Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VALTTERI LAMMINEN

Identiteetin- ja pääsynhallintajärjestelmän käyttöönotto

TIETO- JA VIESTINTÄTEKNIIKAN KOULUTUSOHJELMA
2020

Tekijä Lamminen, Valtteri	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä Joulukuu 2020
	Sivumäärä: 28	Julkaisun kieli Suomi
Julkaisun nimi **Identiteetin- ja pääsynhallintajärjestelmän käyttöönotto**		
Tutkinto-ohjelma Tieto- ja viestintätekniikan koulutusohjelma		
Tiivistelmä Tässä opinnäytetyössä tutkittiin pääsynhallintaa, sen työkaluja, muotoja ja siihen vaikuttavia tekijöitä. Työssä tutustuttiin keskitettyyn identiteetin- ja pääsynhallinnan järjestelmään, mitä sen käyttöönotto vaatii ja mitä hyötyjä sellainen tuo mukanaan. Työssä käytiin läpi myös erilaisia tietoturvaan liittyviä uhkia, ja miten näitä voidaan ehkäistä hyvin toteutetulla pääsynhallinnalla. Tutkimuksessa käytettiin mallina Yritys X:n nykyistä pääsynhallintamallia, ja tutkittiin, miten yrityksessä voitaisiin hyödyntää keskitettyä pääsynhallintajärjestelmää ja millaisia vaikutuksia sillä olisi eri osa-alueisiin.		
Asiasanat pääsynvalvonta, tietoturva, tietojärjestelmät		

Author
Lamminen, Valtteri

Type of Publication
Bachelor's thesis

Date
December 2020

Number of pages
28

Language of publication:
Finnish

Title of publication
Implementation of an Identity and Access Management System

Degree program
Degree Program in Information and Communication Technologies

Abstract

This thesis included studying access management, the tools used in it, the different forms it has and things that factor into it. The thesis focused on finding out what it takes to implement a centralized identity and access management system and what benefits it gives.

The thesis also studied different threats to information security and how they can be prevented using well-executed access management.

Yritys X's current manual access management was used as the base model in the study, and it was explored how the company could benefit from a centralized access management system and which areas it would affect.

Key words
access control, information security, data systems

SISÄLLYS

1 JOHDANTO

Erinäisten tietojärjestelmien käyttö yritysmaailmassa on kasvanut huimaa vauhtia viime vuosikymmeninä. Jatkuvasti kasvavassa automatisoinnin ja sähköistymisen maailmassa, taakse on jäämässä yhä useampi manuaalinen työ. Kun yhä useammat yritykset siirtävät datansa sähköisiin tietokantoihin, ja ennen paperisten lomakkeiden kautta tehty työ siirtyy hoidettavaksi tietojärjestelmien ja ohjelmien kautta, on tärkeää pitää huolta siitä, että oikeat käyttäjät pääsevät käsiksi tarvitsemiinsa järjestelmiin vaivattomasti. Kyseiset järjestelmät ovat pidettävä kuitenkin turvassa luvattomalta käytöltä, niin yrityksen sisä- kuin ulkopuolelta.

Pääsynhallinnalla tarkoitetaan juuri tätä käyttäjien oikeuksien hallintaa eri järjestelmiin. Tässä opinnäytetyössä perehdytään erilaisiin pääsynhallinnan muotoihin, työkaluihin ja vaatimuksiin, sekä yrityksen tietoturvaan ja pääsynhallinnan rooliin tietoturvallisuuden toteutumisessa.

Käytännön osiossa tutkitaan Yritys X:n nykyistä tietojärjestelmien käyttöoikeuksien hallinnointiprosessia yrityksen IT-palvelupisteen näkökulmasta, sekä tehdään vertailua teoreettiseen automatisoidun IAM-palvelun käyttöönottoon. Vertailussa tutkitaan vaikutuksia muun muassa oikeuksien hallinnoitsijoiden työkuormiin ja työnkuvaan, sekä käyttäjiin ja tietoturvallisuuteen kohdistuviin muutoksiin.

2 PÄÄSYNHALLINTA

Tietojärjestelmien pääsynhallinnalla pyritään varmistamaan tietojärjestelmän tarkoituksellinen käytettävyys. Pääsynhallinnalla huolehditaan, että käyttäjillä on pääsy työssä tarvittaviin järjestelmiin ja työtehtäviensä mukaisin oikeuksin. Kuten fyysisen maailman liiketiloissa ihmisten kulkua rajataan lukituin ovin, joihin vain kyseiseen tilaan pääsyn tarvitsevilla on avain, niin myös IT-ympäristössä tulee rajata järjestelmiin pääsyä niin, ettei sinne asiaankuulumattomilla käyttäjillä ole pääsyä. Esimerkiksi HR-henkilökunnan ja esimiehen voi olla tarve päästä näkemään työntekijöidensä tuntikirjauksia, mutta työntekijän kollegoilla ei pidä olla pääsyä näkemään näitä tietoja. Samoin kuin yrityksen ostajien tulee päästä tekemään tilauksia yritykselle, niin ei esimerkiksi yrityksessä toimivan suunnittelijan tule pystyä näitä toimenpiteitä tekemään.

Pääsynhallinnassa on hyvä pitää mielessä tietoturvallisuuteen kuuluva CIA-malli, joka tässä kontekstissa tulee englannin kielen sanoista: Confidentiality (luottamuksellisuus), Integrity (eheys) ja Availability (saatavuus). Luottamuksellisuudella tarkoitetaan, että järjestelmään tai dataan pääsee käsiksi vain siihen valtuutetut käyttäjät. Luottamuksellisuutta pidetään yllä esimerkiksi järjestelmäkohtaisella käyttäjätunnuksella ja salasanalla, ja sitä voidaan vahvistaa esimerkiksi kaksivaiheisella tunnistautumisella. Eheys tarkoittaa datan todenmukaisuutta ja virheettömyyttä. Pitämällä huolen, että vain tarkoituksenmukaiset käyttäjät pääsevät käsittelemään ja muokkaamaan järjestelmässä olevia tietoja, varmistetaan että tiedot pysyvät oikeanlaisina. Eheyden säilyminen voidaan taata varmuuskopioimalla dataa sopivin väliajoin ja estämällä valtuuttamattomilta käyttäjiltä muokkausoikeudet dataan. Saatavuudella tarkoitetaan, että käyttäjillä on mahdollista päästä dataan käsiksi silloin kun heillä on tarve. Ylläpitämällä tietojärjestelmien toimivuutta ja varautumalla vikatilanteisiin saadaan pidettyä saatavuus korkealla. Saatavuutta helpottaa myös yritysverkossa olevien järjestelmien mahdollistaminen käytettäväksi VPN-yhteyden kautta, jolloin käyttäjät pääsevät dataan käsiksi vaikkei käyttäjä fyysisesti olisi yrityksen toimitilassa. Kaikkiin CIA-mallin ominaisuuksiin liittyy omat riskinsä, joita varten yrityksen tulee varautua mahdollisten hyökkäysten estämiseksi. Liiallinen keskittyminen vain yhteen osa-alueeseen voi heikentää toista osa-aluetta. Esimerkiksi liian tiukka luottamuksellisuuden

tarkkailu voi pienentää saatavuutta, mutta liiallinen saatavuus voi heikentää tiedon eheyttä. (Fruhlinger, 2020a)

Kuva 1. CIA-mallin osa-alueet tasapainottavat yrityksen tietoturvaa (Tyson, 2019)

