyötyjä. Palvelutoimittajalle näkyvin hyöty on työmäärän säästö käyttäjätunnuksia luodessa ja poistettaessa. Taulukossa 2 on esitetty asiakkaalle manuaalisesti luotujen käyttäjätunnusten määrä vuoden 2019 aikana. Käyttäjätunnukset luodaan manuaalisesti asiakkaan täyttämän sähköisen lomakkeen tietojen pohjalta. Käyttäjätunnusten määrät ja niihin käytetty työaika on poimittu palvelutoimittajan työnohjausjärjestelmästä. Datasta kävi ilmi, että tarkkaa laskennallista arviota yhtä tunnusta kohden tehdystä työstä oli vaikea arvioida, sillä tunnuksen luomiseen käytetyissä työajoissa oli runsaasti hajontaa. Käytetty työaika on esitetty haarukkana tyypillisesti minimi ja maksimi arvosta, jotka raportilla toistuivat. Samat arvot tulivat ilmi keskustellessa tunnuksia luovien henkilöiden kanssa.

TAULUKKO 2. Asiakas a:lle luodut AD-tunnukset vuoden 2019 aikana

Kuukausi	**Kpl**	**Työaika (min)**
Tammikuu	57	1140 - 2280
Helmikuu	37	740 – 1480
Maaliskuu	38	760 – 1520
Huhtikuu	28	560 - 1120
Toukokuu	89	1780 - 3560
Kesäkuu	63	1260 – 2560
Heinäkuu	74	1480 – 2960
Elokuu	133	2660 – 5320
Syyskuu	53	1060 - 2120
Lokakuu	35	700 – 1400
Marraskuu	34	680 – 1360
Joulukuu	36	720 - 1440

Hiljaisin kuukausi käyttäjätunnusten määrän perusteella on ollut huhtikuu, 28 käyttäjätunnuksen määrällä. Työaikaa kului vähintään 560 minuuttia, eli noin 9 tuntia 30 minuuttia tai 1,25 henkilötyöpäivää. Eniten käyttäjätunnuksia luotiin elokuussa, jolloin luotiin 133 käyttäjätunnusta. Työaikaa näihin meni vähintään 2660 minuuttia, joka tekee noin 44 tuntia ja 20 minuuttia tai melkein kuusi henkilötyöpäivää.

Käyttäjätunnusten luomiseen menevän ajan lisäksi työaikaa kuluu myös lomakkeen täyttäviltä asiakkailta. Jos oletetaan uuden työntekijän käyttöoikeuslomakkeen täyttämiseen menevän viisi minuuttia, on huhtikuussa asiakkaiden aikaa mennyt 144 minuuttia, eli kaksi tuntia ja kaksikymmentä minuuttia. Elokuussa asiakkailla on mennyt käyttöoikeuslomakkeen täyttämiseen arviolta 665 minuuttia, joka tekee lähes puolitoista henkilötyöpäivää. Huomioitavaa kuitenkin on, että käytetty työaika jakaantuu useiden esimiesten kesken useisiin ajankohtiin.

Manuaalisesti ylläpidettävässä käyttöoikeusprosessissa tyypillinen perisynti on poistamatta jäävät käyttöoikeudet, sillä käyttäjätunnusten poistopyynnöt jäävät esimiehiltä

toimittamatta. Tietoturvan näkökulmasta organisaatiolla saisi olla voimassa olevat käyttäjätunnukset vain niillä käyttäjillä, jotka ovat organisaation palveluksessa. Automatisoidulla poistoprosessilla voidaan taata käyttöoikeuksien sulkeminen, kun käyttäjä poistuu organisaatiosta (Linden 2015). Poistoprosessiin voidaan kytkeä käyttäjäkohtaisten sovellus lisenssien vapauttaminen. Kun poistuvien käyttäjien lisenssit saadaan vapautettua automaattisesti tarpeen poistuttua, voidaan suorittaa tiukempaa lisenssioptimointia, josta seuraa asiakkaalle rahallisia säästöjä lisenssien määrien putoamisen myötä. Organisaatioille tyypillisiä käyttäjäkohtaisia lisenssejä ovat Microsoftin Office 365 -lisenssit sekä Adoben tuotteet.

Keskitetyllä identiteetinhallinnalla saadaan parannettua identiteettiin ja käyttäjiin liittyvän datan laatua. Integroimalla eri järjestelmiä, voidaan varmistua tiedon olevan ajan tasalla (Linden 2015). Esimerkiksi organisaatiomuutoksen yhteydessä muuttuvat kustannuspaikat saadaan päivitettyä identiteetinhallinnan avulla automaattisesti käyttäjille kaikkiin liitettyihin järjestelmiin. Lisäksi keskitetty identiteetinhallinta mahdollistaa auditoinnin kaikissa identiteetin elinkaaren vaiheissa.

Identiteetinhallinta antaa organisaatiolle mahdollisuudet uustiin toimintatapoihin. Käyttöoikeuksia, lisenssejä sekä muita kohteita voidaan viedä anottavaksi itsepalveluportaaliin, josta käyttäjä hakee käyttöoikeutta itse. Hakuprosessiin voidaan liittää digitaalisia hyväksyntäkiertoja kuten esimiehen, viranhaltijan tai järjestelmän pääkäyttäjän hyväksyntä.

4.2 Identiteetinhallinnan haasteita

Identiteetinhallinta nojaa identiteetti lähteeseen, johon pitää pystyä luottamaan. Jos identiteetin lähde on esimerkiksi organisaation HR- tai palkanmaksujärjestelmä, kaikki virheet ja puutteet näiden järjestelmien tiedoissa valuvat suoraan identiteetinhallintaan liitettyihin järjestelmiin. Esimerkiksi väärä kutsumanimi voi vaikuttaa suoraan käyttäjän sähköpostiosoitteeseen. Tai jos virheellinen tieto onkin yksilöiväksi tunnisteeksi määritellyssä tiedossa? Eräässä tapauksessa käyttäjälle tuli identiteettilähteestä väärä työsopimuksen voimassaolo päivämäärä. Tämä virhe lukitsi käyttäjän käyttäjätunnukset. Esiin on tullut myös virhe, jossa sadoilta määräaikaisen työsopimuksen käyttäjiltä on jäänyt pakolliseksi määritelty esimiestieto puuttumaan. Yksi tyypillinen ongelma on myös viiveet lähdedatassa. Jos identiteettilähde on HR- tai palkanmaksujärjestelmä ja prosessi käynnistyy esimiehen toimista kyseisessä järjestelmässä, ei hänen aloittava työntekijä saa käyttäjätunnuksia ennen kuin esimies on tehnyt määritellyt toimenpiteet lähdejärjestelmässä.

Identiteetinhallintaa rakennettaessa on helppo sortua kehittämään kerralla massiivista projektia. Parempi tapa on rakentaa hyvä perusta perustoiminnallisuuksin, ja tuoda uusia järjestelmiä ja käytäntöjä sen päälle omina kehityshankkeinaan. Tällöin kehitysprojektit pysyvät pienempinä ja paremmin hallinnassa. Lisäksi uusien toimintojen, ohjeistusten, prosessien ja käytäntöjen jalkauttaminen organisaatioon on helpompaa, kun muuttuvia asioita on kerrallaan vähemmän.

Vaikka identiteetinhallinta automatisoi asioita ja vähentää manuaalista työtä, se vaatii myös uuden roolin luomista organisaatioon. Identiteetinhallinta vaatii pääkäyttäjän, joka huolehtii datan laadusta ja omistaa identiteetinhallintaan liittyvät prosessit.

4.3 Salasanan vaihdon itsepalvelun hyödyt liiketoiminnalle

Yle Uutisten verkkosivuilta löytyvässä uutisessa vuonna 2014 kerrotaan Espoon kaupungin salasanan vaihtojen kustannusten olevan 200 tuhatta euroa vuodessa. Uutisen kirjoitushetkellä Espoon kaupungin tietotekniikkapalvelut ovat olleet ulkoistettu ja yhden salasanan vaihdon hinta on 18 euroa kerta. (Yle Uutiset 2014)

Oheisissa taulukoissa 3 ja 4, on esitetty asiakkaille manuaalisesti tehtyjen salasanojen vaihtojen määrät vuoden 2019 jälkimmäisellä puoliskolla. Kokonaistyöaika on laskettu viiden minuutin keskimääräisellä työajalla yhteydenottoa kohden. Työaika pitää sisällään tapauksen kirjaamiseen menevän ajan.

Asiakas a:lla eniten salasanan vaihtoja on tehty elokuussa. Salasanan vaihtoja tehtiin 293 kappaletta ja työaikaa niiden suorittamiseen käyttötuella kului henkilötyöpäiviksi muutettuna noin kolme henkilötyöpäivää.

Asiakas b:llä eniten salasanan vaihtoja on tehty syyskuussa, jolloin niitä tehtiin 542 kappaletta ja työaikaa niiden suorittamiseen käyttötuella kului henkilötyöpäiviksi muutettuna noin neljä ja puoli henkilötyöpäivää.

TAULUKKO 3. Käyttötuen asiakas a:lle kirjatut salasanojen vaihdot

	Kappaletta	**Kokonaistyöaika minuuttia**
Heinäkuu	188	940
Elokuu	293	1465
Syyskuu	235	1175
Lokakuu	178	890
Marraskuu	177	558
Joulukuu	138	690

TAULUKKO 4. Käyttötuen asiakas b:lle kirjatut salasanojen vaihdot

	Kappaletta	**Kokonaistyöaika minuuttia**
Heinäkuu	379	1895
Elokuu	413	2065
Syyskuu	542	2710
Lokakuu	374	1870
Marraskuu	270	1350
Joulukuu	282	1410

Itsepalveluna tehtävä salasanan vaihto mahdollistaa salasanojen vaihdon ympäri vuorokauden, vaikka palveluntuottajan ja asiakkaan väliset sopimukset tarjoavat vain toimistoaikaisen käyttötuen. Uuden salasanan saa välittömästi, käyttäjän ei tarvitse jonottaa puhelimessa.

Salasanan vaihdon vieminen itsepalveluksi lisää myös tietoturvaa, sillä käyttäjän tunnistamiseen voidaan kytkeä vahvan tunnustuksen elementtejä, ja täten itsepalveluna tehtävä

salasanan vaihto on hyvin suunniteltuna tietoturvan näkökulmasta luotettavampaa kuin puhelimitse käyttötuen tekemänä.

