Laura Lehtiö

Pääsyoikeuksien hallinnan tukeminen säännöllisellä katselmoinnilla

Tieto- ja ohjelmistotekniikan kandidaatintutkielma

20. joulukuuta 2024

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Laura Lehtiö

Yhteystiedot: laura.l.lehtio@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Pääsyoikeuksien hallinnan tukeminen säännöllisellä katselmoinnilla

Title in English: Supporting access management through regular access reviews

Työ: Kandidaatintutkielma

Sivumäärä: 31+0

Tiivistelmä: Pääsyoikeuksien hallintaa voidaan toteuttaa monilla eri malleilla ja niiden yhdistelmillä, mutta ilman säännöllisiä katselmointeja hallinnan malliin voi jäädä aukkoja. Nämä puutteet voivat pahimmillaan johtaa vakaviin seurauksiin, kuten liiketoiminnan keskeytymiseen tai taloudellisiin tappioihin. Tämä tutkielma käsittelee pääsyoikeuksien hallinnan tukemista säännöllisillä pääsyoikeuksien katselmoinneilla. Katselmoinnin on tunnistettu tukevan pääsyoikeuksien hallinnan vahvistamista ja auttavan muun muassa ylimääräisten pääsyoikeuksien tunnistamisessa ja vähimmäisoikeuksien periaatteen noudattamisessa, vaikka lisätutkimusta aiheesta kaivataan.

Avainsanat: pääsyoikeuksien hallinta, pääsyoikeuksien katselmointi, tietoturvariski

Abstract: Access management can be implemented using various models and their combinations, but without regular reviews, gaps may emerge in the management framework. These deficiencies can, at worst, lead to serious consequences, such as business interruptions or financial losses. This study examines how access management can be supported through regular access reviews. Although research on the topic is limited, the findings indicate that reviews help identify excessive access rights and ensure compliance with the principle of least privilege.

Keywords: access management, access review, security risk

Termiluettelo

IAM	Identiteetin- ja pääsyoikeuksien hallinta (engl. *Identity and Access Management*).
MAC	Pakollinen pääsyoikeuksien hallinta (engl. *Mandatory Access Control*).
DAC	Harkinnanvarainen pääsyoikeuksien hallinta (engl. *Discretionary Access Control*).
RBAC	Roolipohjainen pääsyoikeuksien hallinta (engl. *Role-based Access Control*).
ABAC	Attribuuttipohjainen pääsyoikeuksien hallinta (engl. *Attribute-based Access Control*).
PBAC	Sääntöpohjainen pääsyoikeuksien hallinta (engl. *Policy-based Access Control*).

Kuviot

Taulukot

Sisällys

1 Johdanto

Tietojärjestelmien monimutkaistumisen ja tietoturvariskien kasvamisen myötä organisaatioiden tarve hallita työntekijöiden, kumppaneiden ja muiden sidosryhmien pääsyä tietojärjestelmiin on kasvanut. Identiteetin- ja pääsynhallinta (engl. *Identity and Access Management*, IAM) on noussut keskeiseksi modernin IT-organisaation osaksi, tarjoten keinoja vastata pääsyoikeuksien hallintaan liittyviin tietoturvahaasteisiin (Kunz ym. 2019).

Pääsyoikeuksien hallinnan (engl. *Access Controls*) tavoitteena on varmistaa, että organisaation resurssien pääsyoikeudet ovat asianmukaisesti rajattu ja hallinnoitu. Laadukas hallinta on kriittistä, sillä heikko hallinta voi johtaa ylimääräisiin ja hallinnoimattomiin pääsyoikeuksiin, tietovuotoihin ja jopa mainehaittoihin (Baracaldo ja Joshi 2013). Kuten yhdysvaltalaisen Capital One -pankin (2019) tietovuoto osoittaa, hallitsemattomat pääsyoikeudet ovat erittäin riskialttiita, sillä ne voivat avata hyökkääjille pääsyn arkaluontoisiin ja kriittisiin tietoihin. Tapauksen seurauksena noin 100 miljoonan yhdysvaltalaisen ja 6 miljoonan kanadalaisen henkilökohtaiset tiedot vaarantuivat ja noin 140 000 sosiaaliturvatunnusta päätyi vuodon aiheuttajan käsiin (Capital One 2019). Tietovuodon laajuus vahvistaa sitä, että ylimääräisillä pääsyoikeuksilla ja heikolla pääsyoikeuksien hallinnalla voi olla laajoja negatiivisia seurauksia.