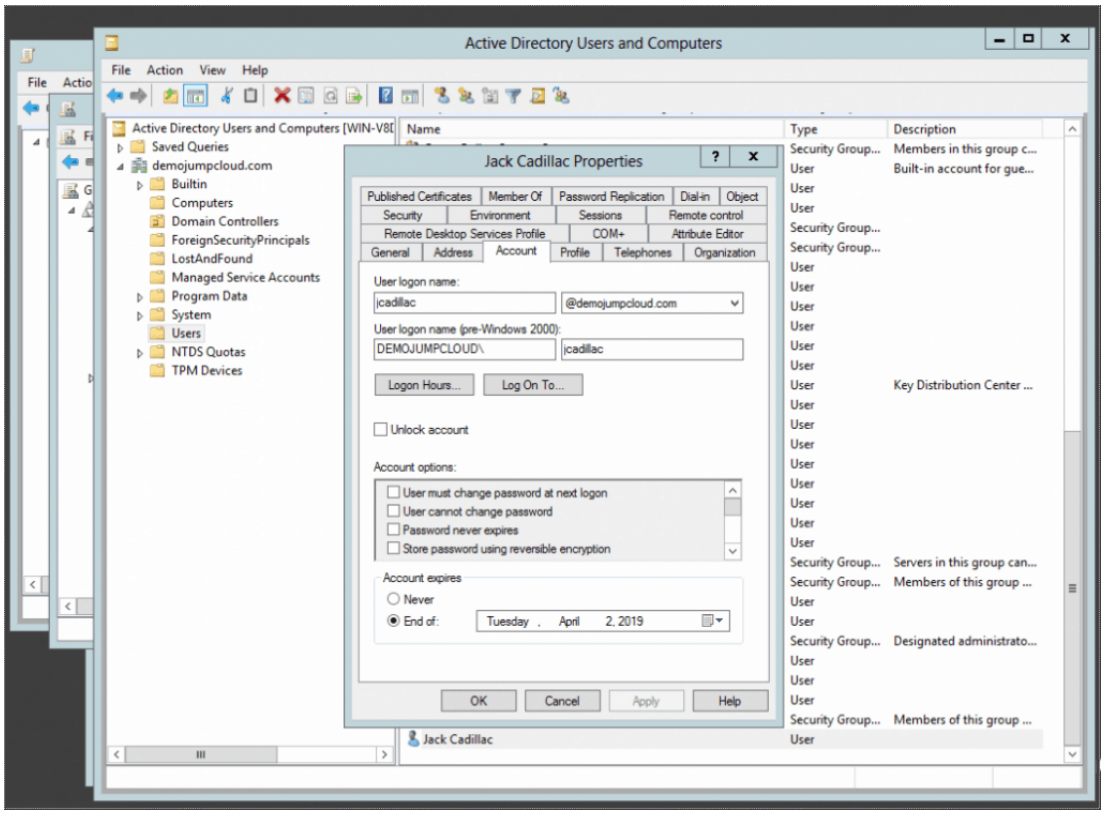
2.1 Pääsynhallinnan työkalut

Pääsyä tietojärjestelmiin voidaan hallinnoida monien työkalujen kautta. Tietojärjestelmä saattaa itsessään sisältää hallintatyökalut järjestelmään pääsyyn, jolloin käyttäjälle pitää luoda tunnus suoraan järjestelmän kautta, tai järjestelmän hyödyntämän tietokannan kautta. Tietojärjestelmiä voidaan myös integroida toimivaksi muiden järjestelmien tunnusten kautta, jolloin käyttäjä voi kirjautua samalla tunnuksella useampaan järjestelmään.

Yksi yritysmaailman tärkeimmistä ja käytetyimmistä työkaluista käyttäjäoikeuksien hallintaan on Microsoftin kehittämä Active Directory (AD) eli aktiivihakemisto. Active Directory on Microsoft Windows-palvelimella toimiva hakemisto, jonka kautta voidaan ylläpitää yritysverkon käyttäjätunnuksia, tietokoneita, ryhmiä sekä näihin

liittyviä oikeuksia. Active Directoryyn voidaan luoda yksi tai useampi Domain eli toimialue, ja näiden alle voidaan luoda useampia Organizational Uniteja (OU) eli organisaatioyksiköitä, joiden myötä eri osa-alueiden hallinnointi helpottuu. Näille Domaineille ja OU:ille voidaan asettaa omia periytyviä sääntöjä ja oikeuksia Group Policyiden kautta, jolloin kaikkiin sinne kuuluviin objekteihin kohdistuu samat säännöt. Active Directoryn käyttäjille voidaan asettaa järjestelmänvalvojan toimesta salasanavaatimuksia, jotka määrittävät salasanan pituus-, monimutkaisuus- ja vaihtovälivaatimukset. Näin saadaan yrityksen vaatimaa tietoturvatasoa pidettyä yllä. (Rouse, 2020a)

Active Directory sisältää myös kahdenlaisia päätyyppejä ryhmille, Security Groupeja ja Distribution Groupeja, eli käyttöoikeus- ja jakeluryhmiä. Security Groupeja käytetään pääosin tuomaan ryhmään kuuluville käyttäjille oikeuksia haluttuun resurssiin yritysverkon sisällä, kun taas jakeluryhmiä käytetään pääosin sähköpostien jakeluun halutulle käyttäjäjoukolle, joskin myös Security Groupeja voidaan käyttää tähän käyttötarkoitukseen. Ryhmien käyttötarkoitus on tärkeää olla selkeä ja yksiselitteinen, jotta käyttäjän lisääminen ryhmään ei tuo oikeutta tahtomatta jonnekin, minne käyttäjän ei pitäisi päästä. Samalle käyttöoikeusryhmälle oikeuden lisääminen useaan resurssiin vähentää tarvittavien ryhmien määrää, mutta ajan myötä ryhmän kaikki käyttötarkoitukset eivät välttämättä ole tiedossa, jos niitä ei ole dokumentoitu tarpeeksi tarkkaan. (Microsoft, 2020)



Kuva 2. Esimerkkikuva Active Directoryn käyttäjänhallinta näkymästä (Network Encyclopedia, 2020)

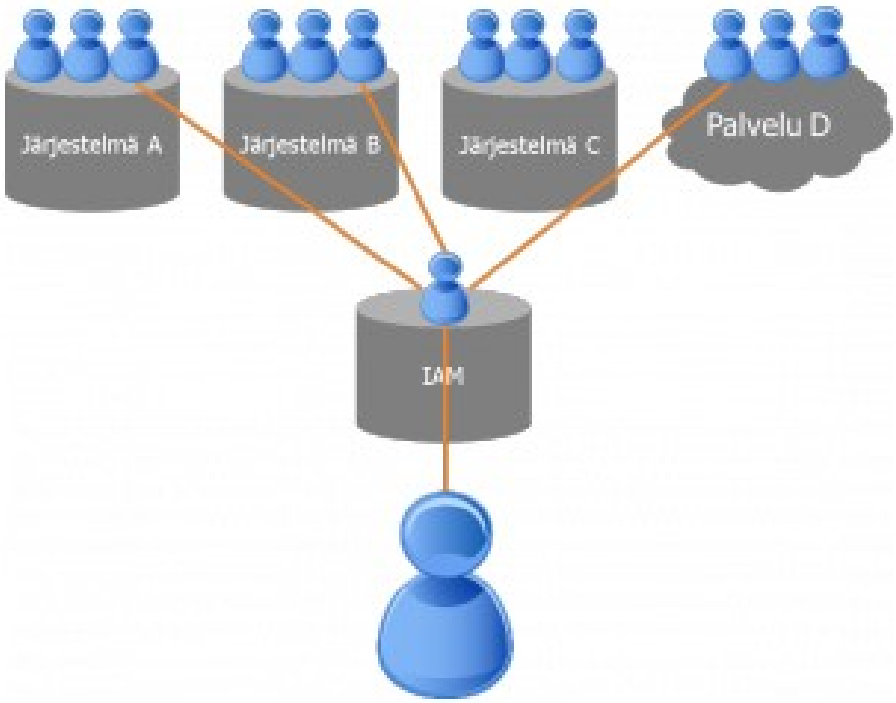
2.2 Käyttäjäoikeuksien ylläpidon muotoja

