Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VILLE NURMILA

Identiteettitiedon (IAM) sekä käyttövaltuushallinnan (MDM) kehittäminen Porin kaupungilla

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2023

TIIVISTELMÄ

Nurmila, Ville: Identiteettitiedon (IAM) sekä käyttövaltuushallinnan (MDM) kehittäminen Porin kaupungilla
Opinnäytetyö, AMK
Tietojenkäsittelyn tutkinto-ohjelma
Toukokuu 2023
Sivumäärä: 37
Liitteitä: 2

Opinnäytetyön tavoitteena oli tutkia Porin kaupungin nykyisiä käytössä olevia järjestelmiä, jotka kohdistuvat identiteettitietojen hallintaan ja käyttövaltuushallintaan. Valitut järjestelmät tähän opinnäytetyöhön olivat Microsoft Azure, Microsoft Intune sekä Efecte IGA. Näistä järjestelmistä pyrittiin löytämään ehdotuksia, miten organisaation toimintaa voitaisiin kasvattaa tehokkaammaksi ja luotettavammaksi. Ehdotuksien avulla voitaisiin säästää Porin kaupungin resursseja ja parantamaan IT-palvelun toimintaa.

Opinnäytetyössä tullaan käsittelemään ensin mitä on identiteettitiedot, identiteettitietojen hallinta (IAM). Tästä siirrytään perehtymään käyttövaltuushallintaan (MDM). Ohessa käydään myös läpi identiteetti- ja käyttövaltuushallinnan vaatimuksia, standardeja ja parhaita käytäntöjä. Aiheessa käsitellään myös rajallisesti tietoturvallisuusvaikutuksista. Näiden käsittelyn jälkeen perehdytään Porin kaupungin käytössä oleviin järjestelmiin ja miten Porin kaupunki näitä hyödyntää toiminnassaan. Lopuksi pohditaan, miten järjestelmien toimintaa voitaisiin kehittää ja parantaa.

Tarkoituksena tällä opinnäytetyöllä on kerätä näitä ehdotuksia, miten Porin kaupungin olemassa olevien järjestelmien toimintaa voidaan parantaa ja esittää nämä ehdotukset organisaatiolle.

Avainsanat: identiteetti, hallintaoikeus, käyttöoikeus, käyttäjätunnukset, standardit, käytäntö, tietoturva

Abstract

Nurmila, Ville: Development of identity and access management in the city of Pori
Bachelor’s thesis
Degree programme in Business Information Systems
May 2023
Number of pages: 37

The aim of the thesis was to investigate the existing systems that the city of Pori now uses, which are aimed at identity information management and access management. The systems chosen for this thesis were Microsoft Azure, Microsoft Intune and Efecte IGA. From these systems, suggestions were sought on how to make the organization's operations more efficient and reliable. With these help suggestions, the resources of the city of Pori could be saved and the operation of the IT service could be improved.

The thesis will first deal with what identity information is, identity information management (IAM). From here we move on to familiarize ourselves with user authorization management (MDM). The requirements, standards and best practices for identity and authorization management are also reviewed in the attachment. In connection with the topic, there is also a limited information security impact. After processing these, we will learn about the systems in use by the city of Pori and how the city of Pori uses them in its operations. Finally, let's consider how to develop and improve the operation of the systems.

The purpose of this thesis is to collect these suggestions on how to improve the functioning of the existing systems of the city of Pori and present suggestions to the organization.

Keywords: identity, management right, access right, usernames, standards, usage, information security

SISÄLLYS

LYHENNELUETTELO

AD	Active Directory, käyttäjätietokanta ja hakemistopalvelu.
IAM	Identity and Access Management, käyttäjätietokannan sekä todennuksen hallinta.
MDM	Master Data Management, ydintieto ja perustietojen hallinta.
ISO 27001	Tietoturvajohtamisen standardi, jossa esitetään vaatimuksia tietoturvalle
Tietoturva	Tiedon eheyden, luottamuksellisuuden, kiistämättömyyden, käytettävyyden ja saatavuuden ylläpitäminen.
Käyttövaltuus	Tietojärjestelmässä myönnetty roolipohjainen käyttöoikeus henkilölle tai henkilöryhmälle.
IGA	Identity and Governance Administration, identiteettien hallinta, toteuttaa IAM toiminnallisuuksia.

1 JOHDANTO

Tässä opinnäytetyössä käsittelemme aiheena identiteettitietojen hallintaa (IAM), sekä näihin liittyviä käyttövaltuuksien hallintaa (MDM). Opinnäytetyön tarkoituksena on kehittää Porin kaupungin käyttövaltuushallinnan kehittämistä. Ensin tutustutaan itse aihepiiriin, jotta saadaan perustuntemus käsiteltävästä aiheesta ja myöhemmin tässä opinnäytetyössä perehdytään Porin kaupungin käyttämiin järjestelmiin ja miten organisaatio niitä hyödyntää. Lopussa käsittelemme, miten näitä järjestelmiä voitaisiin käyttää tehokkaammin parantaakseen organisaation toimintaa.

Opinnäytetyön toimeksiantajana toimii Porin kaupunki. Porin kaupunki on 83 297 asukkaan koti, joista työntekijöihin kuuluu noin 5000 henkilöä. (Oritieto, 2022). Tämän opinnäytetyön aihe saatiin Porin kaupungilta. Aihe on ajankohtainen, sillä Porin kaupunki suunnittelee seuraavaa kehitysaskelta identiteetti- ja käyttövaltuushallinnan kehittämisessä. Opinnäytetyön ratkaistava ongelmana on siis selvittää nykyisten käyttöpalveluiden ja järjestelmien ajantasaisuus sekä miten nykyistä hajautettua käyttöoikeushallintaa voitaisiin kehittää, säästääkseen Porin kaupungin rajattuja resursseja. Nykyinen toteuttaminen vaatii paljon manuaalista tekemistä usealta eri taholta, joka rokottaa vahvasti olemassa olevia resursseja ja ruuhkauttaa toimintaa entisyydestään. Porin kaupungin henkilökunta on alati vaihtuvaa, joka vaatii vahvaa painostusta ICT-yksiköltä jatkuvien henkilöstömuutoksien ja tunnuksien identiteettihallinnan sekä käyttövaltuushallinnan muutoksien kanssa.

Tietojenkäsittelyä koskevat organisaatiot käyttävät arkipäiväiseen toimintaan käyttöoikeuksia ja työhön tarvittavia resursseja. Näitä resursseja voidaan kuvata esimerkiksi tietojärjestelmillä, sovelluksilla, datavarastoja tai hallintoon liittyviä fyysisiä laitteita. Käyttöoikeus kuvataan työntekijän työssään tarvitsemiaan räätälöityjä oikeuksia organisaation resurssien käyttöä varten. Tämä tuottaa organisaatiolle haasteita resurssien ja työntekijöiden laajuuden kanssa, mitä enemmän resursseja ja työntekijöitä organisaatiolla on, sitä enemmän jatkuvaa ylläpitoa ja oikeuksien tarkastelua organisaatio vaatii. Huonosti

organisoitu hallinta vähentää yrityksen ja työntekijän turvallisuutta ja vähentää tuottavuutta. (Valtiovarainministeriö, 2006, s. 9-10.)

Identiteetinhallinta kuvataan menetelmänä, jonka avulla on mahdollista oikein toteutettuna hallita käyttöoikeuksia ja ratkaista käyttöoikeuksiin kohdistuvia yleisiä ongelmia. Identiteetinhallinta kuvataan tässä opinnäytetyössä käyttäjän sähköisen identiteetin ja siihen kohdistuviin käyttöoikeuksiin, niiden hallintaan sekä jakamista eri tietojärjestelmiin. Yleisesti organisaation henkilöstöhallinnolla on järjestelmä, jota kuvataan identiteetinhallintajärjestelmäksi. On tällä ratkaiseva rooli käyttöoikeuksien hallintaprosesseissa organisaation toiminnassa. (Kasanen, 2010, s. 1.)

2 TUTKIMUSONGELMAT

”Tietosuojalaki (Tietosuojalaki 5.12.2018/1050) edellyttää henkilötietojen suojaamista, tietojen tarpeellisuus- ja virheettömyysvaatimuksen, sekä käyttötarkoitussidonnaisuuden vaatimuksen huomioon ottamista. Järjestelmien käyttöoikeuksien määrittäminen asianmukaisesti on edellytyksenä sille, että edellä mainitut vaatimukset sekä niiden valvonta voidaan suorittaa lain edellyttämällä tavalla. Käyttöoikeuksien ja niiden sisällön määrittäminen tulee käytännössä tehdä henkilötasolla. (Valtiovarainministeriö 2006.)” (Salminen, 2022, s. 6.)