Baumerin ym. (2024) mukaan pääsyoikeuksien hallintaa voidaan vahvistaa säännöllisellä pääsyoikeuksien katselmoinnilla. Tässä tutkielmassa tarkastellaan, miten pääsyoikeuksien katselmoinnilla (engl. *Access Review*) voidaan vahvistaa pääsyoikeuksien hallintaa ja vähentää siihen liittyviä tietoturvariskejä. Tutkielma jakautuu seuraavasti: toisessa luvussa määritellään pääsyoikeuksien hallinta, esitellään yleisimmät hallinnan mallit ja hallintaan liittyvät haasteet. Kolmannessa luvussa perehdytään pääsyoikeuksien katselmoinnin prosessiin, haasteisiin ja hyviin käytäntöihin sekä tutkitaan, miten katselmoinnilla voidaan tukea pääsyoikeuksien hallintaa. Viimeisessä luvussa koostetaan yhteenveto tutkielman havainnoista ja hahmotellaan suuntia sekä pääsyoikeuksien katselmoinnin kehittämiselle että tulevaisuuden tutkimuksille.

2 Pääsyoikeuksien hallinta

Pääsyoikeuksien hallinta on olennainen osa organisaation tietoturvaa (Kern ym. 2022). Tässä luvussa tarkastellaan siihen liittyviä käsitteitä ja hallinnan merkitystä. Näiden lisäksi luvussa esitellään keskeisiä pääsyoikeuksien hallintamalleja ja selvitetään, miten esiteltyjä malleja voidaan yhdistellä, jotta pääsyoikeuksien hallinta vastaa modernien tietojärjestelmien tarpeita. Luvun lopussa syvennytään vielä pääsyoikeuksien hallintaan liittyviin haasteisiin sekä niiden negatiivisiin vaikutuksiin.

2.1 Pääsyoikeuksien hallinnan käsitteet ja merkitys

Englanninkielinen termi 'access control' on suomennettu Valtionhallinnon tietoturvasanastossa pääsynhallinnaksi (Vahti 2008). Pääsynhallinta on moniulotteinen käsite, joka kattaa pääsyoikeuksien hallinnan lisäksi pääsynvalvonnan ja -valtuutuksen prosessit. Koska tämä tutkielma keskittyy pääsyoikeuksien valvontaan ja niiden katselmointiin, käytetään tutkielmassa käsitteenä pääsyoikeuksien hallintaa. Tutkielmaan valittu käsite kuvaa pääsynhallintaa tarkemmin pääsyoikeuksiin liittyvää hallintaa.

Wein ja Jarzabekin (1998) mukaan pääsyoikeuksien hallinta perustuu autentikointiin (engl. *authentication*) ja auktorisointiin (engl. *authorization*). Heidän mukaansa käyttäjän identiteetti varmistetaan ennen pääsyn myöntämistä, jonka jälkeen auktorisointi määrittää, mihin resursseihin käyttäjä saa pääsyn (Wei ja Jarzabek 1998). Näiden menetelmien tarkoituksena on varmistaa, että vain valtuutetut käyttäjät voivat käyttää heille rajattuja resursseja (Aftab ym. 2022). Samaratin ja Vimercatin (2001) mukaan käyttäjällä voidaan tarkoittaa ihmistä, konetta tai ohjelman osaa. Tässä tutkielmassa käyttäjällä viitataan kuitenkin vain ihmiseen, sillä tutkielma käsittelee pääsyoikeuksien hallintaa ja katselmointia ihmiskäyttäjien osalta.

Pääsyoikeuksien hallinnan tavoitteena on noudattaa vähimmäisoikeuksien periaatetta (engl. *Least privilege*), jonka mukaan käyttäjälle myönnetään vain ne oikeudet, jotka ovat välttämättömiä hänen tehtäviensä suorittamiseen (Samarati ja Vimercati 2001). Tämän periaatteen lisäksi pääsyoikeuksien hallintaa ohjaavat erilaiset tietoturvan parantamiseen pyrkivät säädökset, lait ja organisaation sisäiset ohjeet (Samarati ja Vimercati 2001). Kansainväliset

standardit, kuten NIST (2020), korostavat pääsyoikeuksien hallinnan merkitystä tietojärjestelmien turvallisuuden parantamisessa ja niihin liittyvien riskien ehkäisyssä.