Lisäksi salasanan vaihdon vieminen itsepalveluun antaa palveluntuottajalle mahdollisuuden reagoida nopeasti mahdollisesti murrettuihin tai kalasteltuihin käyttäjätunnuksiin, sillä palveluntarjoaja voi suorittaa salasanan vaihdon välittömästi, kun havainto väärinkäytöksestä on saatu. Tällöin palveluntarjoajan käyttötuen ei tarvitse välttämättä tavoittaa loppukäyttäjää ennen salasanan vaihtoa, vaan käyttötuki voi vaihtaa salasanan ja tiedottaa käyttäjää tapauksesta, vaikka tekstiviestillä.

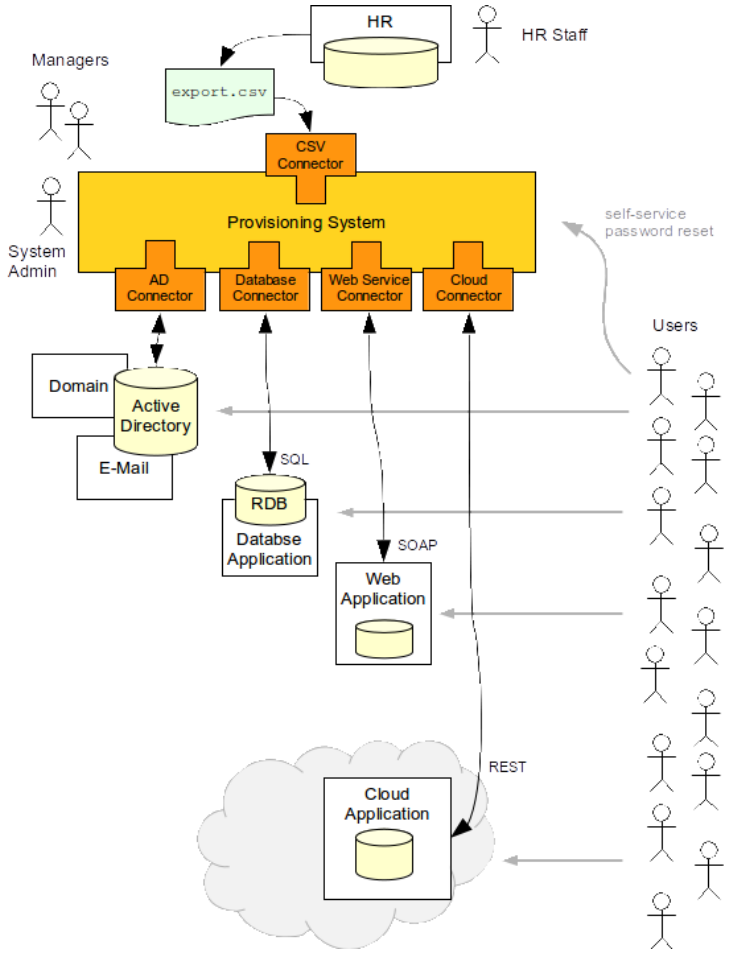
5 IDENTITEETINHALLINTA

Nykypäivänä organisaatioiden käyttäjillä on käytössään suuri määrä palveluita eri tarpeisiin. Osa palveluista voi olla tuotettu organisaation sisältä, kuten sähköposti ja intranet. Osa palveluista voi tulla palveluna organisaation ulkopuolelta, kuten Salesforcen kaltainen SaaS-palveluna tarjottava asiakkuudenhallintajärjestelmä. Identiteetinhallinnan tarve muodostui palveluiden, ja sitä myöten käyttäjätunnusten hallinnan ja ylläpidon määrän kasvettua ongelmalliseksi. Näistä aiheutui myös tietoturvaongelmia, koska käyttäjätunnuksia ei suljettu automaattisesti käyttäjän poistuttua organisaatiosta. Markkinoille alkoi tulla järjestelmiä identiteetin keskitettyä hallintaa varten, pyrkien ratkaisemaan ylläpidolliset ongelmat. (Linden 2015.)

Valtionvarainministeriön asettama Vahti -ryhmä laati vuonna 2016 henkilöstön ja johdon tietoturvabarometri -nimisen raportin. Raportissa avataan valtionhallinon ja julkisen hallinnon organisaation tehtyä kyselytutkimusta. Tutkimuksen mukaan valtiolla työskentelevistä henkilöistä 57,6% on käytössään yhdestä viiteen salasanaa. 30% työntekijöistä käyttää kuudesta kymmeneen eri salasanaa. Kuntapuolella eri salasanoja on tutkimuksen mukaan vähemmän kuin valtiolla. Eri kirjautumistavoista salasanaa käytettiin valtiolla 94.7% ja kunnilla 98,7% osuudella. Loppu jakaantuu kertakirjautumisen, toimikortin ja pin-koodin kesken. (Valtionvarainministeriö 2016.)

Identiteetinhallinnalla saavutetaan käyttäjänhallinnan osalta tehokuuta, parempaa laatua ja tietoturvaa. Kun samat toistuvat tiedot ylläpidetään keskitetyn järjestelmän toimesta, voidaan varmistaa, että tiedot ovat ajantasaiset eri kohteissa. Esimerkiksi sukunimen muutokset, kustannuspaikkatiedot ja esimiestiedot voidaan pitää ajan tasalla kaikissa identiteetinhallinnan piirissä olevissa järjestelmissä. Kun käyttäjän tunnukset kaikissa identiteetinhallintaan kytketyissä järjestelmissä saadaan suljettua automaattisesti, ei organisaatiosta poistuvan käyttäjän tunnukset ja käyttövaltuudet jää aktiivisiksi. (Linden 2015.)

Kuvassa 1 on kuvattu identiteetinhallintajärjestelmän perustoiminta. Uuden käyttäjän kohdalla identiteetinhallinnan työnkulku lähtee liikkeelle lähdejärjestelmästä, joka esimerkin tapauksessa on HR-järjestelmä. HR-järjestelmässä muodostuu siirtotiedosto, jonka identiteetinhallintajärjestelmä lukee ja käsittelee määritellyn rajapinnan kautta. Esimerkissä järjestelmä luo tunnukset yrityksen toimialueelle sekä luo sähköpostitilin, ja antaa käyttäjätunnukselle riittävät käyttöoikeudet eri rajapintoja pitkin eri järjestelmiin. Kun lähdedataan tulee käyttäjän osalta muutoksia, tieto valuisi kaikkiin liitettyihin kohde järjestelmin samaa työnkulkua myöten. (Evolveum 2020.)



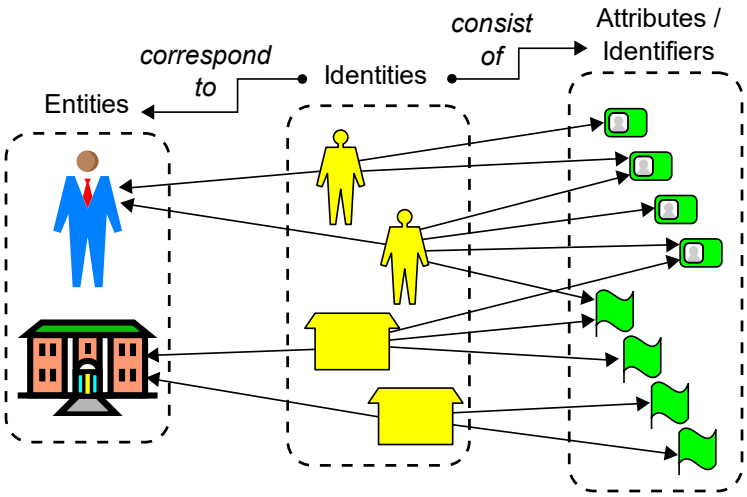
KUVA 1. Identiteetinhallintajärjestelmä (Evolveum 2020)

5.1 Mikä on identiteetti

Digitaalisessa identiteetissä kohteella on yksi henkilöllisyys, johon on liitetty useita identiteettejä eri tietojärjestelmissä. Identiteetti koostuu kohdetta kuvailevista attribuuteista. Identiteetti voi olla henkilön lisäksi myös yritys, laite tai tila, ja näillä kaikilla voi olla kohteen kannalta ominaiset attribuutit kuvaamassa identiteettiä. Yksi henkilöllisyys voi sisältää useita identiteettejä.

Esimerkiksi toimialueen käyttäjätunnuksella voi olla tallennettu sähköpostiosoite, katuosoite ja matkapuhelinnumero omiin attribuutteihin. Yrityksellä attribuutteja voisi olla taas toimitusjohtaja, yhteystiedot ja yritystunnus. (Linden 2015.)

Alapuolella esitetyssä kuvassa 2 on kuvattu sähköisen henkilöllisyyden rakennetta. Henkilöllisyys eli entiteetti on kuvattu vasemmassa laidassa. Yksi henkilöllisyys voi koostua useammasta identiteetistä, ja jokainen identiteetti koostuu joukosta identiteettiä kuvailevia attribuutteja.