2.1 Tutkimusongelma

Porin kaupungin työntekijöiden käyttäjätunnukset ja niihin sisälletyt käyttövaltuusoikeudet luodaan manuaalisesti käsin. Tämän lisäksi näiden tunnuksien hallinta sekä tarpeellinen poistaminen tapahtuu manuaalisesti. Prosessissa ilmenee vakavia ongelmia, mitkä vaikuttavat organisaation toimintaan tunnuksien luomisessa ja niiden valvomisessa. Prosessi alkaa tilauspyynnöstä (liite 1) Active Directoryn (AD) käyttäjätunnuksille, joka täytetään manuaalisesti esihenkilön roolissa olevan työntekijän toimesta itsepalveluportaalin (Efecte IGA) kautta. Pohjana käytetään tunnuksen olemassaolo ja voimassaolo ajalle uuden työntekijän työsuhteeseen perustuvaa aloitus- ja päättymisaikaa.

Tunnuksien luomiseen perustuvat toimenpiteet suorittavat tähän valtuutettu IT-palvelun työntekijä. Pääsääntöisesti toimenpide pohjautuu muistinvaraisiksi ja inhimillisten virheiden tekeminen korostuu. Käyttäjätunnuksien luominen on keskitetty vain muutamalle IT-palvelun tukihenkilölle, mikä hidastaa prosessia tulevina ruuhkatilanteina tai sairas/poissaolotilanteissa. Ruuhkautuneessa tilanteessa tunnuksia pystyy myös muut IT-palveluun kuuluvat työntekijät luomaan, joilla on tarvittavat oikeudet käyttäjätunnuksien tekemiseen. Näissä tilanteissa korostuu inhimilliset virheet ja usein tärkeitä identiteettitietoja rekisteröidään väärin. Tähän usein on syynä puutteelliset opastukset tai

vanhentuneet käytännöt tunnuksien luomisprosessissa. Tunnuksien tarkastelu jälkikäteen suoritetaan yleisesti vasta virheiden ilmaantuessa.

Käyttöoikeuksien lisääminen tunnuksen luontivaiheessa perustuu karkeaan roolimääritykseen. Tämä usein toteutetaan kopioimalla AD:sta vastaavaa työtä tekevän tai samaan toimialaan kuuluvan henkilön rooli. Tämänkaltainen toiminta on erittäin riskialtis, koska nyt uuden käyttäjän käyttöoikeudet eivät välttämättä vastaa työhönsä tarpeellisia oikeuksia. Tämän lisäksi korostuu kopioinnista syntyvät ongelma alttiudet. Henkilö saattaa saada liikaa oikeuksia, jotka voivat aiheuttaa suurta tietoturvariskiä tai käyttöoikeudet voivat jäädä liian pieniksi, mikä estää työntekijän työsuoritusta. Käsin täytettävien käyttäjätunnuksien tiedot ovat myös erittäin alttiita ja haavoittuvaisia inhimillisille kirjoitusvirheille ja tämä toimintatapa on hyvin aikaa kuluttava ja hidas prosessi suorittaa verrattuna kopiointiin. Näiden ongelmien takia tunnuksien luomisprosessi on hidasta ja tämä vaikuttaa pahasti uusien työntekijöiden tunnuksien aktivoimiseen ajallaan, vanhojen tunnuksien hallinnointiin ja organisaatiosta poistuvien työntekijöiden tunnuksien poistamiseen. Ongelmat aiheuttavat kausittaisia ruuhkautumisia tunnuksien hitaan luomisprosessin takia sekä käyttöoikeuksien myöntämisestä tai myöntämättömyydestä aiheuttavat ongelmat lisäävät ruuhkautumista ja palveluiden toimimattomuutta käyttäjillä.

3 IDENTITEETTIEDON HALLINTA IAM

Tietotekniikassa identiteetti koostuu attribuuteista eli ominaisuuksista, jotka kuvaavat kohdetta. Kohde voi olla käyttäjä eli ihminen, määritetty laite tai järjestelmä. Tähän käytetään olemassa olevaa järjestelmää nimeltä IAM. Joka muodostuu sanoista Identity and Access Management, joka käsittelee sisällään eri prosessien, teknologian sekä datan yhteensovittamista. Tällä pyritään luomaan eri käyttäjille, laitteille tai järjestelmille oma identiteetti, jolle pystytään yksilöimään omat tarpeelliset oikeudet tietoihin. (Niemi, n.d.)

Identiteetti pystytään jakamaan neljään erilliseen osioon, jotka kuuluvat autentikointi, auktorisointi, administrointi sekä auditointi. Autentikointi koostuu laitteen, järjestelmän tai käyttäjän tunnistamisesta erillisellä tunnistautumisella mikä voi koostua esimerkiksi käyttäjätunnuksesta ja salasanasta, turvallisempaan tunnistautumiseen voidaan hyödyntää myös vahvoja tunnisteita esimerkiksi kertakäyttöisiä biotunnisteita, mobiilisalasanoja ja verkkopankkitunnuksia. Auktorisointi tarkoittaa tunnistetun identiteetille käyttöoikeuksien määrittelyä tarvittavan tehtävän tai roolin tarvittaviin palveluihin sekä järjestelmiin. Administrointi kuvastaa kokonaisuuden hallintaa. Auditointi on asetettujen vaatimuksien ja säädöksien jatkuvaa valvontaa ja kontrollointia. (Niemi, n.d.)

4 KÄYTTÖVALTUUKSIEN HALLINTA MDM

Tärkeänä osana tietoturvaa on käyttövaltuuksien hallinta, jossa tarkastellaan henkilöiden tai käyttäjien identiteettiä oikeudellisuuden varmistumiseksi. Käyttövaltuuksien hallinnassa käytetään käyttövaltuusperiaatteita, jotka helpottavat organisaation käyttöoikeuksien tarkastelua ja väärinkäyttöjen minimointia. Käyttövaltuusperiaatteet kuuluvat osana käyttövaltuuspolitiikkaan sekä keskeisenä osana organisaatioiden tietoturvallisuuspolitiikkaan.

Periaatteiden avulla ohjataan sekä hallinnoidaan tietojärjestelmien oikeaoppista käyttämistä. Periaatteiden noudattamisella organisaatio pystyy pienentämään kustannuksia pääsemällä pois turhista lisenssikustannuksista. Samalla tietojärjestelmien käyttö yksinkertaistuu ja käyttöoikeuksien väärinkäytöksien mahdollisuudet pystytään minimoimaan. (Opitietosuojaa, n.d.)

Käyttövaltuuksien hallintaa kuvataan myös termistöllä Master Data Management eli MDM. Tämä käsittelee organisaation ydintietoja ja niiden hallintaa omistajuusoikeuksien kautta. MDM pitää sisällään tiedonhallinnan kaikki prosessit, jonka avulla organisaatio varmistaa ylläpidettävän tiedon yhdenmukaisuuden, vastuunjaon sekä hallinnan. Näihin sisältyy muun muassa yrityksen standardit, linjaukset ja tarvittavat välineet toiminnan takaamiseksi. (Itewiki, n.d.)

Tätä ydintietojen hallintajärjestelmää hyödynnetään organisaation datan standardoinnilla eli tietomassojen säilyttämiseen, poistamaan päällekkäisyyksiä sekä virheellisen datan pääsyä järjestelmiin. Yksinkertaisuudessaan Master Data Managementilla pyritään luomaan organisaatiolle luotettava ydintietojen lähdepalvelu. (Itewiki, n.d.)

5 IDENTITEETTI- JA KÄYTTÖVALTUUSHALLINNAN VAATIMUKSET

Käyttövaltuushallinnan tavoitteena on varmistaa, että tiedostoihin ja tietoihin pääsee käsiksi vain niihin oikeutetut henkilöt. Käyttäjätunnuksien oikeuksia sekä voimassaoloaikaa tarkastellaan toistuvasti niiden olemassaolon ajan. Näin voidaan varmistaa, että käyttäjillä on työtoimenkuvaa vastaavat aktiiviset käyttöoikeudet ja asiattomat sekä vanhentuneet käyttäjätunnukset vapautetaan resursseista poistamalla. (Ulkoministeriö, 2020, s. 75.)

Tietoturvallisuus rakentuu viidestä kokonaisuuden eri osatekijästä, joita ovat luottamuksellisuus, eheys, käytettävyys, kiistämättömyys sekä pääsynvalvonta. Luottamuksellisuudella varmennetaan, että tietoihin oikeutettu henkilö pääsee ainoastaan niitä käsittelemään. Käytettävyydellä eli saatavuudella varmistetaan tietoon pääseminen paikasta ja ajasta riippumatta. Eheydellä kuvastetaan tietojen pitävän paikkansa ja olevan ajankohtaista ilman ristiriitoja. Kiistämättömyydellä varmistetaan tiedon alkuperän paikkansapitävyys. Pääsynvalvonnan keinoiksi lasketaan ICT-infrastruktuurin tekniset ja operatiiviset menetelmät. (Turunen, 2018, s.19.)