Kuten aiemmin todettiin, pääsyoikeuksien hallinta on kriittinen osa organisaation tietoturvaa. Sandhu ja Samarati (1994) mukaan pääsyoikeuksien hallinta ei kuitenkaan ole yksinään riittävä turvatoimi, vaan sitä tulee täydentää säännöllisesti toteutettavalla pääsyoikeuksien katselmoinnilla. Myös Kern ym. (2022) painottavat, että hallintaa voidaan vahvistaa katselmoinneilla, jota käsitellään luvussa 3.

2.2 Pääsyoikeuksien hallinnan mallit

Oikean pääsyoikeuksien hallinnan mallin valinta on tärkeää, sillä väärin valittu malli voi altistaa järjestelmän erilaisille tietoturvariskeille. Zhaon ja Johnsonin (2010) tutkimuksessa huomattiin, että joustavan pääsyoikeuksien hallinnan valitseminen voi tarjota organisaatiolle taloudellisia kilpailuetuja ja helpottaa esimerkiksi sairaalaolosuhteissa yllättäviin tilanteisiin reagointia. Toisaalta tutkimuksessa havaittiin myös, että tiukempi pääsyoikeuksien hallinta parantaa tietoturvaa ja ehkäisee tiedon väärinkäyttöä (Zhao ja Johnson 2010). Näiden syiden takia on tärkeää, että organisaation tietoturvan ja joustavuuden tarpeet huomioidaan hallintaa suunnitellessa.

Pääsyoikeuksien hallinnan malleja on paljon, ja uusia kehitetään jatkuvasti vastaamaan modernien järjestelmien ja organisaatioiden tarpeita. Vanhimpia malleja ovat pakollinen (engl. *Mandatory Access Control*, MAC) ja harkinnanvarainen pääsyoikeuksien hallinta (engl. *Discretionary Access Control*, DAC), jotka määriteltiin ensimmäisen kerran Yhdysvaltain puolustusministeriön julkaisemassa Trusted Computer System Evaluation Criteria -dokumentissa (1985).

Tiedeyhteisö ei ole yksimielinen pääsyoikeuksien hallinnan mallien luokittelusta. Samaratin ja Vimercatin (2001) ja Xunin ym. (2022) mukaan pääsyoikeuksien hallinnan mallien päätyyppejä ovat MAC- ja DAC-mallien lisäksi roolipohjoinen pääsyoikeuksien hallinta (engl. *Role-Based Access Control*, RBAC). Aftab ym. (2022) lisää päätyyppeihin edellä mainittujen lisäksi myös attribuuttipohjaisen pääsyoikeuksien hallinnan (engl. *Attribute-Based Access Control*, ABAC).

Aftabin ym. (2022) tutkimus esittelee aiemmin esiteltyjen mallien lisäksi perinteisen RBAC-mallin pohjalta kehitettyjä hybridimalleja. Kukreti (2022) ei käytä hybridimalli-termiä, mutta esittelee muun muassa sääntöpohjaisen pääsyoikeuksien hallinnan (engl. *Policy-Based Access Control*, PBAC). Kuten tutkimuksista voidaan huomata, erilaisia pääsyoikeuksien malleja on paljon, eikä tiedeyhteisö ole yksimielinen niiden ryhmittelystä (Aftab ym. 2022; Kukreti 2022; Samarati ja Vimercati 2001). Tästä syystä tässä tutkielmassa ei tulla luokittelemaan malleja pää- ja hybridimalleihin, vaan keskitytään MAC-, DAC-, RBAC-, ABAC- ja PBAC-malleihin.

2.2.1 Pakollinen pääsyoikeuksien hallinta

Kuten aiemmin todettiin, pakollinen pääsyoikeuksien hallinta on yksi vanhimmista malleista. Se perustuu ennalta määritettyihin turvamäärityksiin ja -luokituksiin, jotka määritellään käyttäjille ja resursseille (Kukreti 2022). Mallissa käyttäjä saa resurssin pääsyoikeuden vain, jos hänen turvamäärityksensä ja -luokituksensa täyttävät resurssin vaatimukset (Kim ym. 2014). MacLennanin ja Zhangin (2024) mukaan MAC-mallissa järjestelmänvalvoja hallitsee pääsyoikeuspolitiikkoja, eivätkä käyttäjät pysty ohittamaan niitä.