KUVA 2. Identiteetin koostumus (Wikipedia 2020a)

Nykypäivänä käyttäjän identiteetti rakentuu muiden muassa seuraavien palveluiden käyttäjätunnuksista:

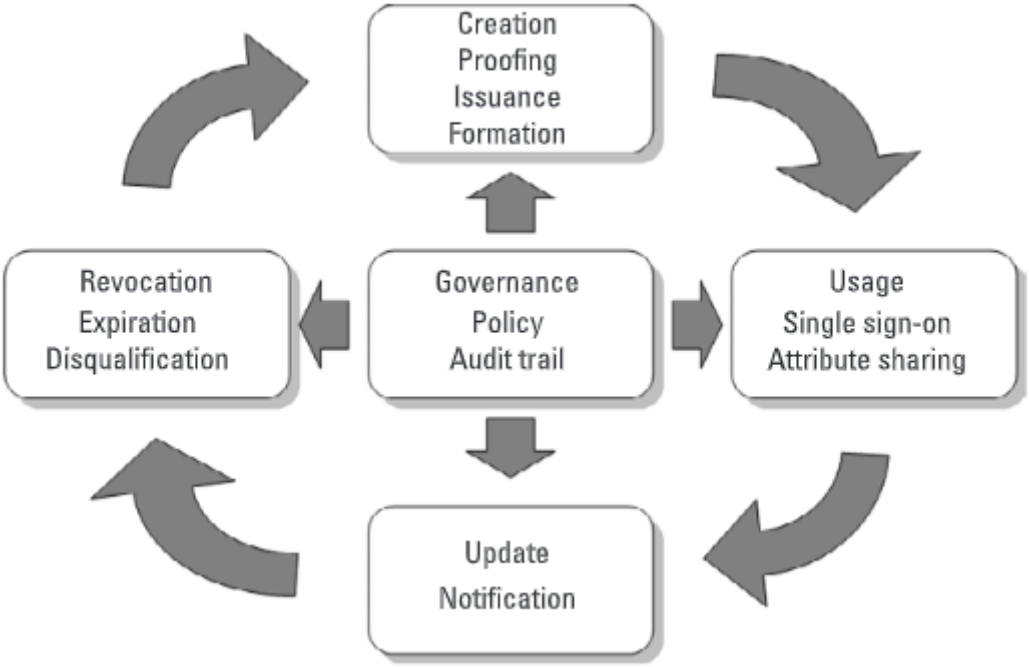
- työpaikan toimialueen käyttäjätunnus, jolla käyttäjä kirjautuu työasemalle sekä verkkolevyille
- Office 365 -pilvitili, johon on liitetty käyttäjän sähköposti, Teams, Intune laitehallintalisenssi sekä mahdollinen pääsy yrityksen pilvi Sharepointiin
- käyttäjätunnukset yrityksen toiminnanohjausjärjestelmään.

Identiteetinhallinnassa on kyse ennen kaikkea identiteetin prosessista ja sopimuksista. Sopimuksellisia asioita ovat esimerkiksi tietojärjestelmien rajapinnat sekä identiteetin formaatit eri kohteissa.

Identiteetillä voi olla yksiköllisiä tunnisteita, joilla varmistetaan identiteetin olevan uniikki. Tyypillisiä käyttäjään liitettyjä yksilöllisiä tunnisteita ovat sähköpostiosoite, yrityksen henkilötietojärjestelmän henkilönumero tai oppilaitoksen opiskelijanumero tai henkilötunnus. Yrityksellä yksilöivänä tunnisteena toimii yritysnumero. (Linden 2015.)

5.2 Identiteetin elinkaari

Samalla tapaa kuin organisaation tai henkilön identiteetti muuttuu ja päivittyy ajan kuluessa, tulee muutoksia myös sähköiseen identiteettiin. Henkilön identiteetin muutokset voivat olla esimerkiksi nimen, tehtävänkuvan tai osoitteen muutoksia. Organisaatiolla voi muuttuva tieto olla katuosoite tai nimi. (Bertino & Kenji 2010, 34-35.)



KUVA 3. Identiteetin elinkaari (Bertino & Kenji 2010, 30)

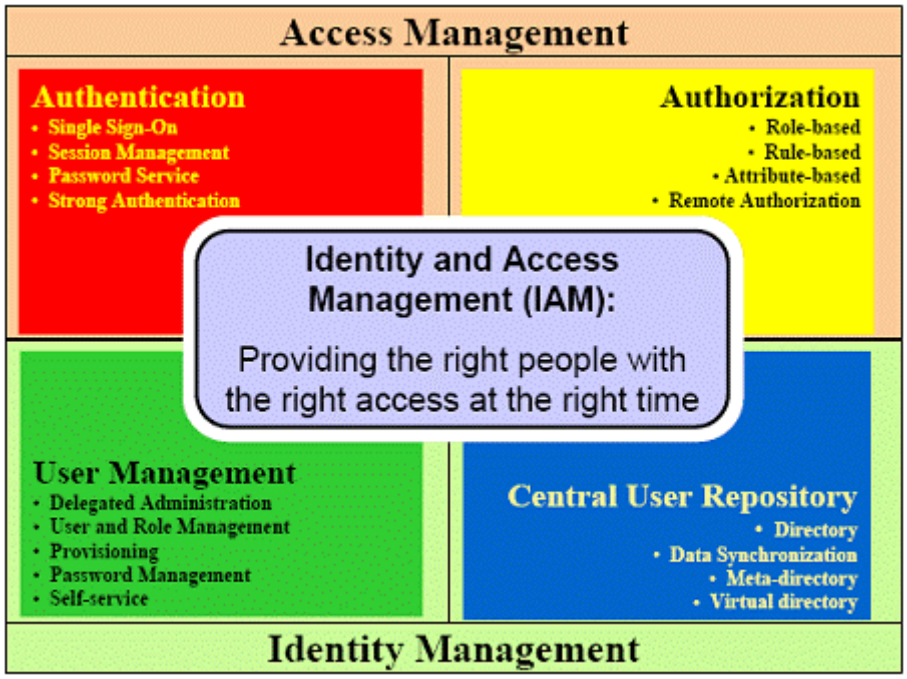
Kuvassa 3 esitetään identiteetin elinkaaren vaiheet, sekä niiden suhde identiteetinhallintapolitiikkaan. Identiteetin elinkaaren keskiössä on identiteetinhallintapolitiikka. Hallintapolitiikka asettuu varsinaisen identiteetinhallintajärjestelmän moottorin yläpuolelle, ja sillä säädellään identiteetinhallintaan ja auditointiin liittyviä säädöksiä. (Microsoft 2019f.)

Identiteetin elinkaari koostuu neljästä toimenpiteestä: luomisesta, käytöstä, päivittämisestä sekä poistosta. Identiteetti saa alkunsa luomisesta. Yksilöiviä tunnisteita verrataan olemassa olevien tunnettujen identiteettien yksilöiviin tunnisteisiin. Tarpeelliset tiedot kerätään identiteetin luomista varten. Yksilöivä tunniste määritellään identiteetin sitomiseksi henkilöllisyyteen.

Identiteetin luomisen jälkeen käyttäjä käyttää identiteettiä määriteltyihin palveluihin tunnistautumiseen. Tunnistautuminen voi tapahtua suoraan järjestelmää vasten, välitettynä tai kertakirjautumisen kautta. Identiteetin päivittyessä, attribuutteja päivitetään tulevan syötteen perusteella. Esimerkiksi sukunimen tai tehtävänimikkeen muuttuessa, tieto päivitetään rajapintoja myöten identiteetinhallinnassa oleviin järjestelmiin. Kun käyttäjä lopulta poistuu organisaatiosta ja siitä saadaan syöte identiteetinhallintaan, käynnistetään ennalta määritellyt toimenpiteet käyttöoikeuksien sulkemiselle ja tietojen poistamiselle järjestelmistä (Bertino & Kenji 2010, 29-35.).

5.3 Identiteetin- ja pääsynhallinta

Identiteetinhallintaan liittyy läheisesti lyhenne IAM. IAM on lyhenne sanoista identity access management, ja sen pääpaino on pääsynhallinnassa. Pääsynhallinta jakaantuu neljään osa-alueeseen: tunnistaminen, varmentaminen, käyttäjänhallinta sekä keskitetty käyttäjä arkisto. Identiteetinhallinta on keskeinen osa IAM kokonaisuutta, toisin sanoen identiteetinhallinnan lisäksi IAM:ssä tulee mukaan pääsynhallinta. (Information Technology Services Office of The Hong Kong Polytechnic University 2019.)



KUVA 4. IAM osa-alueet (Information Technology Services Office of The Hong Kong Polytechnic University 2019)

Kuvassa 4 on kuvattu IAM neljä osa-aluetta, sekä osa-alueiden jakaantuminen pääsynhallinnan ja identiteetinhallinnan kesken. Jokaista osa-aluetta on avattu muutamalla avainsanalla. Tunnistautuminen tuo käyttäjän kirjautumiseen ja tunnistamiseen liittyvät palvelut. Tunnistaminen pitää sisällään käyttäjien istuntojen hallinnan, vahvan tunnistautumisen sekä kertakirjautumisen. Valtuutus pitää sisällään roolipohjaisen ajattelun. Tässä osa-alueessa tehdään päätökset, onko käyttäjällä valtuutus määriteltyyn resurssiin vai ei. Roolipohjaiset säännöt voivat nojata käyttäjän tai resurssin identiteetin attribuutteihin, kuten kellonaikaan tai työtehtävään. Käyttäjänhallinnassa käyttäjien identiteetit luodaan, käsitellään identiteetin elinkaaren mukaisesti ja niille määritellään rooli ja käyttöoikeusryhmät. Käyttäjänhallintaan kuuluu itsepalvelu toiminnallisuudet, kuten salasanan vaihdon

itsepalvelu työkalu ja itsepalveluportaali käyttöoikeuksien ja sovellusten anomista ja asentamista varten.

Keskitetty käyttäjäarkisto on IAM-tuotteen arkisto, johon kohdejärjestelmiä liitetään yksi- tai kaksisuuntaisesti. Lähdejärjestelmästä voidaan pelkästään lukea tietoa tai sinne voidaan myös viedä tietoa tarpeen mukaan. Keskitetyssä arkistossa saadaan eri lähteissä sijaitsevat identiteetit sidottua yhdeksi digitaaliseksi identiteetiksi. (Information Technology Services Office of The Hong Kong Polytechnic University 2019.)

IAM hyödyt tulevat tehokkuuden ja tietoturvan kasvamisesta organisaatiossa. IAM automatisoi ja tekee käyttäjänhallinnasta sekä pääsynhallinnasta järjestelmällisempää. IAM-järjestelmän käyttöönotto auttaa täyttämään lain vaatimukset yksityisyydensuojan tai henkilötiedon sisältävän tiedon osalta. Lisäksi IAM avulla saadaan näkyvyys ja auditointi käyttöoikeuden haltijoista eri järjestelmissä. (Kuntaliitto 2013.)

5.4 Tietosuojalaki ja identiteetti

Tietosuojalaki täydentää ja täsmentää Euroopan parlamentin ja -neuvoston yleistä tietosuoja-asetusta 2016/679 (Tietosuojalaki 2018). Tietosuoja-asetuksesta käytetään myös GDPR-lyhennettä, joka tulee sanoista General Data Protection Regulation. GDPR korvaa aiemman käytössä olevan tietosuojadirektiivin.