Mainitut viisi tietoturvallisuuden perusmääritelmää, jotka ovat suorassa yhteydessä identiteetin sekä käyttövaltuushallinnan toteuttamiseen ja tietoturvallisuuteen. Yksi tärkeimmistä tietoturvan osatekijöistä on luottamuksellisuus, joka linkittyy identiteetin- ja käyttövaltuushallintaan, koska IGA-ratkaisun avulla voidaan hallita käyttövaltuuksia ja varmistetaan, että vain oikeutetuilla henkilöillä on pääsy tietoihin. IGA-ratkaisun käytettävyyttä tuodaan esille esimerkiksi käyttäjälistan ajantasaisuuden, käyttäjän käyttöoikeuksien sekä ylläpitämisen tehtävien kautta. Käyttöoikeuksien tarkistelu säännöllisesti ehkäisee riskiä mahdollisiin vahingossa myönnettyihin oikeuksiin, joita ovat esimerkiksi oikeuksien myöntäminen ajankohtana, jolloin niitä ei pystytä rekisteröimään IAM-järjestelmään. Riski oikeuksien valvontaan pystytään ehkäisemällä säännöllisellä tarkastelulla.

Eheyden merkitys käyttövaltuuksien tilaamisen prosessissa kuvataan tarkkaan määrittelyllä, jossa saadaan vastaukset, kuka tilauksen tilasi, milloin, mitä oikeuksia sekä millä perusteilla. Kiistämättömyydellä ei ole suoranaista näkyvää liitäntää identiteetin tai käyttövaltuuden hallintaan, sillä yleisin käytettävät salausmenetelmät ja biometriikka toimivat jo tunnistautumisena käyttäjälle tehden asian kiistämättömäksi. Asian sisältö liittyy lähinnä täten pääsynhallintaan. (Hakala, 2006; Turunen, 2018.)

Voimme luoda pääsynhallinnan määrittelemällä sille metodin tai mekanismin, jolla käyttäjä pääsee käyttämään sitä paikasta tai ajasta riippuen tai määritetyn ajan sisällä. Tämän avulla käyttövaltuushallintaa pystytään hyödyntämään määrämuotoisissa tilaamisessa tai automaattisen rooliperusteisen oikeuksien hallinnoinnissa tarvittavaan tietojärjestelmään. Järjestelmän pääsynhallinnassa voidaan määritellä AD-ryhmä, joka toimisi automaattisena käyttövaltuuksia valvovana roolina. Asiakas tilatessaan IAM-järjestelmästä tämän oikeuden, hänelle luodaan käyttövaltuus automaattisesti, jolloin asiakkaalla on pääsy järjestelmään. Pääsynhallinta aktivoituu käyttäjän kirjautuessa järjestelmään, jolloin hänen oikeutensa järjestelmän rooleihin tarkistetaan AD-tunnuksen ryhmäjäsenyyksistä.

6 PARHAAT KÄYTÄNNÖT JA STANDARDIT

Standardien määrittelyssä kuvataan termiä pääsynhallinta, jota standardien vaatimukset käsittelevät. Identiteetti ja käyttövaltuushallinta kuvataan standardeissa, vaikka sen termistö kuvataankin eri terminologian avulla. Standardeista käsitellään tärkeintä eli ISO 27001 standardia, jonka pohjalta muut standardit on luotu. (Salminen, 2022)

6.1 ISO 27001

ISO/IEC 27001 on tietoturvallisuuden hallintajärjestelmien käytetyin ja tunnustetuin standardi kansainvälisesti. Standardia käytetään kehittämään ja parantamaan organisaation tietoturvaa hallinnassa sekä tietoturvan tavoitteissa. Standardin avulla pyritään ymmärtämään, miten organisaation näkökohtia voidaan hallita, toteuttaa tälle tarvittavat valvontatoimet ja asettaa kriteerit tietoturvan parantamiselle. (DNV, n.d.)

Standardin nimi tulee sanoista ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission). Yhdessä nämä muodostavat maailmanlaajuisen organisaation, joka erikoistuu standardointiin kansainvälisesti. Ensimmäinen tietoturvastandardi julkaistiin virallisesti vuonna 1999 Britanniassa, josta myöhemmin ISO/IEC omaksui standardin erinimisenä vuonna 2000. Myöhemmin vuonna 2005 standardi sai nykyisen nimensä 27001-standardi. Standardia kehitetään, parannetaan ja uudistetaan jatkuvasti, josta viimeisin versio on vuodelta 2017. (Vetikko, 2019.)

Vaatimuksina standardille on suojata tiedon luottamuksellisuutta, eheyttä sekä saatavuutta hyvin suunnitellulla riskienhallinnan, prosessien, ohjeistuksien ja riskihallintakeinojen avulla. Itse standardi sisältää seitsemän velvoittavaa vaatimusta organisaatiolle, joista jokaisen on toteuduttuvan standardin ehtojen täyttämiseksi. Vaatimukset käsittelevät organisaation toimintaympäristöä,

suunnittelua, johtajuutta, itse toimintaa, tukitoimintoja, suorituskykyä sekä jatkuvaa vaatimuksien kehittämistyön parantamista. (Vetikko, 2019.)

Velvoittavien vaatimusten lisäksi standardi käsittelee erillisessä liitteessä A 114 hallintakeinoa, joilla valitaan riskianalyysin avulla merkittävimmät hallintakeinot toteutettavaksi. Hallintakeinot on jaoteltu neljääntoista kategoriaan. Nämä kategoriat ovat tietoturvapolitiikat, tietoturvallisuuden organisointi, henkilöstöturvallisuus, suojattavan omaisuuden hallinta, pääsynhallinta, salaus, fyysinen turvallisuus ja ympäristön turvallisuus, käyttöturvallisuus, viestintäturvallisuus, järjestelmien hankkiminen, kehittäminen ja ylläpito, suhteet toimittajiin, tietoturvahäiriöiden hallinta, liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia sekä vaatimustenmukaisuus. Standardin mukaisesti, tulee muistaa, ettei standardi käsittele yksittäistä projektia vaan toimintatapaa, jota organisaation tulee hyödyntää ja omaksua osana päivittäistä toimintaansa. (Vetikko, 2019.)

Käyttäjän tunnistautumistietoja, joita ovat muun muassa salasanat, varmennuskortit ja salausavaimet, on hallittava säännöllisesti ja muodollisesti. Tämä tulee esille esimerkiksi käyttäjän kirjautuessa ensimmäistä kertaa organisaation järjestelmään, jolloin käyttäjä voidaan pakottaa vaihtamaan oletus salasana uuteen. Tähän voidaan myös määrittää kriteereitä millainen, salasanan kuuluisi olla, salasanan vahvuutta voidaan arvioida sen pituudella, isoilla kirjaimilla, numeroilla ja erikoismerkeillä. Salasanaan voidaan myös kiinnittää aikaraja, milloin käyttäjän pitää vaihtaa salasana uudelleen. Uuden salasanan vaihdon yhteydessä on hyvä varmistaa myös käyttäjän henkilöllisyys esimerkiksi varmenteen avulla. Organisaation pitää myös laatia tästä tarkat ohjeet käyttäjälle ja varmistaa käyttäjien noudattavan näitä ohjeita. (Krapels, 2018.)

Organisaation työntekijät eivät ole staattisia, työntekijöiden roolit vaihtuvat organisaation sisällä jatkuvasti tai he vaihtavat työpaikkaa. Tämän vuoksi käyttöoikeuksien muuttamisella on jatkuva tarve. Tietovarantojen omistajien on siis syytä säännöllisesti tarkastella ja hallita käyttöoikeuksia ja kiinnittää huomiota ylläpitäjien oikeuksiin arkaluonteisuuden vuoksi. (Krapels, 2018.)

6.2 Parhaat käytännöt

Parhaita käytäntöjä identiteetti ja pääsynhallintaan on IAM-ratkaisuihin keskittyvien organisaatioiden toimesta julkaistu laajasti. Nämä ratkaisut keskittyvät laajoihin ideologioihin mihin aikaisemmin käsitellyt asetukset, lait, ohjeet, standardit ja suositukset opastavat. Parhaat käytännöt eroavat vaatimuksista niiden ollessa toteutukseen kohdistuvia tapoja. (Salminen, 2022, s. 33.)

IAM-työ on syytä aloittaa perusteellisella kartoituksella, mitä ollaan tavoittelemassa ja miten siihen päästäisiin. Ilman tavoitetilaa on vaikea havainnoida kokonaisuutta mitä projektilta vaaditaan. Korkean riskin järjestelmistä pyritään luopumaan, erityisesti legacy-järjestelmistä. Syynä on pilvipalveluiden tarjoama kattava turva tietoturvapäivitysten, salaamisen, integroinnin, segmentoinnin ja suojatun pääsyn vaatimuksien toteuttamiseen. (SailPoint, 2022.)

Identiteetin hallinnan automatisointi työsuhteen alkaessa ja päättyessä, monivaiheiden autentikoinnin käyttöönotto, säännöllinen katselmointi ja orpotilien poistaminen ovat kaikki tunnettuja tehtäviä IAM-järjestelmän keskittämisen lisäksi. Järjestelmien keskittämisellä haetaan nykyisten käyttäjien, sovellusten, tietokantojen sekä portaalien monimuotoisuutta ja koko kokonaisuuden keskittämistä yhdelle järjestelmälle, jonka takana olisi kaikkien organisaatioon kuuluvien identiteetit sekä käyttövaltuudet ja oikeudet. Ratkaisu tuo näin organisaatiolle 360 asteisen suojan ja turvallisuuden valvonnan kenellä on oikeus hallita ja päästä eri järjestelmiin ja tietokantoihin. (SailPoint, 2022.)