Tiukkojen, ennalta määriteltyjen tietoturvaluokitusten takia malli on turvallinen, mutta rakenteeltaan joustamaton (MacLennan ja Zhang 2024). Jäykän rakenteen takia MAC-malli sopii Fanin ym. (2009) mukaan turvallisuusjärjestelmiin, joissa tietoturva on kriittistä ja tietojen arkaluonteisuus edellyttää tiukkaa pääsyoikeuksien hallintaa. Tällaisia järjestelmiä ovat esimerkiksi hallinto- ja sotilasjärjestelmät (Sandhu ja Samarati 1994; Aftab ym. 2022)

MacLennanin ja Zhangin 2024 mukaan MAC-mallin politiikkojen päivittäminen edellyttää aina prosessin keskeyttämistä, mikä heikentää mallin kykyä reagoida muuttuviin tietoturvauhkiin ja tekee mallista staattisen. Dynaamisuuden puutteen lisäksi malliin liittyy skaalautuvuuden ja hallinnan haasteita (Aftab ym. 2022). Aftab ym. (2022) lisäävät myös, ettei malli tue vähimmäisoikeuksien periaatetta.

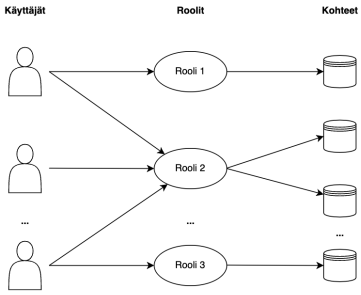
2.2.2 Harkinnanvarainen pääsyoikeuksien hallinta

Harkinnanvarainen pääsyoikeuksien hallinnan malli perustuu resurssin omistajan hallitsemiin pääsyoikeuksiin (Ahn 2018). Tässä yhteydessä resurssin omistajalla tarkoitetaan käyttäjää, joka on joko luonut tai saanut resurssiin oikeudet. DAC-mallissa resurssin omistajalla on oikeus muokata ja jakaa omistamaansa resurssiin liittyviä oikeuksia muille käyttäjille (Ahn 2018). Tämä oikeuksien hallinnointi tekee mallista joustavan, jonka takia sitä käytetään sekä kaupallisissa että teollisissa ympäristöissä (Sandhu ja Samarati 1994). Aftabin ym. (2022) mukaan DAC-mallia hyödynnetään muun muassa verkkosovelluksissa ja käyttöjärjestelmissä, kuten Linuxissa ja Unixissa.

Vaikka käyttäjälle myönnetty pääsyoikeus tarkistetaan ennen pääsyn vahvistamista ennalta määriteltyjen sääntöjen perusteella, liittyy DAC-malliin tietoturvahaasteita (Sandhu ja Samarati 1994). Mallin harkinnanvaraiset pääsyoikeudet vaikeuttavat organisaation sisäisen informaation seuraamista, mikä tekee tiedon turvaamisesta ja sen jakamisen rajoittamisesta haastavaa (Ahn 2018). Informaation ja pääsyoikeuksien helppo jakaminen tekee mallista alttiin muun muassa tietovuodoille, tiedon väärinkäytölle ja haittaohjelmille, kuten Troijan hevosille (Sandhu ja Samarati 1994). Näiden lisäksi malli ei tue vähimmäisoikeuksien periaatetta (Aftab ym. 2022).

2.2.3 Roolipohjainen pääsyoikeuksien hallinta

Roolipohjainen pääsyoikeuksien hallinta perustuu rooleille määritettyihin pääsyoikeuksiin, jotka periytyvät käyttäjille, joille rooli myönnetään (Kukreti 2022). Longin ja Yanin (2019) mukaan mallissa käytetyt roolit voivat olla organisaatiorooleja, jolloin ne jäljittelevät organisaation rakenteita. Kuten kaaviosta 1 ilmenee, käyttäjällä voi olla useita rooleja, joiden perusteella hänen pääsyoikeutensa määräytyvät. Samanaikaisia rooleja voivat olla esimerkiksi esimies- ja työntekijäroolit, jolloin käyttäjälle myönnetään molempiin rooleihin liitetyt oikeudet. Toisin sanoen RBAC-mallissa pääsyoikeudet liitetään rooleihin, ja roolit myönnetään käyttäjille, mikä mahdollistaa käyttäjien pääsyoikeuksien tehokkaan hallinnan (Samarati ja Vimercati 2001). Lisäksi pääsyoikeuksien hallintaa voidaan tehostaa roolihierarkian avulla, jossa ylemmät roolit perivät alempien tasojen roolien oikeuksia (Bertino 2003).