Yrityksen koosta ja käytettävien tietojärjestelmien määrästä riippuen, pääsynhallinta voidaan toteuttaa eri tavoin. Pienemmissä yrityksissä ei välttämättä ole tarvetta automatisoida käyttäjien pääsynhallintaa järjestelmiin, vaan pääsynhallinta voidaan toteuttaa manuaalisen prosessin kautta esimerkiksi yrityksen oman tai ulkoistetun IT-organisaation ylläpitämänä. Jos yrityksellä ei ole tarvetta omalle talonsisäiselle IT-organisaatiolle, voidaan harkita IT as a Service (ITaaS)-toimintamallia, jolloin yritys ostaa palveluntarjoajalta vain tarvitsemansa palvelut, eikä yrityksen tarvitse palkata omaa IT-organisaatiota huolehtimaan IT-infrastruktuurista. Yrityksen on myös mahdollista ulkoistaa vain osa IT-organisaation tehtävistä, jolloin vastuut eri osa-alueista jakautuu yrityksen ja palveluntarjoajan IT:n välille. (Raza, 2020)

2.3 IAM

Suurempiin yrityksiin siirryttäessä ja erilaisten työtehtävien ja käytettävien tietojärjestelmien määrän kasvaessa tulee roolipohjainen, identiteettiin kohdistuva pääsynhallinta entistä tärkeämmäksi. Identity and Access Management, eli lyhyemmin IAM, määrittää käyttäjälle henkilökohtaisen digitaalisen identiteettiprofiilin, jolle määritetään työtehtävien vaatimia rooleja, joiden kautta pääsyä eri järjestelmiin hallitaan.

Ideaalitilanteessa yhdellä tosielämän henkilöllä on IAM-järjestelmässä oleva yksi digitaalinen identiteetti. IAM-järjestelmä yhdistää siis käyttäjän identiteetin muissa järjestelmissä toimiviin käyttäjätunnuksiin. Tällöin pääsynhallintaa ei tarvitse ylläpitää monien eri järjestelmien kautta erikseen, vaan kaikki tapahtuu saman järjestelmän alta. Yhden käyttäjän roolit ja oikeudet ovat helposti seurattavissa tämän identiteetin kautta, jolloin riskit liiallisiin oikeuksiin käyttäjän kohdalla pienenevät. Käyttäjien liialliset oikeudet saattavat aiheuttaa yritykselle tietoturvauhkia sekä tarkoituksellisten pahantekijöiden, että varomattomien työntekijöiden kautta. (Martin & Waters, 2018)



Kuva 3. IAM hallitsee identiteetin pääsyä järjestelmiin. (Niemi, 2020)

IAM-järjestelmän rooleihin voidaan määritellä tarkalleen mitä oikeuksia ja sääntöjä rooli tuo mukanaan, jolloin haluttuun tietojärjestelmään ei tarvitse

järjestelmänvalvojan manuaalisesti luoda käyttäjätunnusta ja määrittää millaiset oikeudet käyttäjälle sinne myönnetään, vaan nämä tapahtuvat automaattisesti IAM-järjestelmän toteuttamana. Rooleihin voidaan erikseen tarkentaa, tapahtuuko järjestelmiin pääsy esimerkiksi Single Sign-On (SSO) menetelmällä vai monivaiheisella tunnistautumisella. SSO-kirjautuminen tarkoittaa, että käyttäjän tunnistauduttua esimerkiksi työasemalle tai verkkosivulle, pääsee hän käyttämään SSO-kirjautumista hyödyntäviä järjestelmiä ilman uutta tunnistautumista. Jotkin yritysten järjestelmistä saattavat pitää sisällään arkaluontoisempaa tietoa, jolloin halutaan viedä tunnistautumisen turvallisuus pidemmälle monivaiheisen tunnistautumisen muodossa. Monivaiheinen tunnistautuminen saattaa erillisen käyttäjätunnuksen ja salasanan lisäksi vaatia esimerkiksi pankkitunnuksilla tai tekstiviestitunnisteella tunnistautumisen. Yhdellä käyttäjällä voi samassa järjestelmässä olla useampia rooleja, jotka vaativat eritasoisen tunnistautumisen, esimerkiksi järjestelmänvalvojaroolin käyttö järjestelmässä saatetaan haluta viedä erillisen kirjautumisen taakse. Eri roolien suunnittelu ja muodostaminen IAM-järjestelmään on tärkeätä tapahtua yrityksen eri organisaatioiden yhteistyönä, jotta roolien kaikki vaaditut ominaisuudet ovat halutunlaiset, eivätkä sisällä ei-toivottuja ominaisuuksia. Roolin lisääminen käyttäjälle voidaan linkittää esimerkiksi yrityksen HR-järjestelmässä olevaan tietoon käyttäjän työtehtävistä ja tarvituista rooleista, jolloin samassa työtehtävässä työskentelevät käyttäjät saavat samanlaiset oikeudet. (Rouse, 2020b)

Kuva 4. IAM-palvelun komponentteja. (Rouse, 2020c)

2.3.1 Pilvihallinta vai On-Premise

On-Premise-toimintamallissa, yrityksen IT-infrastruktuuri sijaitsee yrityksen omissa tiloissa. Palvelimet, yrityksen käyttämät järjestelmät ja laitteet ovat yrityksen vastuulla ja ylläpidettävänä. Jos yrityksellä ei ole resursseja tai tahtoa ylläpitää IAM-järjestelmää On-Premise malliin omilla palvelimillaan, tarjoavat monet palveluntarjoajat Cloud IAM-vaihtoehtoa. Cloud IAM:ssa palveluntarjoaja hyödyntää pilviteknologiaa ylläpitääkseen yritykselle pääsynhallintajärjestelmää. Tällöin yrityksen ei tarvitse itse olla vastuussa järjestelmän vaatimista resursseista, kuten palvelimista eikä myöskään näiden mahdollisista päivitys- ja ylläpitotarpeista ajan myötä. Cloud IAM-palvelut ovat helpommin skaalattavissa yrityksen kokoon, joten käyttäjämäärän kasvu ei rajoita järjestelmän toimivuutta. (Utley, 2020)

Suurin etu On-Premise mallissa suhteessa pilvihallintamalliin on kuitenkin turvallisuus. Kun palvelimet, joissa järjestelmä toimii, on sijoitettu yrityksen omaan palvelinsaliin, pystyy yritys tarkkailemaan tarkalleen, kuka järjestelmään pääsee käsiksi. Mahdollisen tietomurron kohteeksi joutuva ulkoinen palveluntarjoaja saattaakin vuotaa asiakasyrityksen tietoja, aiheuttaen vahinkoa sekä palveluntarjoajalle, että asiakasyritykselle. (Utley, 2020)

2.4 Automatisoinnin tarve

Mahdollinen pääsynhallinnan automatisointi on yritykselle tärkeä päätös. Pienimmillä yrityksillä ei välttämättä ole järkevää investoida suurta summaa automatisoidakseen pääsynhallintaa, jos erilaisia rooleja ja työtehtäviä on vain muutama tai vähemmän. Suuremmilla yrityksillä automatisoinnin tarve on huomattavasti suurempi, sillä erilaisten oikeuksien manuaalinen ylläpito on sekä aikaa, että resursseja vievää. Manuaaliset prosessit ovat myös helpommin altistuvia virheille, kun taas automaation virheet ovat systemaattisia ja täten helposti huomattavissa ja korjattavissa.