One Identity (n.d) lähestyy parhaita käytäntöjä lähestymällä ensin organisaation sisäisten työntekijöiden ja ulkoisten palveluiden työntekijöiden määrittämisellä ja erottamisella. Työntekijän määrittäminen organisaatiossa nopeuttaa ja parantaa IAM-tehtävien toteuttamista järjestelmän kehittyessä ja kasvaa käyttöönoton jälkeen. Tästä käytetään termiä identiteetin määrittäminen, joka tapahtuu parhaiten yhden tietokannan kautta, esimerkiksi LDAP-hakemistoa. LDAP-hakemisto (Lightweight Directory Access Protocol) perustuu kaikkien käyttäjien identiteettien varastoimista yhteen hakemistoon. Mainitaan myös

sähköposti- ja toiminnanohjausjärjestelmä ERP (Enterprise Resource Planning), joka on keskeinen organisaation toiminnan kannalta ja linkittyy suoraan IAM-ratkaisuun. Tavoitetilassa pyritään saada käyttäjä mahdollistamaan kirjautuminen kaikkiin järjestelmiin yhdellä identiteetillä eli tunnuksella. (One Identity, n.d.)

Yhtenä hyvänä käytäntönä kuvataan tietouden ja kontrollien tuottamista liiketoimintaomistajille. Käytännön toteuttamiseen suositaan itsepalvelupohjaista portaaliratkaisua, jossa liiketoimintaomistaja voi tarkastella portaalista kuka pääsee hänen vastuullaan oleviin tietovarantoihin ja järjestelmiin käsiksi. Haltijalla on täydet oikeudet muokata näitä oikeuksia ja tarvittaessa myös poistaa oikeudet työntekijältä. (One Identity, n.d.)

Kolmannen osapuolen työkaluja tulisi käyttää harkiten ja varoen. On syytä varmistua työkalujen turvallisuudesta, jotka ovat käytössä IAM-hallinnassa. Turvallisuutta voidaan lisätä monivaiheisella tunnistautumisella (MFA) sekä kertakirjautumisella (SSO), joita suositellaan käytettäväksi aina kuin vain on mahdollista. Kertakirjautumisella pystytään monitoroimaan käyttäjiä, sillä tunnuksen takana on useampi järjestelmä, mutta vain yksi identiteetti. Tästä on myös käyttäjälle turvallisuusvaikutus, sillä käyttäjän ei tarvitse muistaa kuin vain yksi tunnus ja salasana. (Katz, 2021.)

7 TIETOTURVALLISUUSVAIKUTUKSET

Tietoturvan parantaminen kohdistetaan ensimmäiseksi parantuvana asiana IAM-järjestelmän kannattavuudessa. Arkaluonteisten tietojen leviämistä rajoitetaan organisaation sisäisellä käyttövaltuushallinnalla, jonka ansiosta voidaan ehkäistä identiteettivarkauksia ja tuntemattomien henkilöiden luvatonta pääsyä järjestelmiin. IAM-järjestelmä tarjoaa alustavan suojamuurin hakkerointia, erilaisia haittaohjelmia, kalasteluita ja kyberhyökkäyksiä vastaan. Palvelun tarjoama suojaus ei silti poista asiakkaan tarvetta parantaa suojausta oman organisaationsa standardien tasolle. (Rosencrance, 2020.)

7.1 Ransomware

Ransomware on haittaohjelma, jonka tarkoituksena on estää käyttäjän pääsy tiedostoihin. Käyttäjää kiristetään tiedostojen salaamisella tai niiden julkaisemisella julkiseen verkkoon. Osana on myös tiedostojen varastaminen. Yleisimmät tavat haittaohjelmalle on sen asentaminen tiedottomasti tai tahallisesti toisen ohjelman kautta. Tiedottomasti ohjelma saatetaan ladata laitteelle sähköpostien, salaamattomien verkkosivujen, tuntemattomien lähteiden tai linkkien kautta. (Enisa, 2022, s. 9.)

Uhkan minimointiin Enisa (2022, s. 43.) esittää kymmeniä toimenpiteitä, joista kolme on suoraan sidonnainen identiteetin- ja käyttövaltuushallinnan kokonaisuuteen. IAM-järjestelmän käyttöönotto ja sen auditoiminen sisältäen vähimpien oikeuksien periaatteen ja vaarallisten yhdistelmien välttämisen. Käyttöoikeuksien ja -valtuuksien hallintaa tulisi tehdä vähimpien oikeuksien ja tehtävien erottamisen (Separation of Duties) periaatteiden mukaisesti. Luotettujen laitteiden, prosessien ja käyttäjien identiteettejä tulee hallita ja ne
tulee tarkistaa säännöllisin aikavälein. (Enisa, 2022, s. 43.)

7.2 Malware

Haittaohjelman eli malwaren tarkoitus on käyttää luvatonta ja haitallista koodia käyttäjän järjestelmän eheyden, saatavuuden tai luottamuksellisuuden vahingoittamiseen. Esimerkkinä voidaan käyttää muun muassa erilaiset virukset ja troijalaiset. (Enisa, 2022, s. 46.)

Haittaohjelma voidaan asentaa laitteelle epäluotettavien linkkien kautta, epäluotettavista lähteistä tai erillisestä USB-muistikortista. Haittaohjelmaa voidaan käyttää myös käyttäjän tietojen kaappaamiseen ja luvattomaan jakamiseen, esimerkiksi käyttäjän pankkitietojen tai henkilötietojen anastamiseen tai luvattoman roskapostin jakamiseen. Ohjelman voi havaita omalta laitteeltaan resursseja seuraamalla, sillä ohjelma käyttää käyttäjän laitteen resursseja ohjelman pyörittämiseen, mikä vaikuttaa myös laitteen toimivuuteen. Paras keino välttää haittaohjelmien asentumista on ylläpitää laitteen virustorjuntaohjelmia pitämällä ne ajan tasalla. Ja lataamalla vain luotettavista lähteistä tiedostoja laitteelle. (Kotimikro, 2022.)

7.3 Sähköpostiin liittyvät uhat

Yleisin muoto sähköpostiin liittyvissä hyökkäyksissä on tietojen kalastelu (phishing). Tavalla pyritään varastamaan sähköpostin kautta käyttäjän tietoja, yleisimpinä kohteina on salasanat ja luottokorttitiedot. Kalastelusta on myös olemassa tarkennuksia kuten keihäskalastelu (spear-fishing) sekä valaanpyynti (whaling). Keihäskalastelussa kohteeksi suunnataan organisaatio tai yksilöhenkilö. Valaanpyynnissä taas pyritään saamaan mahdollisimman vaikutusvaltaisessa asemassa oleva henkilö. (Enisa, 2022, s. 56.)

Sähköposteihin kohdistuvissa uhkissa Enisa (2022, s. 58) opastaa suositustoimenpiteinä MFA:n käyttöönoton sekä rajalliset oikeudet. Mitä rajoitetummat oikeudet käyttäjällä on tietoihin, sen vähemmän kyseiseltä käyttäjältä

pystytään anastamaan tietoja kalastelulla. Pääsynhallintaan liittyvä vahva tunnistautuminen ja vahva salasana toimii myös ennaltaehkäisevänä toimenpiteenä.

7.4 Tietoon kohdistuvat uhat

Tietoon kohdistuva uhka tarkoittaa tietovuotoa arkaluonteisen tai luottamuksellisen tiedon jakamisesta epäluotettavalle taholle. Tavoitteena on päästä käsiksi tietoihin, joita pyritään pitämään salassa. Tästä seuraa yleensä jatkotoimenpiteenä puutteellisen tiedon jakaminen tai suoraan väärän tiedon levittäminen. Väärän tiedon jakaminen voidaan jakaa myös kahteen osaan, tahattomaan (misinformaatio) ja tahalliseen väärän tiedon jakamiseen (disinformaatio). Tietomurto yleisesti tapahtuu sisäpiirissä olevan henkilön toimesta, tietojen katoamisesta tai kyberhyökkäyksen seurauksena. (Enisa, 2022, s. 61.)