Kuvio 1. RBAC-mallin pääsyoikeuksien määräytyminen (Samarati ja Vimercati 2001)

RBAC-malli tarjoaa skaalautuvan pääsyoikeuksien hallinnan (Kukreti 2022) ja tekee siitä helpommin hallittavan (Bertino 2003; Shi, Sun ja Yuan 2008), sillä yksittäisten käyttäjien sijaan riittää hallita rooleja ja niihin liitettyjä oikeuksia (Kukreti 2022). Longin ja Yanin (2019) mukaan organisaatioroolien käyttäminen tekee RBAC-mallista loogisen, intuitiivisen ja helposti hallittavan. Hallinnan yksinkertaistuminen voi Shi, Sun ja Yuan (2008) myös laskea pääsyoikeuksien hallintaan liittyviä kuluja ja ajankäyttöä. Malli tukee vähimmäisoikeuksien periaatetta, sillä rooleille myönnetään vain välttämättömät oikeudet ja käyttäjille annetaan mahdollisimman vähän rooleja (Aftab ym. 2022). Aftabin ym. (2022) mukaan RBAC on käytössä muun muassa pankki- ja koulutusjärjestelmissä.

Sekä Long ja Yan (2019) että Puchta, Böhm ja Pernul (2019) korostavat, että RBAC-mallin keskeiset haasteet liittyvät roolien määrän kasvuun. Tämä kasvu vaikeuttaa roolien, roolihierarkioiden ja pääsyoikeuksien hallintaa, ja heikentää mallin tehokkuutta (Puchta, Böhm ja Pernul 2019). Roolien määrän lisäksi mallin haasteena on Shinin, Sunin ja Yuanin (2008) mukaan roolihierarkiaan liittyvä oikeuksien perintä. Heidän mukaansa hierarkia voi johtaa oikeuksien päällekkäisyyksiin ja ylimääräisten oikeuksien periytymiseen (Shi, Sun ja Yuan 2008). Näiden haasteiden lisäksi Longin ja Yanin (2019) mukaan mallissa roolien ja käyttäjien väliset suhteet ovat staattisia eivätkä ne huomioi ympäristön muutoksia. Myös Aftab ym. (2022) korostaa, ettei malli ole dynaaminen.

2.2.4 Attribuuttipohjainen pääsyoikeuksien hallinta

Kuten aiemmin kerrottiin, RBAC-mallin käyttö voi johtaa roolien määrän kasvuun. Tähän ongelmaan Kunz ym. (2019) tarjoavat ratkaisuksi attribuuttipohjaista pääsyoikeuksien hallintaa, joka Longin ja Yanin (2019) mukaan laajentaa perinteistä RBAC-mallia.

ABAC-malli perustuu käyttäjää, kohteen ominaisuuksia ja ympäristöä kuvaaviin attribuutteihin (Pal ym. 2019), jotka voidaan Shenin ja Hongin (2006) mukaan jakaa aihe-, resurssi- ja ympäristöattribuutteihin. Heidän mukaansa aiheattribuutit ovat attribuutteja, jotka kertovat käyttäjän ominaisuuksista, kuten organisaatioroolista ja IP-osoitteesta. Resurssiattribuutit puolestaan kertovat resurssin ominaisuuksista, kuten sen identiteetistä, sijainnista ja koosta. Ympäristöattribuuteilla taasen tarkoitetaan ympäristöön ja tilaan liittyviä attribuutteja, joita voivat olla esimerkiksi kellonaika, päivämäärä ja systeemin tila (Shen ja Hong 2006).

Xu ym. (2022), Kunz ym. (2019) ja Aftab ym. (2022) ovat yksimielisiä siitä, että ABAC-malli on aiemmin tässä tutkielmassa esiteltyjä pääsyoikeuksien hallinnan malleja dynaamisempi ja hienojakoisempi. Mallissa pääsyoikeuksien myöntäminen perustuu roolien sijaan laajempaan attribuuttien kokonaisuuteen, jonka takia malli tukee vähimmäisoikeuksien periaatetta paremmin, kuin aikaisemmin esitelty RBAC-malli (Kunz ym. 2019) ja tekee hallinnasta skaalautuvamman (Shen ja Hong 2006). Attribuuttien käyttäminen madaltaa myös pääsyoikeuksien hallintaan liittyviä kustannuksia, sillä niiden takia hallinta vaatii RBAC-mallia vähemmän poliitikkoja (engl. *policy*) (Long ja Yan 2019). Näiden ominaisuuksien takia ABAC-malli sopii IoT- ja pilviympäristöihin, jotka vaativat pääsyoikeuksien hallinnalta joustavuutta laajan käyttäjämäärän ja resurssien takia (Xu ym. 2022). Mallia käytetään myös muun muassa vakuutus-, lentoliikenne- ja telekommunikaatiojärjestelmissä (Aftab ym. 2022).