3 TIETOTURVA

Tietoturva on yksi tärkeimmistä pääsynhallintaan vaikuttavista tekijöistä. Tietoturvaa laiminlyövä yritys saattaa menettää maineensa tai kokea taloudellisia tai sosiaalisia tappioita. Ilman riittävää pääsynhallintaa, yrityksen dataan saattaa päästä käsiksi eihalutut henkilöt. Vaikka data olisi ulkopuoliselta pääsyltä turvassa, heikko pääsynhallinta voi mahdollistaa yrityksen sisällä toimivan henkilön tahallisen tai tahattoman tietoturvarikkomuksen.

3.1 Tietoturvauhat

Yksi tavanomaisimmista tietoturvauhista yritysmaailmassa on tiedonkalasteluyritykset eli ”Phishing”-yritykset. Kalasteluyritykset tapahtuvat pääasiassa sähköpostitse tai puhelimitse. Kalastelija yrittää saada esimerkiksi sähköpostin kautta käyttäjän klikkaamaan sähköpostissa olevaa linkkiä, joka johtaa huijaussivustolle. Sähköposti on voitu saada näyttämään tulleeksi viralliselta luotettavalta taholta, kuten käyttäjän yritykseltä, pankilta tai operaattorilta. Kalastelun avulla käyttäjän salasana voidaan saada selville ja käyttää pahoihin tarkoituksiin. Jos pääsynhallinnasta ei olla huolehdittu tarpeeksi tarkkaan, tavallisen käyttäjän tunnuksilla voidaan päästä yrityksen luottamuksellisiin tietoihin käsiksi. Kalasteluyrityksiä ja niiden onnistumista voidaan vähentää monitoroimalla sähköpostiliikennettä ja estämällä liikenne tunnistetusta kalasteluosoitteesta, kouluttamalla yrityksen työntekijöitä tunnistamaan kalasteluviestin ja toimimaan yrityksen linjausten mukaisesti tällaisen viestin saadessaan. (Fruhlinger, 2020b)

Kalasteluyritykset tulevat perinteisesti yrityksen ulkopuolelta, mutta uhkia voi löytyä myös yrityksen sisältä. Yrityksen sisäisiin uhkiin kuuluvat muun muassa varomattomat työntekijät, jotka eivät tiedä joutuneensa kalastelun uhriksi tai muun tietoturvarikkomuksen aiheuttajaksi ennen kuin vahinko on jo tapahtunut. On siis syytä pitää työntekijät tietoisina mahdollisista tietoturvauhista ja niiden ehkäisytavoista. Yrityksestä poistuvan työntekijän pääsy järjestelmiin tulee jäädyttää mahdollisimman aikaisin, jotta luottamukselliseen materiaaliin ei ole enää pääsyä poistumisen jälkeen. (Cybersecurity Insiders, 2017)

3.2 Tietoturvallisuuden vahvistaminen pääsynhallinnalla

Hyvin toteutetulla pääsynhallinnalla voidaan pitää huoli yrityksen tietoturvallisuuden säilyvyydestä. Rajoittamalla käyttäjien pääsyä heitä koskemattomiin resursseihin, estetään mahdolliset tietovuodot, jossa käyttäjä saa käsiinsä luottamuksellista tietoa. Käyttäjien pääsyä yrityksen tietojärjestelmiin tulee pystyä valvomaan, jotta tiedetään, kenellä on pääsy mihinkin. Tiettyjen järjestelmäoikeuksien myöntämisen on tärkeää olla rajattua vain rajatulle henkilöstölle, jotta vahinkoa ei pääse tapahtumaan osaamattoman tai pahantahtoisen käyttäjän tekemänä. (Laka, 2019)

4 YRITYS X

Yritys X on suuri, satoja omia työntekijöitä ja alihankkijoita työllistävä teollisuusalan yritys. On-Premise toimintamallilla toteutetussa IT-ympäristössä, yrityksellä on käytössään kymmeniä tietojärjestelmiä, joiden pääsynhallinta tapahtuu pääosin manuaalisesti yrityksessä toimivan IT-palvelupisteen kautta. Neljän työntekijän IT-palvelupisteen työtehtäviin kuuluu käyttöoikeushallinnan lisäksi muun muassa palvelupyyntöjen ratkaisu, ongelman ratkonta ja korjaustoimenpiteet työasemiin ja tietojärjestelmiin liittyen, ohjelmistoasennukset ja toimiminen yhteyspisteenä peruskäyttäjien ja järjestelmien pääkäyttäjien välillä.

4.1 Käyttöoikeuksien hallintaprosessi

Tietojärjestelmien käyttöoikeuksia käsitellään Yritys X:ssä pääasiassa sähköisten käyttöoikeushakemusten kautta. Käyttäjän tarvitessa pääsyä järjestelmään tai haluttuun resurssiin, käyttäjä tai tämän esimies täyttää hakemuksen, jossa pyydetään haluttua oikeutta yrityksen intrasivuilla. Hakemuspohja pitää sisällään valtaosan Yritys X:n käyttämistä tietojärjestelmistä, mutta ei aivan kaikkia. Hakemuksesta puuttuvien järjestelmien oikeuksia pyydetään yleensä joko hakemuslomakkeen Lisätietoja-kentän kautta, tai vaihtoehtoisesti yleisenä palvelupyyntönä. Hakemuksen lähettämisen jälkeen lomake lähetetään hakemusta koskevan esimiehen hyväksyttäväksi. Esimiehen tulee käydä läpi mitä oikeuksia on pyydetty ja hyväksyä pyyntö, jos oikeudet ovat käyttäjän työnkuvan mukaiset. Hyväksynnän jälkeen hakemus muodostuu palvelupyynnöksi Yritys X:n tikettijärjestelmään. Tikettijärjestelmän kautta eri organisaatioiden työntekijät hoitavat oman toimialueensa palvelupyyntöjä oman osastonsa työjonosta.

Palvelupyyntö ohjautuu ensimmäisenä yrityksen HR-henkilöstölle. Tässä vaiheessa hakemuksessa pyydetyistä oikeuksista tehdään kirjaukset Yritys X:n henkilötietojärjestelmään. Henkilötietojärjestelmä, jatkossa HTJ, pitää sisällään käyttäjän henkilötietojen lisäksi tiedot käyttäjän työsuhteen muodosta, työskentelyorganisaatiosta ja tietojärjestelmistä joihin käyttäjälle on pyydetty oikeuksia. HTJ:n tietojärjestelmäoikeusnäkymässä on tietojärjestelmän nimen lisäksi annettu roolitieto, joskin kaikista eri

järjestelmien rooleista ja oikeuksista ei ole HTJ:n tietokannassa omaa roolia, vaan roolina on saatettu ilmoittaa yksinkertaisesti ”peruskäyttäjä” vaikka kyseisestä järjestelmästä useampia rooleja löytyisikin. HTJ:n näkymä ei siis aina anna tarkkaa tietoa mitä oikeuksia käyttäjällä ilmoitetussa järjestelmässä on. HTJ-kirjausten jälkeen, HR-osasto ohjaa tiketin IT-palvelupisteelle.