Henkilötiedoksi määritellään kaikki tiedot, joiden avulla luonnollinen henkilö voidaan tunnistaa joko suoraan tai toiseen tietoon yhdistämällä. Esimerkiksi nimi, henkilökohtainen sähköposti ja puhelinnumero ovat henkilötietoa (Tietosuojavaltuutetun toimisto 2020a). Mikäli henkilötietoa sisältävän rekisterin ylläpitävässä organisaatiossa työskentelee yli 250 henkilöä, tulee tehdä seloste henkilötietojen käsittelytoiminnasta. Selosteen täytyy kattaa kaikki käsittelytoimet. Seloste vaaditaan organisaation työntekijöiden määrästä riippumatta, mikäli henkilötietojen käsittely ei ole satunnaista, käsittely aiheuttaa todennäköisen riskin henkilön oikeuksille, henkilötieto koskee erityisiä tietoryhmiä tai henkilötieto koskee rikostuomioista tai rikkomuksista tuomittuja (Tietosuojavaltuutetun toimisto 2020b).

Tietosuoja-asetus määrittää henkilöille oikeuksia koskien organisaation suorittamaa henkilötietojen käsittelyä. Henkilöllä on oikeus saada tietoa henkilötietojen käsittelystä, saada häntä koskevat tiedot ja mahdollistaa niiden oikaisu, poistaa tiedot, rajoittaa tai vastustaa tietojenkäsittelyä, siirtää tiedot järjestelmästä toiseen sekä oikeus olla joutumatta automaattisen päätöksenteon kohteeksi. Huomioitavaa kuitenkin on, ettei kaikissa tilanteissa

kaikki oikeudet ole voimassa, vaan ne on säädetty tietosuoja-asetuksessa tarkemmin. (Tietosuojavaltuutetun toimisto 2020d.)

Henkilötietoa käsitellessä tulee noudattaa tietosuojaperiaatteita. Rekisterinpitäjän täytyy pystyä osoittamaan noudattavansa näitä periaatteita. Tietosuoja-asetuksen määrittelemät tietosuojaperiaatteet ovat (Tietosuojavaltuutetun toimisto 2020c):

- lainmukaisuus, asianmukaisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- säilytyksen rajoittaminen
- luottamuksellisuus ja turvallisuus.

Identiteetinhallinnan järjestelmässä säilöttävät tiedot ovat yhdistettävissä henkilöllisyyteen. Oikeustieteessä henkilöstä käytetään termiä luonnollinen henkilö. Tällöin identiteetinhallintajärjestelmää pidetään henkilörekisterinä, ja siitä tulee laatia tietosuojalain mukainen seloste henkilötietojen käsittelytoiminnasta. (Linden 2015.)

5.5 Muutamia markkinoilla olevia tuotteita

Markkinoilla useita identiteetinhallinnan järjestelmiä. Osa järjestelmistä asennetaan perinteisesti organisaation ympäristöön, ja organisaatio itse tai kumppani ylläpitää palvelimia. Monet palveluntarjoajat ovat alkaneet tarjota identiteetinhallinnan järjestelmää asiakkailleen palveluna. Alla on lyhyesti esitelty kaksi eri järjestelmää. Microsoftin Identity Manager edustaa pilvipalvelu ratkaisua, jossa asiakas maksaa Azure -lisenssien muodossa kuukausi hintaa palvelusta. Toinen esiteltävä tuote on NetIQ Identity Manager, joka edustaa perinteisesti organisaation itse ylläpitämää ratkaisua.

5.5.1 Microsoft Identity Manager (MIM)

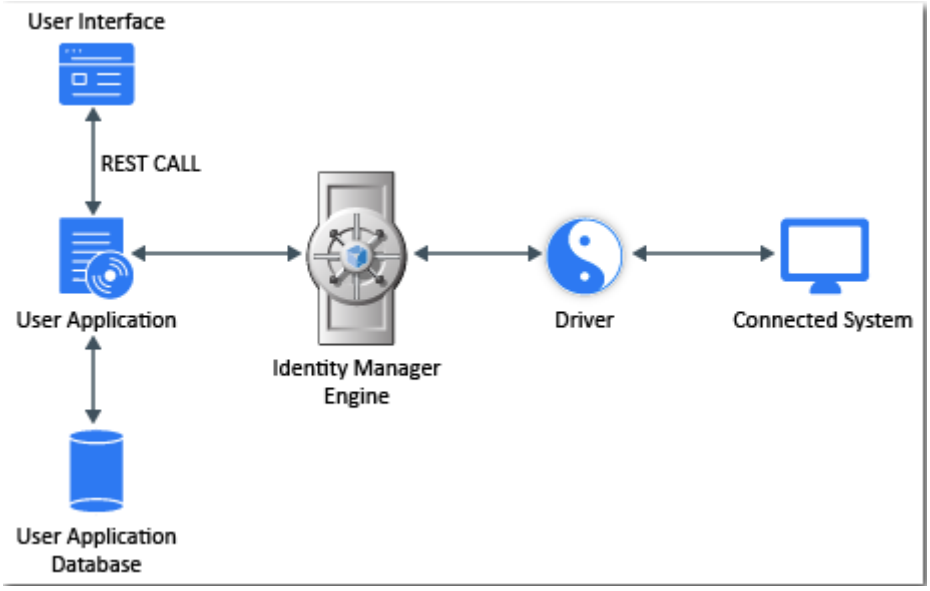
Microsoft identity managerin, lyhennettynä MIM, versio 2016 sisältyy osaksi Microsoft Azure Active Directory P1 ja P2 lisensointia (Microsoft 2019d). MIM sisältää yli kaksikymmentä valmista rajapintaa, joilla järjestelmä saadaan kytkettyä liiketoiminnan sovelluksiin. Valmis rajapinta löytyy esimerkiksi Microsoft, IBM ja Oracle tietokantoihin, Sharepointiin,

Active Directoryyn sekä geneeriset ajurit tekstitiedostoja, Powershell-komentoja ja ldap-kyselyitä varten. Microsoft identity manager tarjoaa mahdollisuuden itsepalveluportaaliin sekä vahvaan tunnistautumiseen (Microsoft 2019a).

5.5.2 NetIQ Identity Manager

NetIQ Identity Managerin kehitti Yhdysvaltalainen Novell, joka siirtyi vuonna 2014 tehdyssä kaupassa osaksi Microfocus yhtiötä ja siten NetIQ:lle, jonka Microfocus oli hankkinut vuonna 2006. Identity Manager tuli markkinoille lokakuussa 2010 Dirxml tuotenimellä. Tuote suunniteltiin synkronoimaan tietoa eri järjestelmien välillä. Myöhemmin järjestelmä kehittyi identity manager tuotteeksi (Wikipedia 2020b).

Kuvassa 5 on kuvattu Identity Managerin toimintaperiaate. Netiq identity managerin pohjalla on eDirectory hakemistopalvelu, jonka päälle asentuu Identity Mangerin moottori. Netiq ratkaisussa identiteetinhallinnan järjestelmä toimii keskitettynä holvina, tallentaen kaiken tiedon eDirectory hakemistoon objekteiksi ja niiden attribuuteiksi. Identiteetinhallinnan moottori liitetään ajureiden avulla lähde ja kohde järjestelmiin. Ajuri on identiteetinhallinnan moottorin pyörittämä toiminnallisuus, joka hyödyntää lähdejärjestelmän tarjoamaa rajapintaa ajurissa määritellyn politiikan perusteella.



KUVA 5. NetIQ Identity Manager (NetIQ 2020)

6 KÄYTTÄJÄN TUNNISTAMISEN TIETOTURVA

Käyttäjätunnus ja salasana -parilla on tarkoitus tunnistaa käyttäjä. Salasana muodostuu merkeistä ja muodostaa merkkijonon, jotka käyttäjä määrittelee ja tietää vain itse. (Valtion tieto- ja viestintätekniikkakeskus 2020.)

Organisaation käyttäjät kirjautuvat työasemalle tai Microsoft Office 365 -palveluun henkilökohtaisella käyttäjätunnuksella. Käyttäjätunnus luodaan organisaation Active Directory toimialueelle ja federoidaan sieltä Microsoft Azureen, josta Office 365 -tunnustietoja käyttää. Microsoft Office 365 -pilvipalvelusta voidaan tuottaa sähköpostin lisäksi useita tiimityöskentelyyn ja tiedostojen jakamiseen liittyviä palveluita. (Microsoft 2020c.)

Tyypillisesti pitkien vuosilomajaksojen, kuten kesä- ja joululomien jälkeen asiakkaiden käyttötuessa näkyy selvä piikki salasanojen vaihdoissa. Riippuen asiakkaan ja palveluntuottajan välisistä sopimuksista ja hinnoittelu malleista, tämä voi tuottaa asiakkaalle merkittäviä lisäkustannuksia, mikäli käyttötuki pohjautuu palvelupyyntö pohjaiseen laskutukseen. (Yle uutiset 2014.)

6.1 Hyvä salasana

Suositukset hyvästä salasanasta ovat hieman muuttuneet ajan saatossa. Näkyvin muutos on tietoturvayhtiöiden sekä Microsoftin suositusten muutos salasanan vaihtoa koskien. Nykyisissä suosituksissa salasanan vaihtopakkoa määräajoin ei suositella, vaan sen tilalle on tuotu vahva tunnistautuminen (Microsoft 2019e). Pakotetun salasananvaihdon vuoksi osa käyttäjistä käyttää uudelleen vanhoja salasanoja, salasanat ovat laadultaan heikkoja tai muuttavat vanhaa salasanaa niin, että hyökkääjän on helppo arvata uusi salasana (Microsoft 2020f).

Viestintäviraston alainen kyberturvallisuuskeskus suosittelee seuraavasti (Viestintävirasto 2020):

- vähintään 15 merkkiä
- salasana ei sisällä oikeaa sanaa, vaan on muodostettu tai lyhennetty esimerkiksi lauseesta
- isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä
- näppäimistön geometristen kuvioiden kuten qwerty, henkilökohtaisten tietojen tai yleistensalasanojen käyttö ei ole suositeltavaa.