Vaikka ABAC-malli tarjoaa Kunzin ym. (2019) mukaan monissa tapauksissa aiemmin esiteltyjä malleja tehokkaamman ratkaisun, liittyy siihenkin haasteita. Longin ja Yanin (2019) tutkimuksessa havaittiin, että ABAC-mallin käyttö voi johtaa pääsyoikeuksien hallintaan liittyvien sääntöjen ja attribuuttien määrän kasvuun, joka voi Xu ym. (2022) mukaan heikentää mallin tehokkuutta attribuutteja hakevien algoritmien hidastuessa.

2.2.5 Sääntöpohjainen pääsyoikeuksien hallinta

Sääntöpohjainen pääsyoikeuksien hallinta on pääsyoikeuksien hallintamalli, jossa pääsyoikeudet määritellään ennalta määriteltyjen sääntöjen ja ehtojen avulla (Pal ym. 2019). Zhin ym. (2009) mukaan mallin keskiössä on sessio eli tilanne, jossa käyttäjä suorittaa tietyn toimenpiteen kohteelle. Mallissa sessioihin liittyviä pääsyoikeuksia voidaan rajoittaa olosuhteiden tarpeiden mukaan, sillä malli käyttää attribuutteja kuvaamaan ABAC-mallista poiketen käyttäjän lisäksi myös kohdetta ja ympäristöä (Zhi ym. 2009). Zhin ym. (2009) mielestä kuvailevammat attribuutit tekevät mallista aiemmin esiteltyjä malleja joustavamman.

Zhin ym. (2009) mukaan PBAC-mallin politiikka koostuu subjektista, kohteesta, toiminnosta, ehdosta ja totuusarvosta ja mallin merkittävin etu onkin heidän mukaansa se, että PBAC-malli kykenee käsittelemään samanaikaisesti useampia politikkoja. Useamman politiikan samanaikaisen käytön takia malli sopii monimutkaisiin pääsyoikeustilanteisiin. Pal ym. (2019) esittävät, että PBAC-malli sopii muun muassa terveydenhuollon kaltaisiin kriittisiin ympäristöihin, sillä malli on joustava ja se kykenee attribuuttiensa takia mukautumaan tehokkaasti ympäristön vaatimuksiin.

2.3 Pääsyoikeuksien hallinnan mallien yhdistäminen

Samaratin ja Vimercatin (2001) mukaan organisaation tietoturvakäytäntöjen tulkinta selkeäksi ja kokonaisvaltaiseksi pääsyoikeuksien hallinnan malliksi on haastavaa. Alaluvussa 2.2 esitellyt pääsyoikeuksien hallinnan mallit on kerätty taulukkoon 1. Kuten taulukosta 1 voidaan huomata, pääsyoikeuksien hallinnan malleilla on erilaisia heikkouksia, jotka voivat aiheuttaa tietoturvaongelmia ja heikentää hallinnan tehokkuutta. Näitä haasteita voidaan yrittää vähentää erilaisten mallien yhdistelmien avulla. Tässä alaluvussa tarkastellaan MAC-, DAC-, RBAC- ja ABAC-mallien yhdistämistä.

Hallinnan mallien yhdistäminen voi tukea pääsyoikeuksien hallintaa, sillä hyvin valitut mallit voivat paikata toistensa puutteita ja tehdä hallinnasta kattavamman. Alaluvussa 2.2.3 esiteltiin Puchtan, Böhmin ja Pernun (2019) huoli RBAC-mallin kasvavasta roolien määrästä ja alaluvussa 2.2.4 nostettiin esille ABAC-mallin kasvavaan attribuuttien määrään liittyvät haasteet. Näitä ongelmia voidaan ratkaista Longin ja Yanin (2019) tutkimuksen mukaan yh-

distämällä RBAC- ja ABAC-mallit rooli- ja attribuuttipohjaisella pääsyoikeuksien hallinnan mallilla (engl. *Role and Attribute Combined Access Control*, RACAC). Tutkimuksessa esitelty RACAC-malli perustuu RBAC-malliin, johon on lisätty attribuuttipohjaisia poliitikkoja. Tämä RBAC- ja ABAC-mallin ominaisuuksien yhdistäminen tekee tutkimuksen mukaan mallista dynaamisemman, joustavamman ja rajoittaa sekä attribuuttien, että roolien määrän kasvua (Long ja Yan 2019).