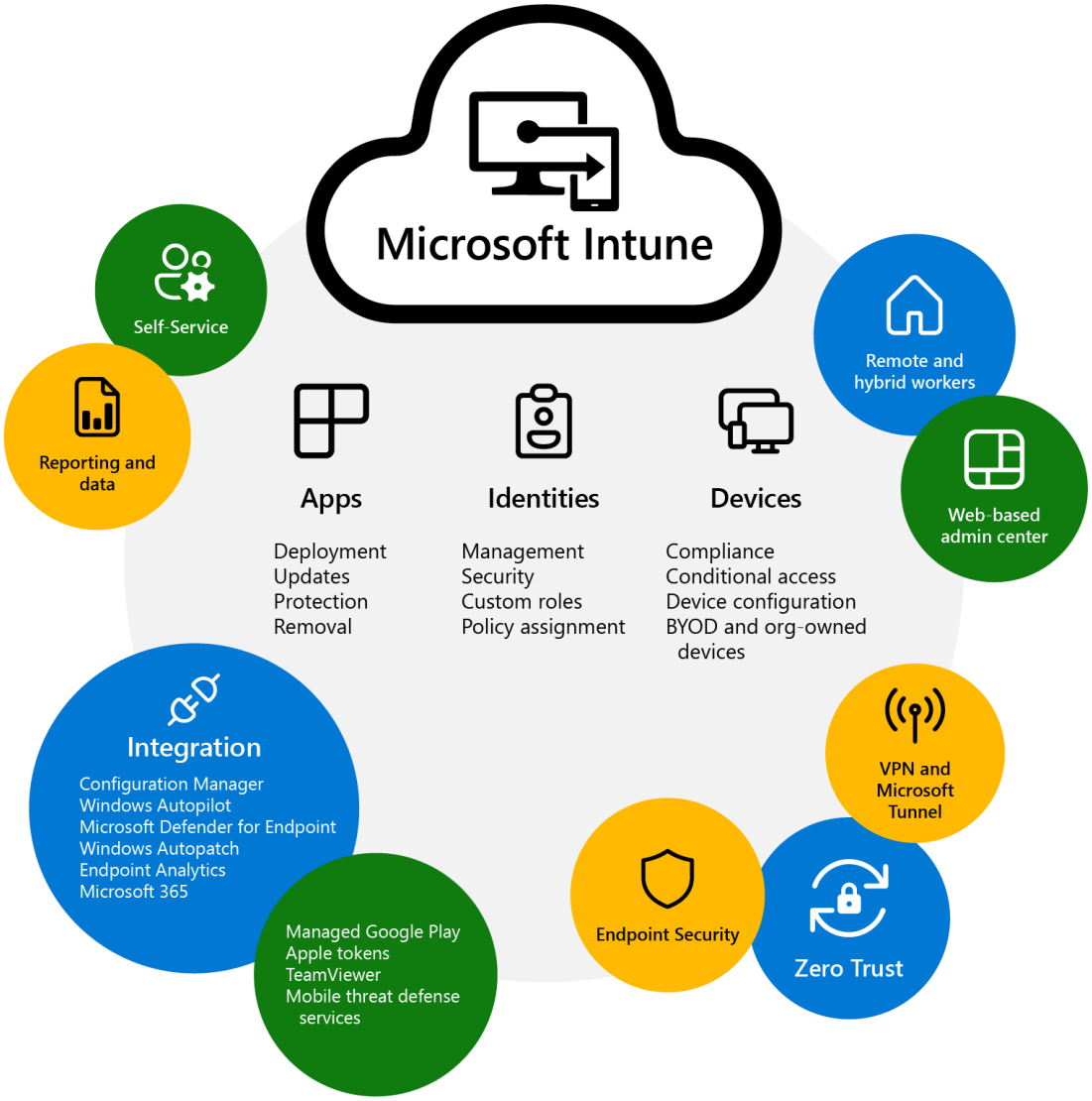
Tietoon kohdistuvien uhkien ehkäisemiseen parhaiten varaudutaan rajoitetuilla oikeuksilla. Oikeuksia tarkastellaan ja lisätään sekä poistetaan tarpeen mukaisesti, uusille työntekijöille lisätään oikeuksia ja poistuvilta työntekijöiltä poistetaan oikeudet ja jatkuvalla tarkastelulla tarkastellaan tarpeiden mukaisia oikeuksia.

8 KAUPUNGIN KÄYTTÄMIÄ JÄRJESTELMIÄ

Porin kaupungilla on lukuisia eri järjestelmiä käytössään, joilla voidaan luoda, määritellä, hallita sekä poistaa tarvittavia identiteettitietoja ja käyttövaltuustietoja. Tässä opinnäytetyössä käsitellään niistä vain osaa, joiden parissa työskentelen Porin kaupungilla henkilökohtaisesti. Tämä auttaa pitämään opinnäytetyön sisällön rajattuna ja keskittymään tutkimusongelmiin, jotka mainittiin opinnäytetyön alussa.

8.1 Microsoft Intune

Microsoft Intune on pilvipohjainen päätelaitteiden hallintajärjestelmä. Järjestelmän avulla voidaan hallita käyttäjiä, käyttäjien pääsyä sovelluksiin ja järjestelmiin, käyttäjien oikeuksia tarkastella valtuuksia sekä hallita päätelaitteita, joihin luetaan mobiililaitteet, tietokoneet ja virtuaalikoneet. Järjestelmän avulla voidaan suojata tiedostoja sekä niihin käsiksi pääseviä käyttäjiä organisaation laitteilla sekä käyttäjien henkilökohtaisilla laitteilla. Microsoft Intune käyttää Zero Trust -tietoturvamallia, mikä yksinkertaisuudessaan tarkoittaa tietoturvamallia missä ei luoteta mihinkään laitteeseen tai käyttäjään, vaan jokaiseen kirjautumiseen vaaditaan vahva tunnistautuminen organisaation internet yhteyden sisällä ja tarvittavat oikeudet ja tunnistautumiset sen ulkopuolella. (Microsoft, 2023, a.)



Kuva 1. Microsoft Intunen käyttömahdollisuudet

8.2 Microsoft Azure portaali

Azure portaali toimii verkkopohjaisena yhdistettynä konsolina, jonka avulla voidaan hallita Azuren käyttäjiä ja tilauksia. Valvoa yksinkertaisista sovelluksista monimutkaisempiin pilvipalveluihin asti. Azure portaalin avulla voidaan muun muassa valvoa tarvittavia käyttövaltuuksia ja hallita identiteettitietoja. Azure portaali on suunniteltu käyttäjäystävälliseksi, joka helpottaa organisaation toimintaa portaalin käyttöönotossa ja sen jatkuvassa käytössä. Azure portaali ei vaadi käyttäjiltä ylläpitotoimia sillä portaali on rakennettu päivittymään automaattisesti, joka vähentää palvelun tukkiutumista. (Microsoft, 2023, b.)

8.3 Efecte IGA

Eurooppalainen ohjelmistokonserni. Efecte IGA on pilviteknologiaan perustuva työkalu ITSM, ESM ja IAM palveluiden hallintaan. Efecten IGA palvelut tarjoavat asiakkailleen modernin ja helppokäyttöisen alustan, joka voidaan räätälöidä vastaamaan organisaation tarpeisiin. Efecte IGA käyttää ISO 27001 datakeskuksia Euroopassa, joka varmistaa ajan tasalla pysymisen standardien ja tietoturvaan liittyvissä muutoksissa. Järjestelmät ovat rakennettu loppukäyttäjiä ajatellen automaattisesti päivittymään ja varmuuskopioimaan, jotta järjestelmät pysyvät aina ajan tasalla. Efecte IGA:n palveluihin koostuu henkilöiden käyttövaltuuksien sekä pääsyoikeuksien varmistaminen laitteista ja sovelluksista riippumatta. (Efecte, n.d.)

9 JÄRJESTELMIEN HALLINNOINTI

Tässä kappaleessa tulemme käsittelemään miten Porin kaupunki käyttää yllä mainittuja järjestelmiä ja mihin käyttötarkoituksiin koskien identiteettitietojen ja käyttövaltuuksien hallintaa.

9.1 Microsoft Intunen hallinta ja käyttäminen

Microsoft Intunea pääsääntöisesti käytetään Porin kaupungilla laitehallintaan, niihin sisältyviin laitekohtaisiin käyttövaltuushallintaan tai sovelluksien oikeuksiin. Käyttäjien tunnuksille myönnetään oikeuksia laitekohtaisesti, joka määräytyy henkilön työn perusteella. Henkilölle voidaan myöntää jälkikäteen lisää oikeuksia, mikäli tämän työtoimenkuva sitä vaatii, mutta nämä muutokset vaativat hyväksymiset esihenkilön toimesta sekä IT-palvelun tukihenkilön puolelta. Nämä myönnetyt oikeudet pitää perustalla kirjallisesti, jotta niistä jää arkistoon merkintä. Osassa tilanteissa myönnettyjä oikeuksia myönnetään vain määräaikaiseksi, tällaisia tilanteita voivat olla koulutukset, projektit tai erilaiset testaamistilanteet.