Microsoftilla on myös omat suositukset Office 365 -pilvipalvelun kanssa käytettävään hyvään salasanaan (Microsoft 2020d):

- vähintään kahdeksanmerkkinen salasana
- ei erikoismerkkien yhdistelmiä
- ei säännöllistä salasanan vaihtopakkoa
- estä yleisimpien salasanojen käyttö
- ohjeista käyttäjiä käyttämään töissä ja vapaa-ajalla eri salasanaa
- vaadi monivaiheinen kirjautuminen.

Taulukossa 5 on esitetty Valtionneuvoston materiaalista esimerkin omaisesti salasanan vaikeuden vaikutus sen murtamiseen kuluvaan aikaan. Valtionneuvoston materiaalin mukaan helppo salasana saadaan nykypäivänä murrettua sekunneissa. Mikäli salasana on sanakirjasta löytyvä sana, mutta siihen lisätään numeroita ja erikoismerkki, pitenee murtoaika kymmeniin tunteihin. Täysin sattumanvarainen merkkijono, joka sisältää erikoismerkkejä ja numeroita kasvattaa salasanan murtamiseen menevän ajan yli kymmeneen vuoteen. (Valtion tieto- ja viestintätekniikkakeskus 2020.)

TAULUKKO 5. Salasanojen vaikeuden vaikutus salasanan murtamiseen kuluvaan aikaan (Valtion tieto- ja viestintätekniikkakeskus 2020.)

Salasana	**Murtoaika (Moderni PC)**	**Murtoaika (klusteri)**
salasana	8.3 kuukautta	2.17 sekuntia
S4las4n@	2130 vuotta	18.6 tuntia
ThxQJ##!09 (VAHTI-suositus)	19.2 milj. vuotta	19.24 vuotta
K2jTTvz%ZwHz/6S	150000 mrd vuotta	150 mrd vuotta
entten tentten teelikamentten	732 miljoonaa triljoonaa	Triljoonaa vuotta

6.2 Salasanojen hallinta

Salasanojen käyttöön on saatavilla myös apuohjelmistoja ja palveluita kuten F-Secure Key ja Lastpass kaupallisista ratkaisuista, sekä ilmaisista KeePass. Näissä apuohjelmissa käyttäjätunnuksista ja salasanoista luodaan tietokanta, joka salataan pääavaimella. Käyttäjän määrittelemän pääsalasanan takana on kaikki hänen ohjelmistoonsa lisäämät salasana. Näin muistettavana on vain yksi salasana usean sijaan. (Viestintävirasto 2020.)

Valtionvarainministeriön tietoturvabarometrin mukaan, valtiolla kyselyyn vastanneista salasanojen hallintaohjelma on käytössä 18,7% työnantajan toimesta. Kunnilla vastaava osuus oli 21,6%. (Valtionvarainministeriö 2016.)

Salasanan hallintaohjelmistoa käytettäessä pääsalasanan on oltava tietoturvallinen. Kaupallinen Lastpass -palvelu suosittelee pääsalasanaksi kahdestakymmenestä kolmeen kymmentä merkkiä pitkää salasanalausetta, jossa on mukana hyvän salasanan mukaisesti eri kokoisia kirjaimia, numeroita ja erikoismerkkejä. (Lastpass 2018). Salasananhallinta ohjelmistoon kirjautumiseen voi kytkeä salasanan lisäksi myös lisäturvaa tuomaan jotain käyttäjällä fyysisesti olevaa. Tällöin saadaan luotua kirjautumiseen vahva tunnistautuminen. Yksi vaihtoehto on käyttää usb-muistitikun kaltaista Yubico -laitetta. (Lastpass 2020.)

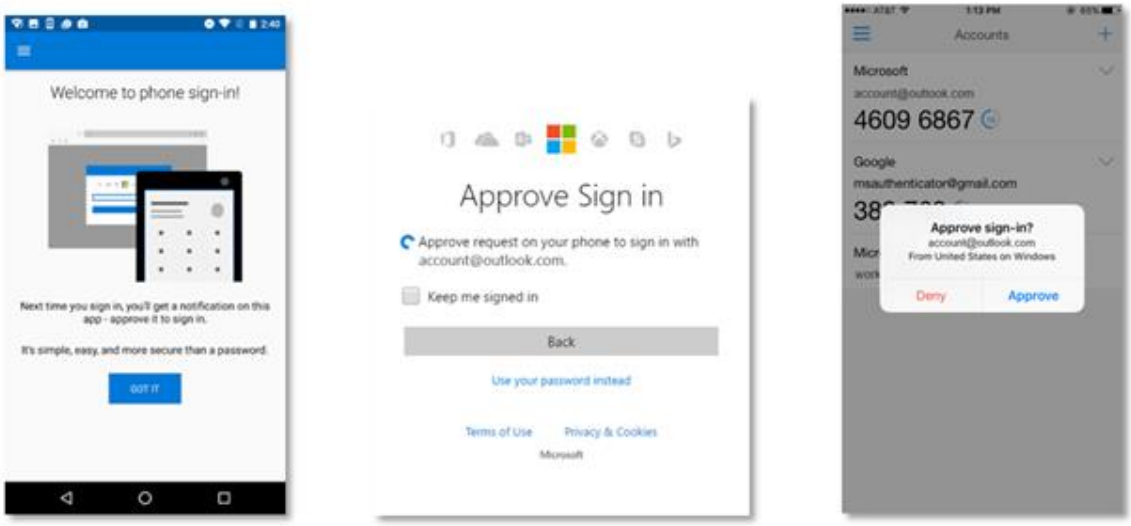
6.3 Vahva tunnistautuminen

Pelkkä käyttäjätunnus ja salasana ovat heikko tunnistautumisen tapa. (Valtion tieto- ja viestintätekniikkakeskus 2020) Vahvalla sähköisellä tunnistautumisella tarkoitetaan käyttäjän tunnistamista luotettavasti. Tunnistautumisessa tarvitaan jotain, jota vain käyttäjä tietää ja jotain joka käyttäjällä on (Virtualdcs 2015). Esimerkiksi verkkopankkiin kirjautuessa aiemmin vaadittiin käyttäjätunnus-salasana -parin lisäksi avainlukulista. Nykyisin pankkien mobiilisovellukset ovat korvanneet avainlukulistoja (Yle Uutiset 2019). Vahvasta tunnistautumisesta on säädetty laissa: laki vahvasta tunnistautumisesta ja sähköisistä luottamuspalveluista (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 2019).

Vahva sähköinen tunnistautuminen voidaan toteuttaa esimerkiksi Googlen ja Microsoftin tapaan palvelun kirjautumistiliin kytkettävällä mobiilisovelluksella, varmenteella tai toimikortilla. Joissain palveluissa kirjautuminen voidaan ohjata myös verkkopankin kautta.

Kaksivaiheiseen tunnistautumiseen voi käyttää myös useita eri sovelluksia. Esimerkiksi Google ja Microsoft ovat molemmat julkaisseet Apple Store ja Google Play kauppaan

ladattavaksi omat authenticator sovellukset. Sovellusten ajatuksena on, että käyttäjä lataa sovelluksen ja yhdistää sen etukäteen suojattavan palveluun käyttäjätiliin. Palveluun kirjautuessa järjestelmä kysyy käyttäjätunnuksen ja salasanan, sekä tämän jälkeen vaatii antamaan sovelluksessa näkyvän numerokoodin. Numerokoodi on vain hetken voimassa. (Microsoft 2017b.)



KUVA 6. Microsoft authenticator sovellus (Microsoft 2017a)

Kuvassa 6 on kuvattu esimerkinomaisesti Microsoft authenticator sovelluksen toimintaa loppukäyttäjän näkökulmasta. Esimerkissä käyttäjä kirjautuu järjestelmään, johon on kytketty authenticator sovellus. Kirjautumisen yhteydessä käyttäjä avaa sovelluksen, ja saa vahvistuspyynnön.

Kaksivaiheisen kirjautumisen ollessa käytössä, käyttäjä saa ilmoituksen poikkeavista kirjautumisista. Tämä ei lisää suoraan käyttäjän turvallisuutta, mutta mahdollistaa valvonnan ja antaa käyttäjälle mahdollisuuden vaihtaa salasanaansa ennen kuin ulkopuolinen taho ehtii tehdä haittaa tai päästä tietoihin käsiksi. Poikkeavista kirjautumisista tulee myös virheellisiä hälytyksiä, käyttäjän kirjautuessa ensimmäistä kertaa ennestään tuntemattomalta laitteelta. (Viestintävirasto 2020.)

6.4 Tietomurtojen vaikutukset

Varsinkin Office 365 -käyttäjätunnuksia urkitaan kalasteluviestejä käyttäen. Kalasteluviestissä voi olla linkki valheelliselle Microsoftin Office 365 -sivustolle, One Drive -tiedostolinkki tai muu mekanismi, jolla käyttäjätunnus ja salasana urkitaan rikollisten tietoon.

Kyberturvakeskuksella on ollut elokuusta 2018 saakka voimassa varoitus Office 365 -tunnusten kalastelusta. Uhkaa ja määriä arvioidessa on syytä huomata, että Kyberturvakeskus saa tiedot tapahtuneista tietomurroista tietoturvailmoitusten kautta, eikä kaikilla organisaatioilla ole ilmoitus velvollisuutta. (Kyberturvakeskus 2019.)

Tietomurtoja kohdistetaan tyypillisesti organisaation johtoryhmän jäseniin. Tietomurrolla hankittuja käyttäjätunnuksia on käytetty petoksien tekemiseen ja niiden yrityksiin. Tunnukset saatuaan hyökkääjä pääsee käyttäjän sähköpostiin ja One Drive -tiedostoihin. Monissa tapauksissa hyökkääjä asettaa sähköpostiin edelleen lähetyssääntöjä, sekä käyttää murrettua tiliä uusien kalasteluviestien edelleen lähetykseen. Suurista kalastelu- ja mainosviestimääristä voi päätyä sähköpostiylläpitäjien mustalle listalle, jolle aiheuttaminen voi johtaa ongelmiin sähköpostien perillemenon kanssa. Mikäli tietomurron seurauksena joudutaan uudelleen asentamaan kokonaisia tietojärjestelmiä, voi se aiheuttaa organisaatiolle mittavia kustannuksia ja häiriötä liiketoimintaan.