Samarati ja Vimercati (2001) esittävät, että myös MAC- ja DAC-mallit voidaan yhdistää. Fan ym. (2009) puhuvat DAC- ja MAC-mallit yhdistävästä pääsyoikeuksien hallinnan mallista FEMAC-nimellä (engl. *Formal Evaluation of Minimum Access Control*, FEMAC). Heidän mukaansa FEMAC-malli yhdistää MAC-mallin tiukat turvallisuuspolitiikat ja DAC-mallin joustavuuden. Malli mahdollistaa tilapäisten valtuutuksien käytön ja DAC-mallin soveltamisen määritellyissä tilanteissa (Fan ym. 2009). Nämä ominaisuudet tekevät mallista turvallisemman kuin DAC ja joustavamman kuin MAC. Samarati ja Vimercati (2001) ovat samaa mieltä mallien yhdistämisen kannattavuudesta. FEMAC:in kaltaiset mallit tarjoavat vaihtoehtoisen tavan hyödyntää useampien hallintamallien vahvuuksia.

Myös MAC- ja RBAC-mallit voidaan Kimin ym. (2014) mukaan yhdistää toimivaksi pääsyoikeuksien hallinnan malliksi. He esittävät, että mallit voidaan yhdistää kartoittamalla mallien yhteensopivat kohdat ja ominaisuudet. Malli perustuu taulukosta 1 löytyviin MAC- ja RBAC-mallien ominaisuuksiin. Kimin ym. (2014) mukaan ominaisuudet organisoidaan erillisiksi konfiguroitaviksi ominaisuuksiksi, joita voidaan yhdistellä kohdejärjestelmän tarpeiden mukaisesti. Yhdistäminen mahdollistaa sekä roolien, että turvallisuustasojen käyttämisen, jonka takia malli voi olla hyödyllinen esimerkiksi julkishallinnon, puolustusvoimien ja sairaaloiden tietoturvallisuutta vaativissa ympäristöissä (Kim ym. 2014).

Malli	Kuvaus	Vahvuudet	Heikkoudet
MAC	Perustuu ennalta määritettyihin tietoturvaluokituksiin ja -määrityksiin. Käyttäjien pääsy määräytyy resurssien ja käyttäjien tietoturvaluokitusten perusteella.	Korkea tietoturvataso.	Joustamaton ja staattinen malli, joka ei tue vähimmäisoikeuksien periaatetta.
DAC	Perustuu resurssin omistajan hallinnoimiin harkinnanvaraisiin pääsyoikeuksiin.	Joustava.	Tiedon kulun seuraaminen on haastavaa. Riskinä luvattomalle tiedon jakamienn ja tietovuodot. Ei tue vähimmäisoikeuksien periaatetta.
RBAC	Käyttäjien pääsy määritellään rooliensa perusteella, sillä pääsyoikeudet määritellään rooleille, jotka peilaavat organisaation rakennetta.	Skaalautuva ja intuitiivinen roolipohjainen rakenne. Tukee vähimmäisoikeuksien periaatetta.	Roolien määrän kasvu voi tehdä mallin hallinnasta monimutkaista.
ABAC	Pääsy määräytyy attribuuttien perusteella.	Joustava, tukee useiden politiikkojen samanaikaista käyttöä ja vähimmäisoikeuksien periaatetta.	Hidas suurten attribuuttitietokantojen kanssa attribuuttien määrän kasvaessa.
PBAC	Pääsy määräytyy sääntöjen ja politiikkojen perusteella, jotka huomioivat käyttäjän, resurssin ja olosuhteet.	Joustava. Tukee useiden politiikkojen samanaikaista käyttöä ja vähimmäisoikeuksien periaatetta.	Mallin määrittely voi olla haastavaa. Sääntöjen määrän kasvu.

Taulukko 1. Pääsyoikeuksien hallintamallit sekä niiden vahvuudet ja heikkoudet.