Nimi:	Matti Meikäläinen	**Nimilyhenne:**	MAME			
Henkilötunnus:	123456-123X	**Työsuhteen muoto:**	Määräaikainen	**Organisaatio:**	IT	
Tietojärjestelmä	**Rooli**	**Voimassaolo alku**	**Voimassaolo loppu**	**Myönnetty**	**Hylätty**	**Poistettu**
Tietojärjestelmä A	Peruskäyttäjä	1.1.2020	31.12.2021	ABC - 30.12.2019		
Tietojärjestelmä B	Peruskäyttäjä	1.1.2020	31.12.2021	ABC - 30.12.2019		
Tietojärjestelmä C	Peruskäyttäjä	10.1.2020	31.12.2021	ABC - 12.1.2020		
Tietojärjestelmä C	Erikoisrooli X	10.1.2020	31.12.2021		ABC - 12.1.2019	
Tietojärjestelmä C	Erikoisrooli Y	31.3.2020	31.12.2021	ABC - 3.4.2019		
Tietojärjestelmä D	Peruskäyttäjä	1.5.2020	31.12.2021	ABC - 2.5.2019		
Tietojärjestelmä E	Peruskäyttäjä	1.5.2020	31.12.2021	ABC - 2.5.2019		
Tietojärjestelmä E	Erikoisrooli X	1.5.2020	31.12.2021	ABC - 2.5.2019		
Tietojärjestelmä F	Peruskäyttäjä	3.6.2020	31.12.2021	ABC - 10.6.2020		

Kuva 5. Mockup-mallikuva Yritys X:n henkilötietojärjestelmästä.

IT-Palvelupiste vastaa haettujen oikeuksien myöntämisestä, tai joidenkin järjestelmien tapauksissa pyynnön välittämisestä eteenpäin järjestelmän pääkäyttäjälle. Käyttöoikeuspyyntöjen laajuus saattaa vaihdella yhden järjestelmäroolin lisäämisestä uuden käyttäjätunnuksen luomiseen moneen eri järjestelmään. Jotkin tietojärjestelmäoikeudet vaativat myös järjestelmien tiettyjen osa-alueiden vastuuhenkilöiden erillisluvan ennen oikeuksien myöntämistä. Nämä erillisluvat IT-palvelupiste pyytää sähköpostitse tältä vastuuhenkilöltä, sillä näillä vastuuhenkilöillä ei aina ole pääsyä tikettijärjestelmään, joten pyyntöä ei voi osoittaa vastuuhenkilölle hyväksyntää varten. Tämän vaiheen ajaksi oikeuspyynnöt saattavat jäädä pitkiksi ajoiksi työjonoon odottamaan luvan saamista, jos kyseessä on esimerkiksi tietyn koulutuksen vaativa järjestelmäoikeus. Erillisluvan saavuttua sähköpostitse, liitetään hyväksyntä käyttöoikeuspyyntöön ja edetään oikeuksien myöntämiseen.

Käyttäjätunnusten luominen ja oikeuksien lisääminen Yritys X:n järjestelmiin tapahtuu pääasiallisesti joko tietojärjestelmän oman käyttöliittymän kautta, tai sellaisen tietokannan kautta, jota useammat järjestelmät hyödyntävät. Jotkut järjestelmäoikeudet, kuten yrityksen verkkolevyillä olevien resurssien luku- tai kirjoitusoikeudet tai yhteiskäyttöön tarkoitettujen sähköpostilaatikoiden käyttöoikeudet ovat linkitettyjä Active Directory-ryhmiin. Kaikille eri verkkolevyrakenteille ei kuitenkaan ole erikseen luotu

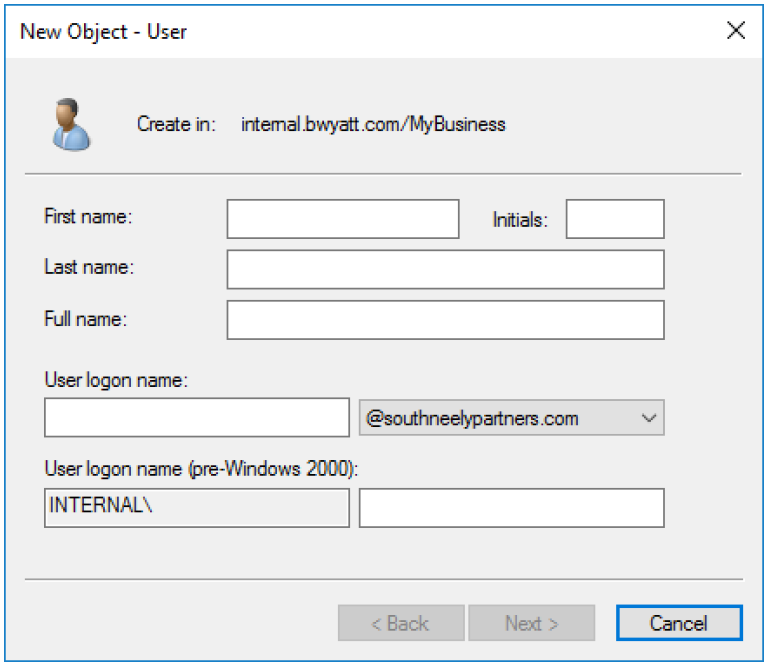
omaa käyttöoikeusryhmää, tai ryhmä, jolle on myönnetty oikeus haluttuun rakenteeseen saattaa antaa oikeuksia myös ei-haluttuihin resursseihin, joten näiden oikeuksien lisääminen ei ole kovin suoraviivaista.

4.1.1 Uuden käyttäjän luonti työasemaverkkoon

Uuden käyttäjän saapuessa töihin Yritys X:lle, tulee käyttäjälle luoda työasemaverkon käyttäjätunnus yrityksen Active Directoryyn. Jotta käyttäjän töihin saapuminen sujuisi mahdollisimman mutkattomasti ja käyttäjän tunnukset olisivat valmiina työsuhteen alkaessa, tulee IT-palvelupisteelle tieto uusista, luotavista työasemaverkon käyttäjätunnuksista viikoittaisessa raportissa, olettaen, että tieto käyttäjän töihin saapumisesta ja aloituspäivästä on kirjattu HTJ:hin vähintään viikkoa ennen työsuhteen alkua. Viikoittain aloittavien työntekijöiden määrä vaihtelee keskimäärin välillä 1–5, mutta tiettyinä ajankohtina vuodessa, viikon aikana aloittavia voi olla jopa kymmeniä. Jos tieto ei ole tulostunut raportille, ilmoitetaan saapuvista käyttäjistä joko erillisellä ilmoituksella tai käyttöoikeushakemuksella. Joskus ilmoitusta ei kuitenkaan tule etukäteen, tällöin käyttäjän työsuhteen alkamispäivänä tunnuksia ei ole valmiina, vaan ne luodaan sen hetken työkuormien sallimana ajankohtana, kunhan tieto työasematunnuksista löytyy HTJ:stä. On myös mahdollista, että käyttäjän aloitusajankohta siirtyy alkuperäisestä ajankohdasta tai peruuntuu kokonaan. Näistä muutoksista ei tule ilmoitusta raportille, jolloin tunnusten luontiin käytetty työaika menee hukkaan.

Käyttäjätunnuksen luonti tapahtuu manuaalisesti IT-palvelupisteen toimesta. Tunnuksen luominen aloitetaan avaamalla Active Directory ja HTJ. HTJ:n tietojärjestelmäoikeusnäkymästä voidaan tarkistaa, onko käyttäjällä entuudestaan työasematunnuksia mahdollisen edellisen työjakson jäljiltä vai tuleeko ne luoda alusta alkaen. Uutta tunnusta luodessa, HTJ:ssa ilmoitettu tieto työsuhteen muodosta määrittää mihin Active Directoryn OU:hun käyttäjätunnus luodaan. Vakituiset, määräaikaiset ja alihankkijakäyttäjät luodaan erillisiin OU-rakenteisiinsa. Kun oikea OU on tiedossa, luodaan sinne uusi User-objekti. Käyttäjän luontinäkymässä (Kuva 5) asetetaan kirjautumisessa käytettävän käyttäjätunnuksen lisäksi HTJ:ssa ilmoitetut nimi- ja nimilyhennetiedot (Kuva 4). Näiden tietojen syöttämisen jälkeen käyttäjälle asetetaan Yritys X:n

salasanapolitiikan mukainen ensikirjautumista varten käytettävä salasana. Tämän vaiheen jälkeen käyttäjätunnus muodostuu valittuun OU:hun.