Salasanoja urkitaan tietoon teknisillä salakuuntelumetodeilla, kuten näppäintallenninohjelmistoilla, jotka tallentavat ja lähettävät kaikki käyttäjän näppäimen painallukset rikolliselle. Rikollinen voi myös manipuloida käyttäjää esiintymällä toisena tahona ja urkkimalla näin tarpeelliset tiedot. Rikolliset voivat myös hyödyntää tunnettuja tietoturva aukkoja. Myös erilaiset sanakirjaan ja väsytys hyökkäykset ovat tapa murtaa salasanoja. Näissä menetelmissä rikolliset arvaavat salasanaa uudelleen ja uudelleen listojen, taulujen ja sanakirjojen pohjalta. (Valtion tieto- ja viestintätekniikkakeskus 2020.)

Kyberturvakeskuksen arvion mukaan tietomurtojen takana voi olla teollisuusvakoilua ja järjestäytynyttä rikollisuutta taloudellisen hyödyn tavoittelemana. Yksityiseen henkilöön kohdistuvan tietomurron motiivina voi olla myös kiusanteko. (Kyberturvakeskus 2018)

Maaliskuussa 2018 rikolliset onnistuivat lisäämään kiristysohjelman Norjalaisen Norsk Hydro yrityksen tietojärjestelmiin. Hyökkäyksestä arvioidut kustannukset yritykselle, olivat 71 miljoonaa dollaria. (Microsoft 2019c.)

Mikäli epäillään tietomurron tapahtuneen, on syytä tehdä ilmoitus Kyberturvallisuuskeskukselle sekä poliisille rikosilmoitus. Tämän lisäksi tulee eristää murrettu järjestelmä muusta ympäristöstä, salasanat tulee vaihtaa ja lokitiedot tulee ottaa talteen jatkokäsittelyjä varten. Jos joudutaan palautumaan varmuuskopioista menneeseen tilanteeseen, on syytä varmistaa, että varmistukset ovat puhtaat ja ettei rikollinen ole tällöin ole ollut järjestelmässä. (Kyberturvakeskus 2020.)

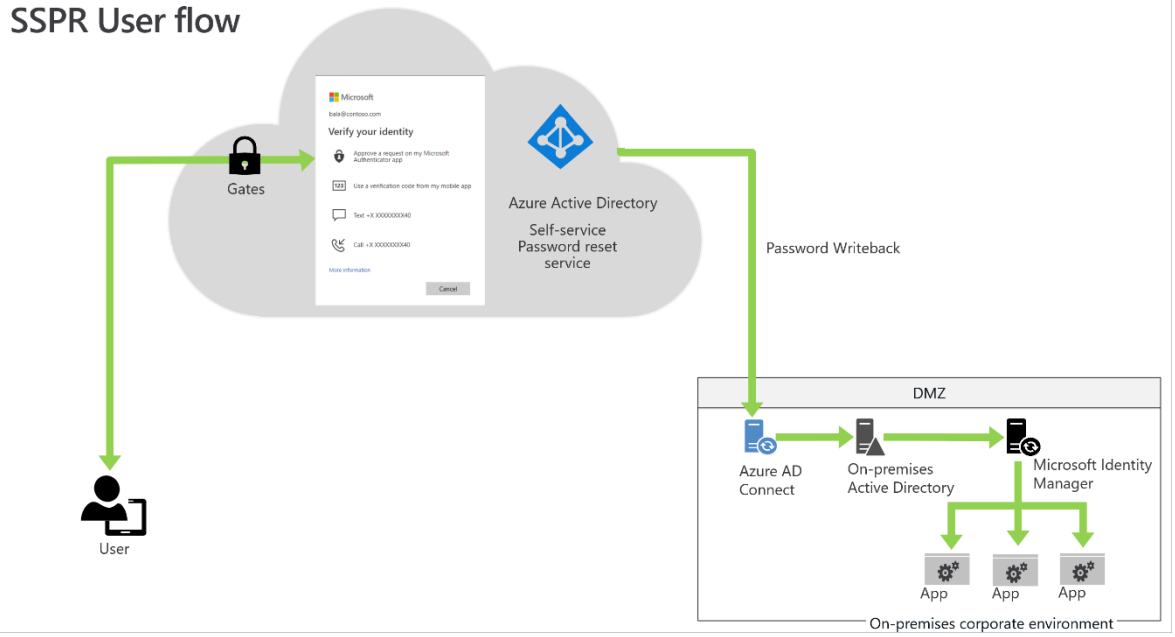
6.5 Eri toteutusvaihtoehtoja

Markkinoilla useita salasanan itsepalvelun tarjoavia ratkaisuja. Osa ratkaisuista asennetaan perinteisesti organisaation ympäristöön, ja organisaatio itse tai kumppani ylläpitää palvelimia. Alla on lyhyesti esitelty kaksi eri ratkaisua. Microsoftin Azure Active Directory self-service password reset on pilvipalvelu pohjainen ratkaisu, jossa asiakas maksaa Azure -lisenssien muodossa kuukausihintaa palvelusta. Toinen esiteltävä tuote on ManageEngine yrityksen ADself-service plus, joka edustaa perinteistä organisaation itse ylläpitämää ratkaisua.

6.5.1 Microsoft SSPR

Microsoftin ratkaisu salasanan vaihdon automatisoimiseksi, on Azure Active Directory self-service password reset työkalu, lyhennettynä SSPR (Microsoft 2020e). SSPR vaatii Azure Active Directory lisenssin ja lisensointi on käyttäjäkohtainen (Microsoft 2020a).

Kuvassa 7 on kuvattu Azure Active Directory self-service password reset työkalun toimintaperiaate. Käyttäjä kirjautuu Office 365 -tilillä Azure Active Directoryä vasten. Vaihtoehtoisen tunnistautumis menetelmän jälkeen Azure AD connect päivittää salasanan yrityksen toimialueen AD:lle.



KUVA 7. Microsoftin SSPR (Microsoft 2020e)

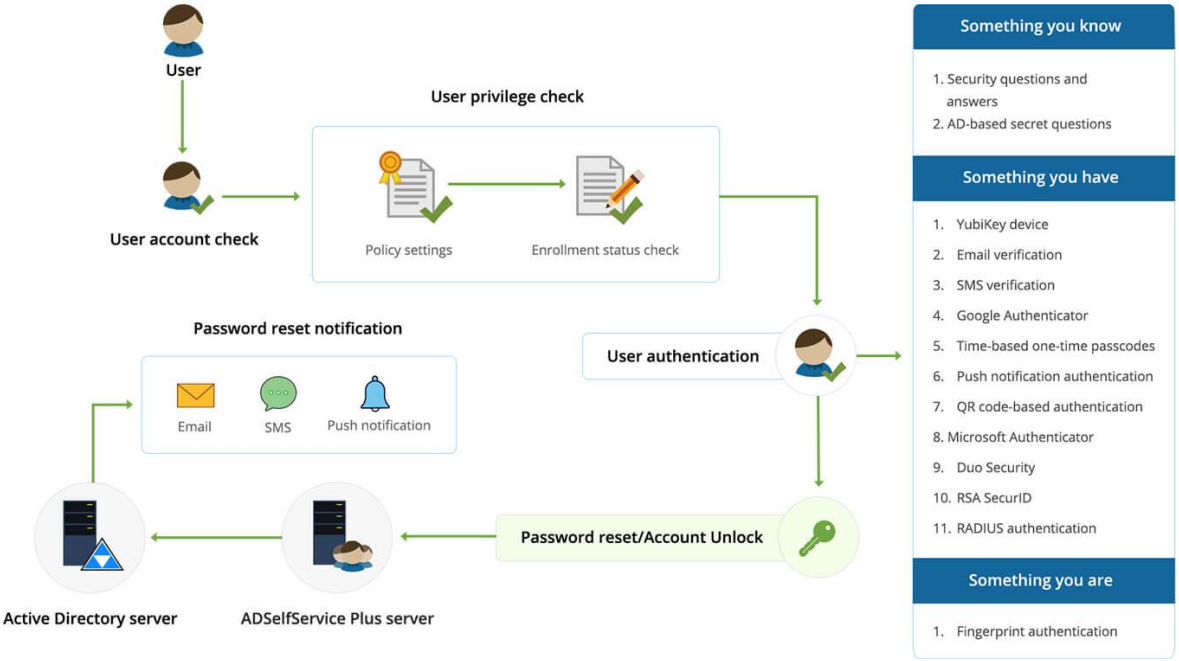
Kun SSPR on kytketty päälle, ensimmäisellä kerralla O365 -sivustolle kirjautuessa käyttäjää pyydetään valitsemaan ja täyttämään vaihtoehtoiset tunnestautumismekanismit.

Tarjolla on matkapuhelin- ja sähköpostivaihtoehdot, joista käyttäjä voi valita toisen tai molemmat. (Microsoft 2020b.)

6.5.2 ManageEngine ADSelfService plus

ManageEnginen ratkaisu salasanan itsepalveluun on password self-service tuote. Järjestelmä asennetaan organisaation hallitsemalle palvelimelle, josta on yhteydet AD toimialueen ohjauskoneelle. Kuvassa 8 on kuvattu ManageEnginen ratkaisun toimintaperiaate. Käyttäjä kirjautuu järjestelmään ja hänelle suoritetaan vahva tunnistautuminen. Tunnistautumisen jälkeen käyttäjä määrittelee uuden salasanan ja järjestelmä kirjoittaa sen organisaation toimialueen Active Directoryyn. (ManageEngine Self-service 2020b.)

SelfService plus lisensoidaan organisaation toimialueen käyttäjämäärän perustella. Hinta nousee käyttäjämäärän kasvaessa. (ManageEngine 2020a.)



KUVA 8. ManageEngine ADSelfService plus (ManageEngine 2020b)

7 LOPPUANALYYSI

7.1 Tulokset

Opinnäytetyössä tutkittiin identiteetinhallinnan sekä salasanan itsepalvelun tuomia höytyjä IT-palveluntuottajalle sekä asiakasorganisaatiolle. Opinnäytetyössä seurattiin tutkimuspäiväkirjan kautta kahden asiakkaan IDM-järjestelmän suunnittelua sekä salasanan itsepalvelun käyttöönottoa. Tutkimuspäiväkirjan lisäksi analysoitiin palveluntoimittajan työnohjausjärjestelmästä tuotettuja raportteja asiakkaan käyttötuen osalta. Työssä etsittiin vastauksia seuraaviin tutkimuskysymyksiin:

- Mitkä ovat identiteetinhallinnan hyödyt IT-palvelutoimittajan liiketoiminnalle?
- Mitkä ovat salasanan itsepalvelun hyödyt IT-palvelutoimittajan liiketoiminnalle?