Porin kaupunki hallinnoi näitä oikeuksia Microsoft Intunen kautta, jossa luodaan profiileja käyttäjille. Näihin profiileihin myönnetään oikeuksia, joiden avulla käyttäjät pystyvät käyttämään organisaation sisäisiä palveluita laitteissaan. Ilman näitä oikeuksia, työntekijä ei pääse kirjautumaan tunnuksillaan organisaation palveluihin. Laitteet otetaan käyttöön henkilön käyttäjätunnuksella, johon oikeudet ovat myönnetty. Tämä sitoo laitteen henkilökohtaiseksi kyseiselle käyttäjälle ja tämän jälkeen hän ei saa luovuttaa laitettaan kenellekään, joka ei ole valtuutettu laitetta käyttämään tai huoltamaan. Laitteessa on henkilön tunnukset, joilla työntekijä pääsee työnsä vaatimiin järjestelmiin. Laitteen käyttöönotossa laitteeseen tulee määrittää myös vahva salasana, joka väärin kirjoitettuna tarpeeksi monta kertaa palauttaa laitteen tehdasasetuksiin. Tämä suojaa organisaation laitteita varastamiselta ja laitteen väärinkäytöltä. Laitetta ei voida aktivoida ilman Porin kaupungin myöntämiä tunnuksia ja

oikeuksia laitteen käyttöön, sillä laite käynnistyessään ottaa automaattisesti yhteyden Intunen palvelimeen, josta se kyselee näitä oikeuksia laitteen profiiliin nimetyltä käyttäjätunnukselta.

Organisaation mobiililaitteisiin automatisoidaan asentumaan työprofiilit Intunen avulla, jonka käyttäjä aktivoi saamallaan työsähköpostiosoitteellaan, joka toimii samalla henkilön käyttäjätunnuksena. Käyttöönoton jälkeen laite on aktiivisesti yhteydessä Porin kaupungin palvelimeen, josta se kyselee muuttuneita oikeuksia ja mahdollisia päivityksiä. Laitteet ovat integroitu päivittymään automaattisesti määritettynä ajankohtana. Tämä helpottaa käyttäjien laitteen käyttöä ja ennaltaehkäisee ongelmia, jotka liittyvät sovelluksien ja järjestelmäpäivityksien yhteensopivuuksiin. Käyttäjältä vaaditaan vain oman käyttäjätunnuksensa pitämistä aktiivisena, joka tapahtuu ajastetuin aikavälein tunnuksen vahvan salasanan vaihtamisella kolmen kuukauden välein.

9.2 Microsoft Azure portaalin hallinta ja käyttäminen

Microsoft Azure portaali on verkkopohjainen konsoli, jota IT-palvelun asiantuntijat Porin kaupungilla käyttävät identiteetti ja käyttövaltuustietojen luomiseen sekä hallintaan. Porin kaupungilla on luotu omat roolit IT-palvelun asiantuntijoiden työtoimenkuvaa vastaamaan. Roolien ansiosta tietoturvaa pystytään parantamaan ja valvomaan toimintaa tehokkaammin. Jos ulkopuolinen taho pääsisi IT-palvelun asiantuntijan käyttäjällä kirjautumaan sisään, ei hän pääsisi kaikkeen mahdolliseen tietoon mitä palvelut pitävät sisällään käsiksi vaan rajoitettuihin tietoihin mihin anastetun käyttäjän roolin käyttöoikeudet riittäisivät.

Uuden käyttäjän identiteettitunnuksien luomisprosessissa luodaan käyttäjän tietojen perusteella käyttäjätunnukset, joilla uusi käyttäjä pääsee kirjautumaan laitteisiin ja ohjelmistoihin mistä hänen työtoimenkuvansa vastaa. Tämä prosessi on jaettu usealle eri roolille, joista jokainen vastaa omasta toimenkuvansa toteutumisesta. Tunnuksien luomisen hoitaa tähän erikoistunut asiantuntija, jonka jälkeen luotuun tunnukseen lisätään yksitellen tarvittavat

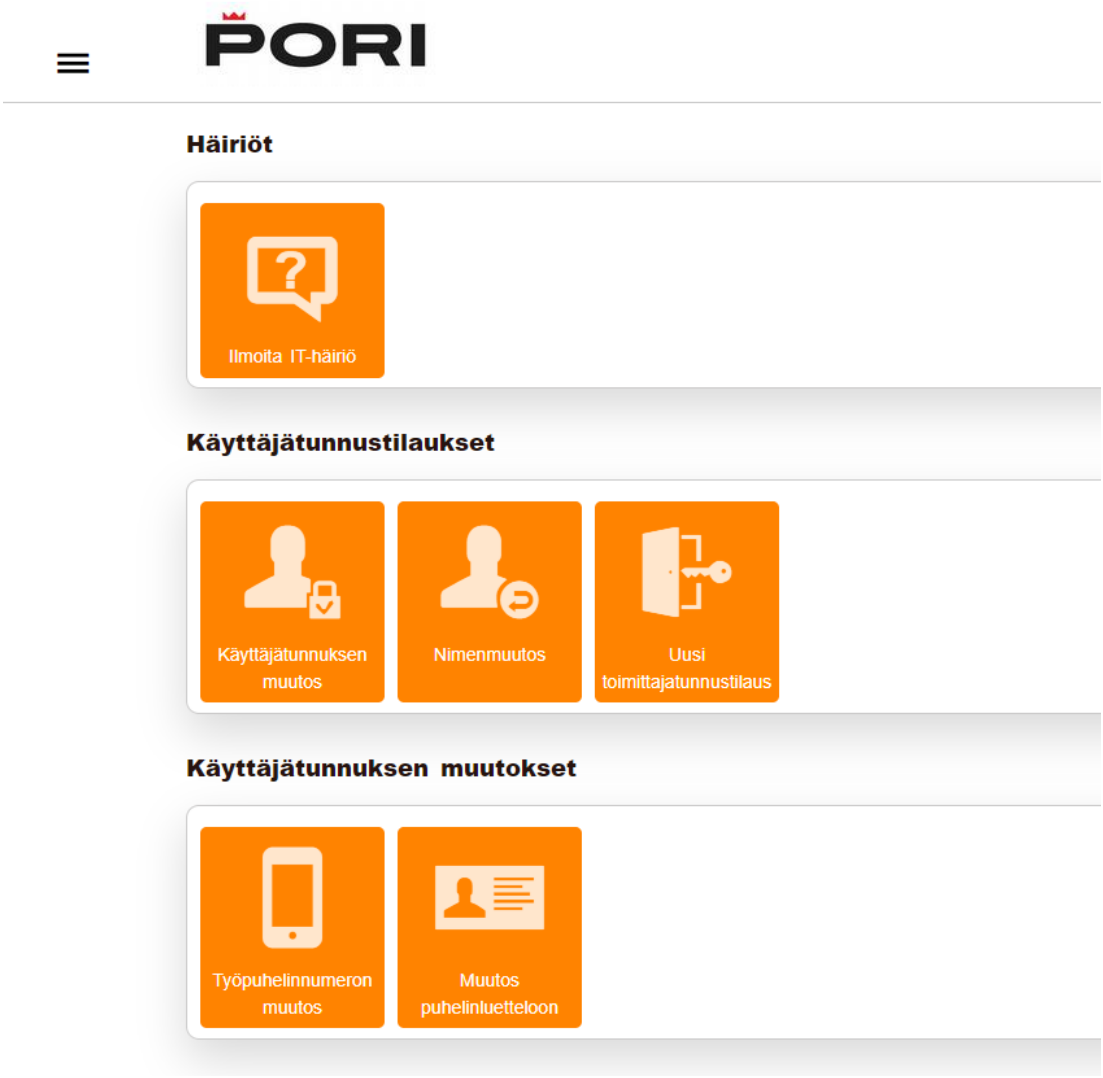
käyttövaltuusoikeudet vastaamaan työntekijän työroolia. Näihin käyttövaltuuksiin kuuluu esimerkiksi laitehallintaoikeudet, järjestelmäoikeudet, ohjelmistooikeudet sekä tarpeelliset lisenssioikeudet. Näiden oikeuksien lisäämisen hoitaa, tähän erikoistunut asiantuntija, joka vastaa kyseisestä hallinnasta.

9.3 Efecte IGA:n hallinta ja käyttäminen

Efecte IGA on suunniteltu yksinkertaiseksi loppukäyttäjälle, mikä tekee siitä loistavan työkalun Porin kaupungin käyttöön. Efecte IGA:n käyttö onkin monipuolistettu kaikille työntekijöille erilaisille rooleille.

Kaupungin ei IT-palvelun esihenkilöt käyttävät palvelua tilatakseen ICT-yksiköltä uusia tunnuksia tuleville työntekijöille tai ilmoittaakseen mahdollisista muutoksista työntekijän roolista, laitteista tai työkohteen muutoksista. Ei IT-palveluun kuuluva työntekijä käyttää palvelua ilmoittaakseen mahdollisista

ongelmista, jotka liittyvät työntekijän tunnuksiin, laitteisiin kohdistuviin ongelmiin tai tarpeellisista päivityksistä omiin tietoihinsa (liite 2).



Kuva 2. Itsepalveluportaalin näkymä IT-palvelun näkymästä.

IT-palvelun työntekijät ohjaavat nämä ongelmat oikealle ICT-tukihenkilölle, joka pyrkii käsittelemään ongelman mahdollisimman nopeasti ja suorittaa tarpeelliset ratkaisut. Näitä voidaan esimerkiksi luokitella tarpeelliset laitetilaukset, käyttäjätunnustilaukset, kirjautumisongelmat, sovellusongelmat, synkronointiongelmat ja tukipalvelu. Palvelun ratkaisut yleisesti ilmoitetaan käyttäjälle sähköpostitse, puhelimitse, itse Efecte IGA:n palvelun kautta tai asiakkaan haluamalla yhteyden otolla.