Kuva 6. Esimerkkikuva Active Directoryn uuden käyttäjän luontinäkymästä. (Wyatt, 2018)

Käyttäjätunnuksen muodostumisen jälkeen asetetaan käyttäjätunnuksen voimassaoloaika, aluksi kaksi viikkoa aloituspäivämäärästä. Yritys X vaatii työaseman käyttäjiltä lyhyen verkkokoulutuksen, jotta työasematunnus säilyy käytettävissä kahden viikon jälkeen. Koulutus antaa nopean läpikäynnin työaseman ja työverkon turvalliseen käyttöön. Koulutuksen käymisen ja todistuksen toimittamisen jälkeen käyttäjän tunnuksen voimassaolo asetetaan työsuhteen loppupäivämäärään asti määräaikaisilla, vakituisten kohdalla vanhentumisajankohdaksi asetetaan ”never”. Kaikille käyttäjille lisätään aloitusvaiheessa tiettyjä AD-ryhmiä, jotka mahdollistavat muun muassa yrityksen intrasivuille pääsyn sekä oman työskentelyorganisaation yhteisiin resursseihin pääsyn. Käyttäjätunnukselle asetetaan myös henkilökohtainen kotiasema, jonne käyttäjä voi tallettaa työmateriaalia, joka säilyy turvassa palvelimella, vaikka työasemalle sattuisi jotain.

Perus Active Directory-tunnuksen luonnin jälkeen käyttäjälle pitää käydä luomassa sähköpostilaatikko Yritys X:n sähköpostipalvelimelle. Käyttäjän sähköpostilaatikko luodaan Microsoft Exchange Admin Centerin kautta, josta olemassa olevaan AD-

käyttäjään saadaan suoraan yhdistettyä uusi sähköpostilaatikko. Sähköpostilaatikon lisäksi, käyttäjille tulee mahdollistaa Yritys X:n pikaviestintäohjelmiston käyttö, joka tapahtuu kyseisen järjestelmän oman hallinnointipalvelimen kautta. Käyttäjätunnusten luonnin jälkeen työasemaverkkotunnusten myöntö kuitataan tehdyksi HTJ:hin tunnustentekijän nimilyhenteellä ja tunnukset tulostetaan odottamaan käyttäjän saapumista taikka lähetetään aloittavan käyttäjän esimiehelle Yritys X:n salatun turvasähköpostin kautta.

4.2 Kehitysalueet

Nykyinen manuaalinen pääsynhallintamalli Yritys X:n kokoisessa yrityksessä ei ole kovin tehokas. Monien käytössä olevien järjestelmien oikeuksien myöntäminen on rutiininomaista ja automatisoitavissa oikeanlaisilla työkaluilla. Myös monivaiheisempien oikeuksien myöntöprosessissa on kehitettävää, joka mahdollistaisi suoraviivaisemman pääsynhallinnan ja nopeamman käyttöoikeuspyynnön läpimenoajan, ja täten nopeuttaisi käyttäjien pääsyä tarvitsemiinsa resursseihin.

Myös oikeuksien monitoroinnissa on omat haasteensa. Käyttäjän järjestelmäoikeuksista osan näkee HTJ:n kautta, mutta HTJ:n näkymä ei aina kerro tarkkaa tietoa. HTJ:n roolitiedot eivät sisällä kaikkien eri järjestelmien kaikkia rooleja, eikä tieto lisätystä oikeudesta päivity automaattisesti HTJ:hin. Yksittäisille käyttäjille on saatettu myös lisätä oikeuksia tiettyihin verkkoresursseihin suoraan käyttämättä näille luotuja Active Directory-ryhmiä, näiden monitorointi ei ole keskitetysti mahdollista nykyisellä mallilla.

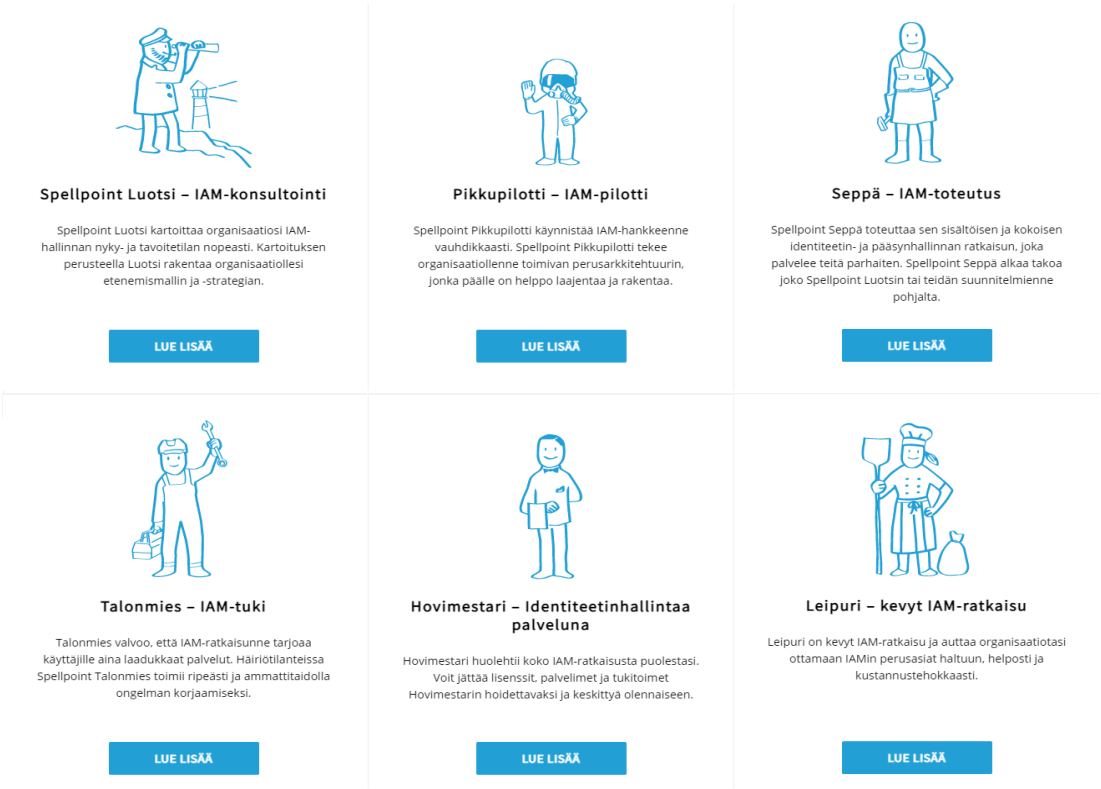
5 IAM-JÄRJESTELMÄN KÄYTTÖÖNOTTO YRITYS X: SSÄ

Yritys X:ssä ollaan ottamassa käyttöön keskitettyä IAM-pääsynhallintajärjestelmää korvaamaan nykyistä manuaalista toimintamallia eri tietojärjestelmille. Tässä luvussa tutustutaan erilaisten mahdollisten toteutusmallien vertailuun, käyttöönotossa ja suunnittelussa huomioitaviin asioihin, etukäteen kartoitettaviin tarpeisiin ja käyttöönoton vaikutuksiin eri osa-alueisissa Yritys X:ssä.