IT-palvelutoimittajan työohjausjärjestelmään kirjattujen tapausten analysointi osoitti asiakkaan käyttötuella menevän runsaasti työaikaa manuaalisesti tehtäviin käyttäjätunnuksiin sekä salasanan vaihtoihin. Käyttäjätunnusten luomisen käytettyä työmäärää laskettiin vain asiakas a:n osalta, sillä asiakas b:llä oli työn aloitushetkellä käytössään identiteetinhallinnan järjestelmä, jolla käyttäjätunnusten luominen on automatisoitu. Salasanan vaihtojen osalta työmäärä laskettiin molemmilta asiakkailta.

Vuoden 2019 datan perusteella, asiakas a:n käyttäjätunnusten automaattinen luominen identiteetinhallinnan järjestelmällä säästäisi noin kolmekymmentä henkilötyöpäivää vuodessa. Asiakas a:n käyttäjien salasanan vaihtoihin palvelutoimittajan käyttötuella on mennyt työaikaa vuoden 2019 jälkimmäisellä puoliskolla noin 13 henkilötyöpäivää. Asiakas b:n käyttäjien salasanojen vaihtoihin palvelutoimittajan käyttötuella on mennyt työaikaa vuoden 2019 jälkimmäisellä puoliskolla 25 henkilötyöpäivää.

Asiakkaan näkökulmasta käyttäjätunnushakemuksen täyttämiseen arvioitiin menevän noin viisi minuuttia täytettyä lomaketta kohden. Vuoden 2019 aikana, asiakkaan esimiehet ovat käyttäneet yhteensä seitsemän ja puoli henkilötyöpäivää käyttäjätunnushakemusten täyttämiseen.

Salasanan vaihtojen viemää työaikaa asiakkaan näkökulmasta ei työssä tarkkaan arvioitu. Jos kuitenkin arvioidaan asiakkaalta kuluvan viisi minuuttia ongelman havaitsemisesta puhelimessa tapahtuneeseen salasanan vaihtoon, on asiakas a:n käyttäjillä kulunut vuoden 2019 jälkimmäisellä puoliskolla työaikaa reilut 13 henkilötyöpäivää salasanojen vaihtamiseen. Asiakas b:llä vastaava määrä olisi noin 25 henkilötyöpäivää.

Käyttäjätunnusten automatisointi identiteetinhallinnan järjestelmän avulla tuo IT-palvelutoimittajalle tuntuvan säästön manuaalisen työn vähentymisenä. Identiteetinhallinnan projektin kuoletusaika saadaan arvioitua selvittämällä manuaalisesti luotavien, muokattavien ja poistettavien käyttäjätunnusten määrät sekä niihin kuluvan työajan. Lopulliseen laskelmaan projektin kuoletusajasta vaikuttaa vahvasti myös asiakkaan ja palvelutoimittajan väliset sopimukset ja laskutusperusteet.

Identiteetinhallinta tuo käyttäjätunnusten hallintaan yhteneväisyyttä ja ajantasaisuutta. Kun sähköisiä identiteettejä ja niihin sidottuja käyttäjätunnuksia ylläpidetään automaattisesti lähdetiedon perusteella, ei asiat ole enää esimiehen muistamisen varassa. Kun esimerkiksi käyttäjän nimi, työnkuva, vastuuyksikkö tai työsuhteen kesto muuttuu, saa identiteetinhallinta siitä tiedon lähdejärjestelmästä, jonka jälkeen muuttunut tieto viedään eteenpäin integroituihin järjestelmiin. Näin tieto on aina ajantasainen kaikissa järjestelmissä. Identiteetinhallinnalla voidaan myös varmistaa, ettei ympäristössä ole aktiivisia käyttäjätunnuksia organisaation palveluksesta poistuneilla henkilöillä. Automaattinen poistoprosessi mahdollistaa myös tarkemman lisenssioptimoinnin Microsoft Office 365 -kaltaisiin kuukausimaksullisiin käyttäjäperusteisiin palveluihin.

Salasanan itsepalvelulla on mahdollista vähentää palvelutoimittajan käyttötuen työmäärää. Asiakkaan saamat taloudelliset säästöt riippuvat asiakkaan ja IT-palvelutoimittajan välisistä sopimuksista. Itsepalvelun käyttöönotossa haasteeksi tunnistettiin palvelun jalkauttaminen loppukäyttäjille. Mikäli palvelulla pyritään tuntuviin työmääränsäästöihin, suositeltavaa on sopia asiakkaan kanssa selkeästä linjasta, jossa käyttötuki ohjaa käyttäjiä tekemään salasanan vaihdot ensisijaisesti itsepalvelun kautta. Ennen kesälomakausia on hyvä lähettää käyttäjille muistutusviesti esimerkiksi tekstiviestillä, jolloin ohjeet jäävät talteen matkapuhelimeen.

7.2 Haasteet

Tutkimuspäiväkirjassa seuratuissa asiakasprojekteissa suurin haaste liittyi henkilöresursseihin. Projektin alkupuolella palveluntoimittajan toisen suuren asiakkaan projekti vei projektille varatut asiantuntijaresurssit. Asia tuli hieman viiveellä projektiryhmän tietoon, ja sitä koitettiin korjata korkeassa asemassa olevan johtajan kautta tuloksetta.

Palvelutoimittajan projektipäällikkö oli kuukauden pois. Hänelle saatiin välittömästi varahenkilö, joka suoriutui tehtävästä hyvin, mutta ei voinut käyttää projektille yhtä paljoa työaikaa kuin varsinainen projektipäällikkö.

Asiakas b:ltä projektiin resursoitu asiakkaan tietohallinnon edustaja oli poissa reilut kolme viikkoa, joka viivästytti uuden IDM-järjestelmän käyttöönottoa. Yhteyshenkilön palattua tuli koronaepidemia, ja uuden IDM-järjestelmän käyttöönottoa lykättiin myöhemmäksi asiakasorganisaation keskittyessä tukemaan omaa liiketoimintaansa.

Palveluntoimittajan projektiin resursoima IDM-arkkitehti vaihtui kesken projektin, uuden arkkitehdin ollessa huomattavasti kokeneempi, kuin projektiin alun perin resursoidut. Asiakas a:n osalta suunnitelma saatetaan joutua tekemään kokonaan uudelleen siinä havaittujen puutteiden vuoksi. Puutteet tunnistettiin, kun uusi arkkitehti alkoi tarkastelemaan suunnitelmaa. Asiakas b:n osalta suunnitelma pohjautui pitkälti olemassa olevaan ympäristöön. Suunnitelmaan ja toteutukseen saatetaan tehdä vielä muutos tuplatunnusten estävän toimintalogiikan lisäämisen osalta.

Salasanan itsepalvelun osalta käyttöönottojen kanssa on kestänyt pitkään. Viivästys johtuu asiakkaan ja palveluntoimittajan välisistä keskusteluista liittyen palvelun sopimuksellisiin asioihin.

7.3 Jatkosuunnitelma

Molempien asiakkaiden osalta identiteetinhallinnan järjestelmien käyttöönotto pitää suunnitella. Käyttöönotto vaatii käyttöohjeiden viemisen käyttäjien saataville sekä näkyvän tiedottamisen uusiin toimintamenetelmiin. Esimiesten tulee ymmärtää, miten käyttäjätunnusprosessi menee jatkossa.

Salasanan vaihdon itsepalvelun osalta täytyy seurata ja arvioida jalkauttamisen onnistumista. Toteutuksessa käyttäjien täytyy ensimmäisellä kerralla rekisteröidä itselleen pin-koodi. Jos vertaamme pin-koodin asettaneiden määrää kokonaiskäyttäjämäärään, voimme laskennallisesti arvioida toiminnallisuuden piirissä olevien määrää. Viimeistään lomakauden lähestyessä on suositeltavaa lähettää uusi muistutusviesti käyttäjille, sillä tutkitusti suurimmat salasanojen vaihtopiikit ovat lomalta palatessa.

Kun identiteetinhallinta on saatu otettua käyttöön ja käyttäjät alkavat omaksua uusia toimintamalleja, olisi hyvä alkaa tutkimaan mahdollisuutta itsepalvelun toiminnallisuuksien laajentamiseen. Lisäksi itsepalvelun toiminnallisuuksia olisi hyvä kerätä yhteen portaaliin, esimerkiksi linkittämällä. Identiteetinhallintajärjestelmä antaa mahdollisuuden automatisoida sovellusten, sovellusoikeuksien ja -lisenssien hyväksyntää ja asentamista.

Asiakkaiden kanssa voisi suorittaa myös pohdintaa identiteetinhallinnan laajentamista pääsynhallinnaksi, eli siirtymä IDM -ratkaisusta IAM -ratkaisuun. Asiakkaalle voitaisiin

tehdä työnohjausjärjestelmän tapausten ja käyttöoikeuspyyntöjen pohjalta analyysiä säästyvästä työmäärästä esimiesten ja palvelutoimittajan osalta. Lisäksi voitaisiin analysoida ratkaisun tietoturvavaikutuksia kyseisissä toimintaympäristöissä.

Identiteetinhallinnan tai viimeistään pääsynhallinnan käyttöönoton jälkeen kannattaisi myös pohtia auditoinnin tuomista ratkaisuun. Tällöin voitaisiin jälkikäteen auditoida olleita identiteettejä sekä käyttöoikeuksia eri järjestelmissä.

8 YHTEENVETO

Opinnäytetyössä tutkittiin identiteetinhallinnan ja salasanan itsepalvelu toiminnallisuuden käyttöönoton hyötyjä ulkoistetussa it-ympäristössä, sekä käynnistettiin kahdelle asiakkaalle järjestelmien suunnittelu- ja käyttöönottoprojektit. Opinnäytetyössä käytettiin hyödyksi tutkimuspäiväkirjamenetelmää sekä analysoitiin palveluntoimittajan työnohjausjärjestelmän dataa.