Roolituksen avulla saadaan luotua tietoturvallisempi ympäristö, minimoitua päällekkäisyyksiä ja väärin täytettyjä tietoja. Tämä auttaa organisaatiota säästämään resursseissa ja ylimääräisissä kuluissa. Tietoturvan kannalta henkilö pystyy vaikuttamaan vain roolinsa sisällettyihin oikeuksien sallimiin sisältöihin. Eli perinteinen käyttäjä pääsee vain ilmoittamaan ongelmista, virheistä tai muutoksista. Esihenkilön asemassa oleva työntekijä pystyy lähettämään tilauspyyntöjä henkilökunnan työvälineisiin ja muutoksiin tunnuksissa liittyvissä asioissa. Vain ICT-yksikön valtuutettu asiantuntija pystyy näitä muutoksia tekemään.

Efecte IGA toimii myös Porin kaupungin käytössä laitteiden integroituna palvelimena, johon pyritään kaikki Porin kaupungin hallussa ja käytössä olevat laitteet kirjaamaan ylös, niiden työtarkoitus, käyttäjät, toimipaikka, laitteen tarpeelliset tunnistetiedot ylös sekä laitteen tilaustiedot ja päivämäärät. Tämä auttaa ongelmien ratkonnassa, sillä IT-palvelun työntekijä pystyy tarkistamaan laitteen tiedot palvelusta käsin, ilman fyysistä laitteen käsittelyä. Näin voidaan myös ennalta ehkäistä tulevia ongelmia vanhentuneiden laitteiden kanssa ja vaihtaa laitteet ennen niiden tietoturvapäivityksien loppumista.

10 JÄRJESTELMIEN SEKÄ KÄYTTÄJIEN KEHITTÄMINEN

Tässä kappaleessa käsittelemme aikaisemmin mainittujen käyttöjärjestelmien ongelmia sekä miten niitä voitaisiin mahdollisesti parantaa organisaation näkökulmasta itse työtaakkaan kohdistuvissa asioissa, tietoturvan puoleisissa asioissa sekä itse organisaation resurssien hallinnan kannalta.

10.1 Efecte IGA:n kehittäminen

Efecte IGA:n itsepalveluportaalin kautta toimivia tilauslomakkeiden päivittämisellä voitaisiin ratkaista tunnuksien luomisessa syntyviä ongelmia. Lomakkeet voitaisiin päivittää vaatimaan käyttäjää täyttämään lomakkeen kaikki kyselykentät. Näitä kyselykenttiä voitaisiin jatkossa hyödyntää skriptejä käyttämällä. Skripti eli komentoriviohjelma, jolla pystyttäisiin automatisoida lomakkeiden lukeminen ja niiden sisältämien datan tallentaminen.

Datan avulla pystyttäisiin luomaan käyttäjätunnukset ilman manuaalista syöttämistä, mikä poistaisi inhimillisten virheiden syntymistä. Active Directoryn kautta voitaisiin luoda enemmän profiileja, joiden avulla järjestelmä voisi kategorioida tarvittavat käyttövaltuuksien oikeudet uusille käyttäjille ilman näiden manuaalista syöttämistä jälkikäteen. Tunnuksien olemassaoloaika määritettäisiin työsopimuksen mukaisesti ja tunnuksien voimassaoloaika sidottaisiin tunnuksen salasanvaihtojen yhteydessä aktiiviseksi. Jos käyttäjä unohtaa säännöllisesti vaihtaa tunnuksiensa salasan, tunnus menisi epäaktiiviseksi ja tämä voitaisiin uudelleen aktivoida IT-palvelun kautta tunnuksen salasan vaihtamisella.

Käyttäjätunnuksen tilauslomakkeisiin (liite 1) voitaisiin lisätä aloittavan työntekijän toimipaikka ja työpaikan nimike. Näistä tiedoista voitaisiin luoda Active Directoryn avulla lisää profiileja, joihin voitaisiin toimipaikan tai yksikön mukaisesti asettaa käyttäjälle perinteiset oikeudet, joita toimipaikallaan tarvitaan.

Työpaikan nimikkeen mukaisesti tulisi korkeammat tarkennetut oikeudet, jotka sallisivat käyttäjän pääsyn organisaation järjestelmiin.

10.2 Käyttäjien kehittäminen

Isoimpana muutoksena odotettaisiin esihenkilöiden asemassa olevien työntekijöiden aktiivisuudella. Esihenkilöt lähettäisivät tarpeelliset muutokset ja uusien työntekijöiden käyttäjätunnuspyynnöt ajoissa, jotta ruuhkaantumiselta voitaisiin välttää. Esihenkilöille tehtäisiin näistä muutoksista kirjalliset ohjeet, joita he voisivat tulevaisuudessa noudattaa. Uuden käyttäjän tunnuksien astuessa voimaan, olisi näistä käyttäjälle pidettävä perehdytys. Käyttöjärjestelmien käyttämisestä olisi syytä myös dokumentoida ohjeistukset yleiselle palvelimelle, mistä henkilökunta voisi näitä ohjeita hakea. Järjestelmiä on Porin kaupungilla useita erilaisia, jonka vuoksi niistä jokaisesta pitäisi olla vähintään yksinkertaiset ohjeet niiden käyttämiseen olemassa.

11 YHTEENVETO JA POHDINTA

Opinnäytetyön aihe, joka saatiin Porin kaupungilta. Oli minulle mielenkiintoinen ja avartava tutkimusprojekti, jonka ansiosta pääsin perehtymään Porin kaupungin käyttämiin järjestelmiin paremmin. Järjestelmien käytöistä löytyi useita ongelmia, jotka pääsääntöisesti suuntautuvat käyttäjän inhimillisten virheiden aiheuttamiksi. Löydetyistä ongelmista merkittävimpänä kohdistui käyttäjätunnuksien oikeuksien automatisointi, jonka ansiosta Porin kaupungin IT-palvelua voitaisiin kehittää nopeammaksi ja tehokkaammaksi samalla vähentäen inhimillisten virheiden synnyttämiä ongelmia.

Inhimilliset virheet, jotka syntyvät työntekijöiden kirjoitusvirheistä, väärinymmärtämisestä, huolimattomuusvirheistä tai puutteellisesta ohjeistuksesta. Aiheuttavat IT-palvelulle suurta ruuhkautumista, työtaakan kertymistä, kuluttaen henkilöresursseja sekä aikaa. Inhimillisiä virheitä ei voida eliminoida kokonaisuudessaan pois, mutta riskiä voidaan vähentää ja ennaltaehkäistä suuresti kattavalla kouluttamisella, kirjavalla ohjeistuksella sekä huolellisuudella.

Useasti nämä virheet korostuvat esihenkilön asemassa olevan työntekijän puutteellisten lomakkeiden täyttämisissä, joissa jätetään tärkeitä yksityiskohtia puuttumaan tai lomakkeen täyttämisen aikana syntyneistä kirjoitusvirheistä. Nämä ongelmat yleisesti johtavat lomakkeiden tarkasteluiden yhteydessä tietojen synkronointi ongelmiin tai puuttuvien tietojen tarpeettomien kyselyiden perään. Tämä aiheuttaa lomakkeiden käsittelyssä suurta ongelmaa operaation hidastuessaan entisyydestään, mikä vaikuttaa suuresti IT-palvelun tehokkuuteen ja toimintaan.

Opinnäytetyön tutkimus toteutettiin omien työtunnuksieni sallimien oikeuksien rajoissa, jotka sallivat minulta peruskäyttäjän oikeudet Porin kaupungin järjestelmiin. Opinnäytetyön tarkoituksena oli perehtyä identiteettiedon hallintaan, käyttövaltuushallintaan sekä tutkia Porin kaupungin olemassa olevan järjestelmän toimintaa ja löytää siihen mahdollisia kehitystoimia. Näihin tavoitteisiin mielestäni on päästy ja opinnäytetyö on ollut kokonaisuudeltaan

mielenkiintoinen projekti. Aihe on ollut ajankohtainen ja hyödyllinen itselleni tulevaisuuden urallani ja kehitystoiminnan kannalta Porin kaupungille.

Opinnäytetyön tutkittavia järjestelmiä olisi voitu avata käyttäjälle avarimmin, mutta rajoitettujen käyttöoikeuksieni myötä ei järjestelmiä päästy käsittelemään laajemmin. Uskon silti työn sisältävän kattavasti tietoa identiteettitiedon hallinnasta, käyttövaltuuksien hallinnasta sekä Porin kaupungin käytössä olevista järjestelmistä.