5.1 Toteutusmallivaihtoehdot

Ensimmäisenä vaiheena IAM-käyttöönottoprojektia on toteutusmallin valinta. Yritys X:n IT-ympäristö on toteutettu On-Premise mallilla ja myös IAM-järjestelmä tahdotaan käytettäväksi tällä mallilla. Pilvihallintana ulkoisen palveluntarjoajan kautta toteutettu pääsynhallinta tarkoittaisi, että yrityksen järjestelmien pääsynhallinta tapahtuisi yrityksen ulkopuolisten palvelimien kautta. Tämä toimintamalli ei kohtaa Yritys X:n näkemysten kanssa, jossa tietoturvallisuus on etusijalla ja yritysten järjestelmien tahdotaan olevan yrityksen sisäisesti hallittavissa. On-Premise mallin vahvempi turvallisuus ja Yritys X:llä käytössä olevat resurssit tukevat On-Premise mallin valitsemista pilvihallinnan sijaan.

Toteutusmallin tultua valituksi, pitää etsiä yritykselle sopiva palveluntarjoaja. IAM-palveluita tarjotaan aina pääsynhallinnan kartoituksesta, itse pääsynhallintajärjestelmän toteutukseen ja ylläpitoon. Koska Yritys X:llä ei ole entuudestaan keskitettyä pääsynhallintajärjestelmää, mutta tahtotilana on, että pääsynhallinta on edelleen Yritys X:n käsissä, hyvänä vaihtoehtona voidaan pitää palveluntarjoajaa, jonka kanssa järjestelmän kartoitus ja toteutus onnistuu tuomalla IAM-järjestelmä osaksi Yritys X:n omaa IT-ympäristöä ja hallinnoimalla IAM-järjestelmää sisäisesti.



Kuva 7. Spellpointin tarjoamia IAM-palveluita. (Spellpoint, 2020)

5.2 IAM-järjestelmän suunnittelu ja käyttöönotto

Yritys X:n pääsynhallinta tapahtuu nykymallilla lähes täysin ihmisen toimesta ja koska prosessi ei ole täysin suoraviivainen kaikkien järjestelmäoikeuksien suhteen ja siihen sisältyy monia vaiheita, mahdollisuuksia inhimillisen virheen sattumiseen on paljon. Suuressa yrityksessä on tärkeätä, että pääsynhallinta on hyvin toteutettu, jotta sekä yrityksen tietoturvallisuus säilyy ja käyttäjille saadaan heidän tarvitsemansa käyttöoikeudet nopeasti ja sujuvasti käyttöön. Yritys X:n valtavan suuren IT-infrastruktuurin ja järjestelmien määrän vuoksi, on järkevää suorittaa IAM-järjestelmän käyttöönotto integroimalla eri järjestelmien pääsynhallinta IAM:iin vaiheittain, jotta kaikkien järjestelmien käytettävyys ei kärsi, jos pääsynhallinnassa ilmenee ongelmia IAM:in käyttöönottovaiheessa. Keskitetyn IAM-järjestelmän käyttöönoton myötä myös yksittäisen käyttäjän oikeuksien monitorointi helpottuu, kun kaikkien järjestelmien tarkat oikeustasot ovat selvitettävissä samasta paikasta.

IAM-käyttöönottoprojektin suunnitteluvaiheessa on tärkeätä eri järjestelmien pääkäyttäjien ja vastuuhenkilöiden olla mukana suunnittelemassa pääsynhallintaa yhdessä

IAM:in toteuttajan kanssa, jotta vaatimukset eri järjestelmärooleille ovat selvillä. Kun tietylle roolille määritetään attribuutteja, tulee tarkkaan olla tiedossa mitä kaikkia järjestelmäoikeuksia tiettyyn rooliin kuuluu. Järjestelmäoikeuksien yhdistäminen tiettyyn rooliin varmistaa, että kyseisen roolin omaavilla käyttäjillä on aina vastaavat oikeudet, vähentäen monivaiheisten oikeuksien myöntämisestä aiheutuvia virhemahdollisuuksia.

Ensimmäisenä IAM-integrointiin on järkevää ottaa käsittelyyn yrityksen Active Directory. Active Directory toimii yrityksen pääsynhallinnan selkärankana, sillä lähestulkoon kaikkien Yritys X:n käyttämien järjestelmien vaatimuksena on, että käyttäjältä löytyy AD-tunnus. Perusmuotoisen AD-käyttäjätunnuksen luonti tapahtuu myös suhteellisen suoraviivaisesti aiemmin mainitun kaavan mukaan ja on täten mahdollista automatisoida tiettyjä sääntöjä noudattamalla. IAM-projektin suunnitteluvaiheessa luodaan rooli, joka pitää sisällään tämän perusmuotoisen AD-tunnuksen, olkoon se nimeltään ”AD-perus”. Kun uusi työntekijä on aloittamassa Yritys X:n palveluksessa, voisi esimies tehdä pyynnön alaisensa työasematunnuksista, joka laittaisi IAM-järjestelmässä prosessin käyntiin tunnusten luomiseksi. Aloittavaa henkilöä vastaava identiteetti saisi roolin ”AD-perus”. IAM-järjestelmä hakisi tarvittavat tiedot HTJ:sta, jonka jälkeen suunnitteluvaiheessa asetettujen parametrien mukaisesti se luo AD-käyttäjätunnuksen, jolloin käsin tehtyä tunnuksen luontia ei enää vaadittaisi.

Toinen tärkeä ominaisuus joka IAM-järjestelmään tulee ottaa käyttöön projektin alkuvaiheessa, on identiteetin elämänkaaren hallinta. Identiteetin elämänkaari alkaa työsuhteen alkaessa ja päättyy työsuhteen päättymisen mukana. Kun käyttäjä poistuu yrityksen palveluksesta, tulee käyttäjällä olleet roolit poistaa hänen identiteetistään, jolloin myös pääsy roolien mukaisiin järjestelmiin päättyy. Tieto käyttäjän työsuhteen alusta ja lopusta löytyy HTJ:sta, joten IAM-järjestelmän tulee aktiivisesti verrata löytyvien identiteettien voimassaoloa HTJ:ssa löytyvään tietoon. Elämänkaari pitää sisällään myös mahdolliset muutokset esimerkiksi käyttäjän organisaatiosta. Jos käyttäjän organisaatio muuttuu työsuhteen aikana, tulee tämän myötä muuttaa myös käyttäjän Active Directory-tunnuksen ryhmät vastaamaan uutta organisaatiota.

IAM-järjestelmän käyttöönotto vaatisi muutoksia myös Yritys X:n tikettijärjestelmään, tarkennettuna käyttöoikeuspyyntöjen käsittelyyn. Nykyisen hakemuksen

liikkuessa ihmiskäsittelijältä toiselle, tulisi näiden oikeuspyyntöjen mennä IAM-järjestelmän käsiteltäväksi, kun hakijan esimies on hyväksynyt pyynnön. Tiettyjen roolien myöntäminen käyttäjille voitaisiin automatisoida IAM-järjestelmän kautta, jos kyseinen rooli ei vaadi erillishyväksyntöjä, nopeuttaen huomattavasti perusoikeuksien myöntöaikoja.

Erikoisroolien lisääminen käyttäjälle, jotka nykymallilla vaativat sähköpostitse kysyttävän erillisluvan, voitaisiin toteuttaa ohjaamalla kysely suoraan IAM-järjestelmän kautta luvan myöntämisestä vastaavalle vastuuhenkilölle. Vastuuhenkilö voisi IAM-käyttöliittymän kautta joko hyväksyä tai hylätä pyynnön. Hyväksytyn pyynnön kohdalla, IAM-järjestelmä lisää käyttäjälle pyydetyn roolin, jonka kautta tarvittu järjestelmäpääsy mahdollistuu. Hylättyyn pyyntöön voitaisiin asettaa kenttä, johon kerrotaan hylkäämisen perustelu, esimerkiksi ”puuttuva koulutus”. Tätä samaa mallia voitaisiin myös soveltaa muiden haluttujen erikoisroolien osalla, joiden kohdalla halutaan varmistaa, kenelle käyttäjille kyseistä roolia lisätään. Tämä suoraviivaistaisi oikeuden myöntöprosessia erikoisroolien kohdalla, ja vähentäisi IT-palvelupisteelle kasaantuvien, hyväksyntää odottavien pyyntöjen määrää.