Palvelutoimittajan työnohjausjärjestelmän raporttien pohjalta tehdyssä analyysissä löydettiin mahdollisuuksia huomattaviin työajan säästöihin käyttäjien salasanan vaihtojen sekä manuaalisesti tehtävien käyttäjätunnusten osalta. Lisäksi tunnistettiin tietoturvaa edistäviä hyötyjä identiteetinhallinnan sekä salasanan itsepalvelun osalta.

Identiteetinhallinnan osalta saatiin molemmille asiakkaille suunnittelu vietyä seurantajaksojen aikana loppuun. Toiselle asiakkaista toteutus saatiin testattua käyttöönottovalmiiksi, ja toiselle järjestelmän kehitys saatiin alkamaan seurantajaksojen loputtua. Salasanan itsepalvelu saatiin otettua kokonaan käyttöön toiselle asiakkaista, toisen asiakkaan kohdalla odotetaan vielä asiakkaan ja palvelutoimittajan sopimuksellisten asioiden valmistumista teknisten asioiden ollessa valmiina.

Asiakasprojekteissa suurimmat haasteet olivat realisoituneet henkilöriskit. Projektin aikana palvelutoimittajan projektipäällikkö, sekä asiakas b:n edustaja olivat pitkään poissa. Lisäksi molempien asiakasprojektien IDM-arkkitehti vaihtui kesken projektin.

Työnohjausjärjestelmän datan pohjalta tehty analyysi osoitti, että käyttötuen manuaalisesti suorittamat salasanan vaihdot sekä käyttäjätunnusten luonti vievät paljon käyttötuen työaikaa. Salasanan vaihtojen vieminen itsepalvelusta loppukäyttäjien tehtäväksi, sekä automatisoitu identiteetinhallinta mahdollistavat merkittävät työmäärä säästöt. Analyysissa jouduttiin tekemään käytetyn työajan osalta oletuksia työnohjausjärjestelmän tapausten heikon kirjauslaadun takia. Työnohjausjärjestelmän tapausten kirjaamisen laatuun on puututtu käyttötuen esimiehen toimesta, ja korjaavia toimenpiteitä on käynnistetty lisäkoulutuksen ja ohjeistuksen muodossa.

Salasanan vaihdon itsepalvelutoiminnallisuuden suunnittelu ja käyttöönotto ovat suoraviivainen prosessi, mutta käytännön jalkauttaminen loppukäyttäjille asti on syytä suunnitella huolella ja tiedotus hoitaa näkyvästi.

Identiteetinhallinnan suunnittelussa tarvitaan asiakkaan käytäntöjen ja järjestelmien asiantuntijuutta. Projektia suunnitellessa onkin syytä varata riittävästi aikaa ja resursseja identiteettilähteen perusteiden läpikäymiseen, koska ne toimivat pohjana koko ratkaisulle.

Sähköinen identiteetinhallinta sekä salasanan vaihdon itsepalvelumalliin ohjaaminen luovat palvelutoimittajalle sekä asiakkaalle hyvän pohjan jatkokehittää itsepalvelua.

LÄHTEET

Bertino, Elisa & Takahashi, Kenji. 2010. Identity Management: Concepts, Technologies, and Systems. Boston: Artech House

Evolveum. 2020. Identity Management for Dummies. [viitattu 3.5.2020]. Saatavissa: https://docs.evolveum.com/iam/identity-management-for-dummies/

Information Technology Services Office of The Hong Kong Polytechnic University. 2019. Identity and Access Management. [viitattu 3.5.2020]. Saatavissa: https://www.polyu.edu.hk/ags/Newsletter/news0911/IAM_details.html

Kuntaliitto. 2013. Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri [viitattu: 3.5.2020]. Saatavissa: https://www.kuntaliitto.fi/sites/default/files/media/file/Kuntasektorin%20k%C3%A4ytt%C3%B6valtuushallinnan%20viitearkkitehtuuri.pdf

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617.

Lastpass. 2018. How to make a strong master password. [viitattu: 3.5.2020]. Saatavissa: https://blog.lastpass.com/2015/07/how-to-make-a-strong-master-password.html/

Lastpass. 2020. Enable the YubiKey Multi-Factor Authentication for your LastPass Account on Desktop, Android and iOS. [viitattu: 3.5.2020]. Saatavissa: https://www.lastpass.com/yubico

Liikenne- ja viestintäministeriö Kyberturvakeskus. 2018. Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota! [viitattu: 3.5.2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Liikenne- ja viestintäministeriö Kyberturvakeskus. 2019. Aktiivista kalastelua ja tietomurtoja. [viitattu: 3.5.2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/aktiivista-kalastelua-ja-tietomurtoja

Liikenne- ja viestintäministeriö Kyberturvakeskus. 2020. Näin suojaudut tietomurrolta. [viitattu: 3.5.2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nain-suojaudut-tietomurroilta

Linden, Mikael. 2015. Tampereen teknillinen yliopisto. Tietotekniikan laboratorio. Raportti 6. identiteetin- ja pääsynhallinta. [viitattu: 3.5.2020]. Saatavissa: https://tutcris.tut.fi/portal/files/3087873/linden_identiteetin_ja_paasyn-hallinta.pdf

ManageEngine. 2020a. Pricing details. [viitattu: 3.5.2020]. Saatavissa: https://www.manageengine.com/products/self-service-password/pricing-details.html

ManageEngine. 2020b. Self-service password reset software for Active Directory and cloud applications. [viitattu: 3.5.2020]. Saatavissa: https://www.manageengine.com/products/self-service-password/self-service-password-reset.html

Microsoft. 2017a. No password, phone sign in for Microsoft accounts! [viitattu 3.5.2020]. Saatavissa: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/no-password-phone-sign-in-for-microsoft-accounts/ba-p/245254#

Microsoft. 2017b. Sign in to your work or school account using your two-factor verification method. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/fi-fi/azure/active-directory/user-help/multi-factor-authentication-end-user-signin

Microsoft. 2019a. Connect to your directories. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/fi-fi/microsoft-identity-manager/supported-management-agents

Microsoft. 2019b. Download and install the Microsoft Authenticator app. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/fi-fi/azure/active-directory/user-help/user-help-auth-app-download-install

Microsoft. 2019c. Hackers hit Norsk Hydro with ransomware. The company responded with transparency. [viitattu 3.5.2020]. Saatavissa: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Microsoft. 2019d. Microsoft Identity Manager 2016 licensing and downloads. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-licensing

Microsoft. 2019e. Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/fi-fi/archive/blogs/secguide/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903

Microsoft. 2019f. What is Azure AD Identity Governance? [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview

Microsoft. 2020a. Azure Active Directory Pricing. [viitattu: 3.5.2020]. Saatavissa: https://azure.microsoft.com/en-us/pricing/details/active-directory/

Microsoft. 2020b. Let users reset their own passwords. [viitattu: 3.5.2020]. Saatavissa: https://docs.microsoft.com/fi-fi/microsoft-365/admin/add-users/let-users-reset-passwords?view=o365-worldwide

Microsoft. 2020c. Microsoft 365 and Office 365 platform service description. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-platform-service-description

Microsoft. 2020d. Password policy recommendations. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

Microsoft. 2020e. Plan an Azure Active Directory self-service password reset deployment. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

Microsoft. 2020f. Set the password expiration policy for your organization. [viitattu 3.5.2020]. Saatavissa: https://docs.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide

Microsoft. 2020g. Tuen päättyminen Windows Server 2008:lle ja Windows Server 2008 R2:lle. [viitattu 3.5.2020]. Saatavissa: https://support.microsoft.com/fi-fi/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2

Netiq. 2020. Understanding the Components of CPRS. [viitattu 3.5.2020]. Saatavissa: https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/ne-tiq-identity-manager-cprs-components.html

Tietosuojalaki 5.12.2018/1050.

Tietosuojavaltuutetun toimisto. 2020a. Mikä on henkilötieto? [viitattu 3.5.2020]. Saatavissa: https://tietosuoja.fi/mika-on-henkilotieto

Tietosuojavaltuutetun toimisto. 2020b. Seloste käsittelytoimista. [viitattu 3.5.2020]. Saatavissa: https://tietosuoja.fi/seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2020c. Tietosuojaperiaatteet [viitattu 3.5.2020]. Saatavissa: https://tietosuoja.fi/tietosuojaperiaatteet

Tietosuojavaltuutetun toimisto. 2020d. Tunne oikeutesi. [viitattu 3.5.2020]. Saatavissa: https://tietosuoja.fi/tunne-oikeutesi

Valtion tieto- ja viestintätekniikkakeskus. 2020. Millainen on hyvä salasana – sekä muuta tunnusten ja salasanojen hallinnasta. [viitattu 3.5.2020]. Saatavissa: https://valtioneuvosto.fi/documents/10623/5390546/JHDTTV5/79764e6d-84e1-497b-b3d6-5ad57fe49e8b/JHDTTV5.pdf

Valtionvarainministeriö. 2016. Henkilöstön ja johdon tietoturvabarometri [viitattu 3.5.2020]. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79060/VAHTI3_henkiloston_ja_johdon_tietoturvabarometri.pdf?sequence=1&isAllowed=y

Viestintävirasto. 2020. salasanat haltuun. [viitattu 3.5.2020]. Saatavissa: https://kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Virtualdcs. 2015. Should two factor authentication be the norm? [viitattu 3.5.2020]. Saatavissa: http://www.virtualdcs.co.uk/blog/should-two-factor-authentication-be-the-norm

Yle Uutiset. 2014. Lomalla unohtuneista salasanoista tulee jättilasku työnantajalle – jopa 200 000 euroa vuodessa. [viitattu 3.5.2020]. Saatavissa: https://yle.fi/uutiset/3-7362012

Yle Uutiset. 2019. Verkkopankkiin ei pääse pian pelkällä pahvilapulla – turvallisuus kasvaa, mutta perinteinen tunnuslukulista ei vielä katoa. [viitattu 3.5.2020]. Saatavissa: https://yle.fi/uutiset/3-10897752

Wikipedia. 2020a. Identity management. [viitattu 3.5.2020]. Saatavissa: https://en.wikipedia.org/wiki/Identity_management

Wikipedia. 2020b. Novell [viitattu 3.5.2020]. Saatavissa: https://en.wikipedia.org/wiki/Novell