LÄHTEET

DNV. (n.d). ISO/IEC 27001 - tietoturvallisuuden hallintajärjestelmä. Haettu 8.1.2023 osoitteesta https://www.dnv.fi/services/iso-iec-27001-tietoturvallisuuden-hallintajarjestelma-3327?gclid=CjwKCAiAh9qdBhAOEiwA-vxIok_1mAh52m3n8ujVBTPvePDEgsYyJhbVuvPr-Dxy-PITqkkwd1QGS59hoC0xQQAvD_BwE

Efecte. (n.d). Pilvipohjaista Palvelunhallintaa. Haettu 30.4.2023 osoitteesta https://www.efecte.com/fi/palvelunhallinnan-alusta

Enisa. (2022). Enisa Threat Landscape 2022. PDF-dokumentti. Päivitetty 3.11.2022. Haettu 13.1.2023 osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Hakala, H., Vainio, M. & Vuorinen, O. (2006). Tietoturvallisuuden käsikirja. Docendo.

Itewiki. (n.d). Master Data Management (MDM). Haettu 29.4.2023 osoitteesta https://www.itewiki.fi/opas/master-data-management-mdm/

Kasanen, H. (2010). Keskitetty identiteetinhallinta, referenssiarkkitehtuuri. Haettu 28.12.2022 osoitteesta https://www.slideshare.net/hannuk/idmreferenssiarkkitehtuuri

Katz, E. (28.6.2021). Top 5 Identity and Access Management Best Practices for DevSecOps. Haettu 10.1.2023 osoitteesta https://spectralops.io/blog/top-5-identity-and-access-management-best-practices-for-devsecops/

Kotimikro. (2022). Mitä on malware. Haettu 20.1.2022 osoitteesta https://kotimikro.fi/tietoturva/haittaohjelmat/mita-on-malware

Krapels, J. (22.6.2018). ISO27002 explained, part 2. Haettu 9.1.2023 osoitteesta https://ictinstitute.nl/iso27002-explained-part-2/

Kuntaliitto. (2013). Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri. PDF dokumentti. Haettu 10.1.2023 osoitteesta https://www.kuntaliitto.fi/sites/default/files/media/file/Kuntasektorin%20k%C3%A4ytt%C3%B6valtuushallinnan%20viitearkkitehtuuri.pdf

Microsoft. (3.4.2023.a) Microsoft Intune securely manages identities, manages apps, and manages devices. Haettu 28.4.2023 osoitteesta https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft. (13.9.2022.b) What is the Azure portal? Haettu 28.4.2023 osoitteesta https://learn.microsoft.com/en-us/azure/azure-portal/azure-portal-overview

Niemi, K. (n.d) Identiteetin ja pääsynhallinta (IAM). Haettu 6.12.2022 osoitteesta https://www.itewiki.fi/opas/kayttajahallinta-iam/

One Identity. (n.d). 8 Best Practices for Identity and Access Management. Haettu 13.1.2023 osoitteesta https://www.oneidentity.com/mx-es/whitepaper/8-best-practices-for-identity-and-access-management827122/

OpiTietosuojaa. (n.d). Käyttövaltuusperiaatteet. Haettu 7.12.2022 osoitteesta https://opitietosuojaa.fi/index.php/fi/lainsaeaedaentoe/49-tyokalupakki/periaatteet-politiikat-ja-suunnitelmat/52-kayttovaltuusperiaatteet

Pori. (2022). Pori-tieto. Haettu 2.5.2023 osoitteesta https://www.pori.fi/kaupunki-ja-hallinto/pori-tieto/

Rosencrance, L. (23.11.2020). 7 Reasons Identity and Access Management Is Important. Haettu 9.1.2023 osoitteesta https://www.techtarget.com/whatis/8-Reasons-Identity-and-Access-Management-Is-Important

SailPoint. (2022). 7 Best Practices for Identity Security. Haettu 12.1.2023 osoitteesta https://www.sailpoint.com/identity-library/7-best-practices-for-identity-security/

Salminen, T. (2022). Identiteetin- ja käyttövaltuushallinnan kehittäminen Sipoon kunnassa. Kaakkois-Suomen ammattikorkeakoulu. Kyberturvallisuuden koulutus. Opinnäytetyö. Haettu 20.1.2023 osoitteesta https://www.theseus.fi/bitstream/handle/10024/747649/Teppo%20Salminen%20Opinn%c3%a4ytety%c3%b6_final.pdf?isAllowed=y&sequence=2

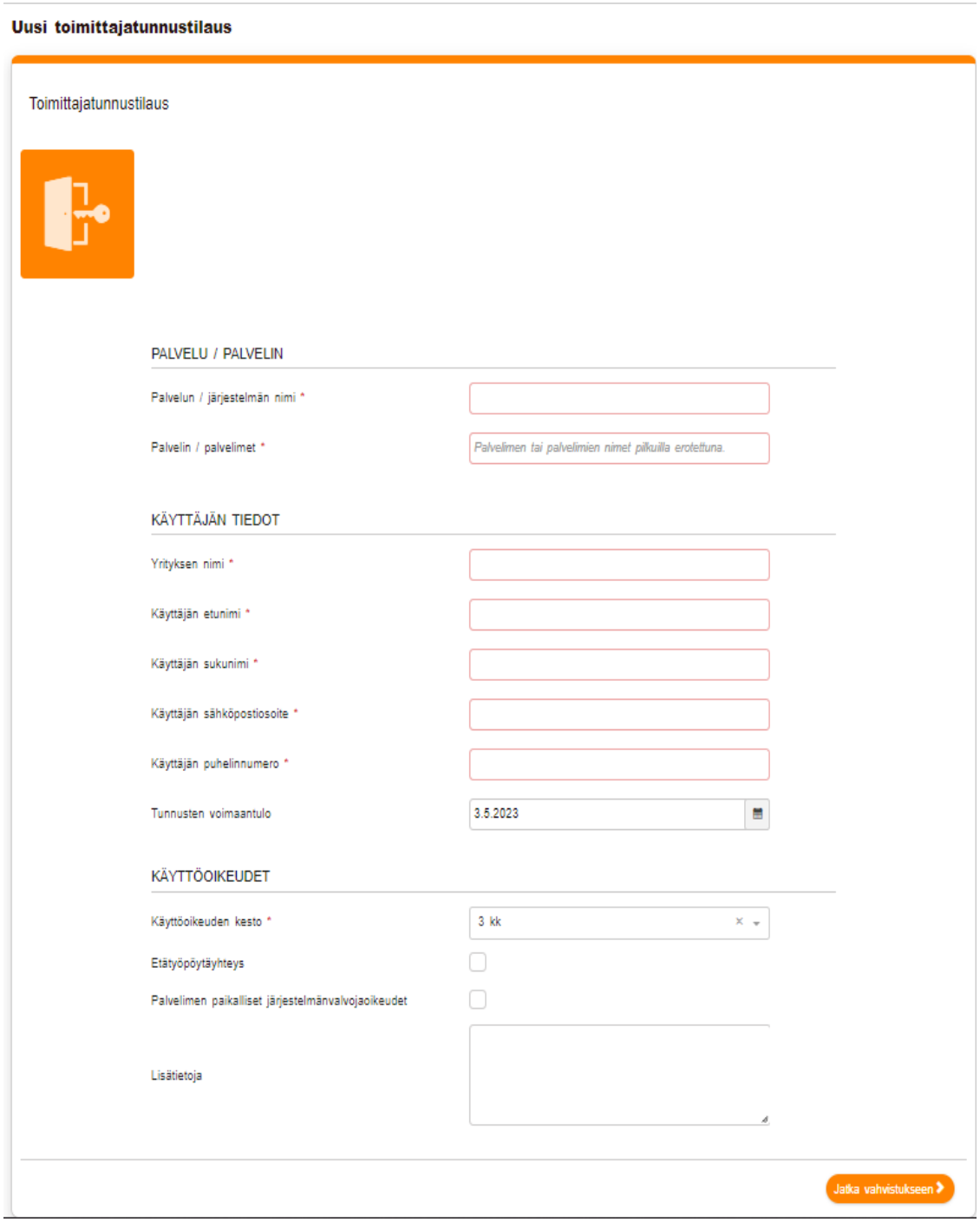
Turunen, T. (2018). Kyberturvallisuuden hallintamallin kehittäminen. Kaakkois-Suomen ammattikorkeakoulu. Teknologiaosaamisen johtaminen. Opin-näytetyö. Haettu 9.1.2023 osoitteesta https://urn.fi/URN:NBN:fi:amk-2018101616032

Ulkoministeriö. (2020). Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Traficomin julkaisusarja 232/2020. PDF-dokumentti. Haettu 13.1.2023 osoitteesta https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf

Valtiovarainministeriö. (2006). Käyttövaltuushallinnan periaatteet ja hyvät käytännöt. PDF-dokumentti. Haettu 11.1.2023 osoitteesta https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_9_2006.pdf

Vetikko, P. (18.1.2019). Mikä on ISO 27001 -standardi? Haettu 10.1.2023 osoitteesta https://www.insta.fi/nakemyksia/tietoturvapalvelut/mika-on-iso-27001-standardi

LIITE 1: KÄYTTÄJÄTUNNUKSEN TILAUSLOMAKE



LIITE 2: ITSEPALVELUPORTAALIN IT-HÄIRIÖ LOMAKE