5.3 IAM-käyttöönoton vaikutukset

Keskitetyn pääsynhallintajärjestelmän käyttöönotolla on suuria vaikutuksia yritykseen. Manuaalisesta pääsynhallinnasta aiheutuvat palvelupyynnöt ja käyttöoikeushakemukset muodostavat suuren osan IT-palvelupisteen työkuormasta. Käyttöoikeushakemuspyyntöjä käsitellään palvelupisteen toimesta jopa satoja kuukausittain, joten keskitetyn ja automatisoidun pääsynhallinnan myötä, työaikaa vapautuu muille työtehtäville. IT-palvelupisteen toimintaa voitaisiin kehittää kattamaan useamman järjestelmän ongelman- ja vianratkaisua, jolloin kyseisten ongelmien ratkaisuun käytettyä aikaa vapautuisi järjestelmävastaavilta.

Käyttäjän näkökulmasta IAM-järjestelmä toisi jouhevuutta oikeuksien käsittelyyn. Käyttäjien tekemät oikeuspyynnöt eivät joutuisi enää kulkemaan monen käsiparin kautta, jolloin pyyntöjen ratkaisuajat nopeutuisivat. Käyttäjien pääsy työssään tarvitsemiin heti työsuhteen alusta tapahtuisi nopeammin, kun käyttäjän työroolin mukaiset

IAM-roolit lisättäisiin käyttäjälle. IAM-järjestelmän käyttöönotto osaksi oikeuksien hakuprosessia selkeyttäisi myös oikeuksien hakulomaketta. Kymmenien eri järjestelmien ja näiden alla olevien yksittäisten oikeuksien hakemisen sijaan, käyttäjälle haettaisiin eri rooleja, jotka pitävät sisällään tarvittavat, ennalta määritetyt järjestelmäoikeudet.

Eräs suurimmista IAM-järjestelmän vaikutusalueista on Yritys X:n tietoturvallisuus. Vaikkakin nykyinen malli onkin tarkkaan valvottu, mahdollisuus inhimilliselle virheelle on aina olemassa. Tietyn käyttäjän oikeuksien tarkasteleminen vaatii nykyisellään kirjautumisen haluttuun järjestelmään järjestelmänvalvojaoikeuksilla, ja tarkastamalla tätä kautta käyttäjän oikeudet kyseiseen järjestelmään. Keskitetyn pääsynhallinnan kautta kaikki käyttäjään kohdistuvat roolit kertovat mihin käyttäjällä tarkalleen on pääsy ja millaisin oikeuksin, vähentäen tiedostamattomia tai liian laajoja oikeuksia. Kun IAM-järjestelmä on rakennettu antamaan käyttäjälle roolin mukaiset oikeudet tiettyyn järjestelmään, tapahtuu oikeuksien myöntö roolin kautta aina samalla tavalla, vähentäen virheiden mahdollisuutta oikeudenmyöntöprosessissa.

6 YHTEENVETO

Pääsynhallinta on suuri tekijä yrityksen toimivuuden kannalta. Hyvin toteutettuna se kasvattaa yrityksen tietoturvallisuuden tasoa ja mahdollistaa työntekijöiden tehokkaan työskentelyn, kun työnmukaiset oikeudet järjestelmiin saadaan kuntoon nopeasti. Huolimaton pääsynhallinta voi johtaa yrityksen luotettavuuden ja tietojen eheyden menetykseen, kun taas liian tiukka pääsynhallinta voi vaikeuttaa yrityksen työntekijöiden työntekoa rajoittamalla pääsyä tarvittaviin järjestelmiin. Pääsynhallinnan toteutus yrityksessä ei ole vain IT- tai tietoturvaorganisaation vastuulla, vaan pääsynhallinta tulee toteuttaa yrityksen eri organisaatioiden yhteistyönä sen tehokkuuden takaamiseksi.

Opinnäytetyön tarkoituksena oli tutkia manuaalisesti toteutetun käyttöoikeuksien ja pääsynhallinnan prosessia Yritys X:ssä ja tutustua keskitetyn identiteetin- ja pääsynhallintajärjestelmän suunnittelussa ja käyttöönotossa huomiotaviin asioihin, ja muutoksiin joita IAM-järjestelmän käyttöönotto toisi mukanaan. Todettiin, että IAM-järjestelmä toisi mukanaan vahvempaa tietoturvaa, helpotettua käyttöoikeuksien hallintaa ja monitorointia sekä vähentäisi manuaalista työtä. Yritys X:n kokoisessa suuressa yrityksessä IAM-järjestelmän käyttöönotto on aikaa vievä, mutta tuottelias ja kannattava projekti.

LÄHTEET

Cybersecurity Insiders. 2017. Insider threat 2018 report. Viitattu 27.11.2020 https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf

Fruhlinger, J. 2020a. The CIA triad: Definition, components and examples. Viitattu 16.11.2020 https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

Fruhlinger, J. 2020b. What is phishing? how this cyber attack works and how to prevent it. Viitattu 27.11.2020 https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Laka, P. 2019. The risks of not having an identity and access management system. Viitattu 27.11.2020 https://www.e-point.com/blog/the-risks-of-not-having-an-identity-and-access-management-system

Martin, J. A., & Waters, J. K. 2018. What is IAM? identity and access management explained. Viitattu 27.11.2020 https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

Microsoft. 2020. Active directory security groups (windows 10) - Microsoft 365 security. Viitattu 27.11.2020 https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups

Morrow, S. 2018. Top 5 ways to identify and address insider threats. Viitattu 27.11.2020 https://resources.infosecinstitute.com/topic/top-5-ways-to-identify-and-address-insider-threats/

Network Encyclopedia. 2020. Active directory. Viitattu 27.11.2020 https://networkencyclopedia.com/active-directory/

Niemi, K. 2020. Identiteetin ja pääsynhallinta (IAM). Viitattu 27.11.2020 https://www.itewiki.fi/opas/kayttajahallinta-iam/

Rouse, M. 2020a. What is active directory (AD)? Viitattu 18.11.2020 https://searchwindowsserver.techtarget.com/definition/Active-Directory

Rouse, M. 2020b. What is identity and access management? guide to IAM. Viitattu 14.11.2020 https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

Rouse, M. 2020c. What is identity management? A definition from WhatIs.com. Viitattu 14.11.2020 https://searchsecurity.techtarget.com/definition/identity-management-ID-management

Spellpoint. 2020. IAM-palvelut ja IAM-ratkaisut - identiteetin ja pääsynhallinta. Viitattu 27.11.2020 https://spellpoint.fi/iam-palvelut-uusi/

Tyson, J. 2019. The CIA triad – interests and insights. Viitattu 16.11.2020 https://blog.jamestyson.co.uk/the-cia-and-dad-triads

Utley, G. 2020. Cloud identity and access management vs. on-premise: Which is best? Viitattu 19.11.2020 https://thinkred.redriver.com/cloud-identity-and-access-management

Wyatt, B. 2018. [Tool] create and configure active directory and office 365 users at once. Viitattu 20.11.2020 https://www.thelazyadministrator.com/2018/07/11/tool-create-and-configure-active-directory-and-office-365-users-at-once/