2.4 Pääsyoikeuksien hallinnan haasteet

Pääsyoikeuksien hallinnan malleihin liittyy monia haasteita, kuten alaluvun 2.2 taulukko 1 osoittaa. Nämä haasteet kietoutuvat usein toisiinsa syy-seuraussuhteiden kautta muodostaen erilaisia pääsyoikeuksien hallinnan haasteita. Ne voivat eskaloitua pienistä hallinnollisista virheistä merkittäviksi turvallisuusuhiksi, jotka uhkaavat sekä organisaation tietojen eheyttä että liiketoiminnan jatkuvuutta. Koska yksittäisten hallinnan mallien haasteet on koottu alaluvun 2.2 taulukkoon 1, käsitellään tässä alaluvussa hallinnan haasteita laajemmasta näkökulmasta.

Alaluvussa 2.3 todettiin, että tietoturvakäytäntöjen tulkitseminen yksikäsitteiseksi pääsyoikeuksien hallintamalliksi ja politikoiksi on haastavaa. Epätarkoista ja vanhentuneista politiikoista voi seurata ylimääräisiä ja luvattomia pääsyoikeuksia (Kern ym. 2023), jotka voivat olla vähimmäisoikeuksien periaatteen vastaisia (Kukreti 2022). Ylimääräiset pääsyoikeudet voivat johtaa esimerkiksi tietojen väärinkäyttöön, luvattomaan informaation jakamiseen (Zhao ja Johnson 2010; Hummer ym. 2016) ja tietovuotoihin (Kukreti 2022). Edellä mainittujen riskien lisäksi ylimääräiset pääsyoikeudet voivat altistaa organisaation myös sisäpiiriuhille, joista voi seurata edellä esiteltyjen kevyempien seurauksien lisäksi vakavampia seurauksia, kuten taloudellisia tappioita, liiketoiminnan keskeytyksiä ja organisaation maineen heikkenemistä (Baracaldo ja Joshi 2013).

Näiden haasteiden lisäksi tietoturvan ja joustavuuden tasapainoa voi olla vaikeaa löytää. Liian tiukat pääsyoikeuksien hallinnan rajoitukset voivat heikentää organisaation kykyä reagoida nopeasti kehittyviin tietoturvauhkiin (Zhao ja Johnson 2010). Ne myös vähentävät työntekijöiden tuottavuutta, joka voi epäsuorasti lisätä turvallisuusriskejä (Hummer ym. 2016). Tiukat oikeudet voivat olla erityisen haastavia sairaalaympäristössä, jossa pääsyoikeuksien hallinnan tulee sopeutua nopeasti muuttuvaan ympäristöön. Toisaalta liian joustava pääsyoikeuksien hallinta voi vähentää hallinnan tehokkuutta ja altistaa organisaation aikaisemmin esitellyille tietoturvauhille ja -haasteille (Zhao ja Johnson 2010).

Sisäpiiriuhkien ja ylimääräisten oikeuksien ennaltaehkäisy edellyttää tarkkaa ja toimivaa pääsyoikeuksien hallintaa, jota voidaan Sandhun ja Samaratin (1994) mukaan tukea jatkuvalla arviointiprosessilla. Heidän mukaansa arviointiprosessi auttaa myös tunnistamaan pää-

syoikeuksien hallinnan prosessin haasteita, joka voi auttaa hallinnan parantamisessa. Yksi arvioinnin kohde on pääsyoikeudet, joiden katselmointiin ja sen mahdollisuuksiin paneudutaan luvussa 3.

3 Pääsyoikeuksien katselmointi

Tässä luvussa käsitellään pääsyoikeuksien katselmointia. Luku jakautuu viiteen alalukuun: ensimmäisessä esitellään pääsyoikeuksien katselmoinnin tavoitteita ja merkitystä, toisessa käydään läpi katselmoinnin prosessin vaiheet, kolmannessa tarkastellaan katselmointiin liittyviä haasteita, neljännessä vastataan kysymykseen: ”Miksi pääsyoikeuksien katselmointia kannattaa toteuttaa säännöllisesti?”, ja viidennessä luvussa esitellään katselmointiin liittyviä hyviä käytänteitä.

Pääsyoikeuksien katselmointia on tutkittu akateemisesti vähän, vaikka pääsyoikeuksien katselmointi on Kernin ym. (2022) mukaan vakiintunut organisaatioiden IAM-prosessi. Nykyinen tutkimus keskittyy ratkaisemaan pääsyoikeuksien katselmoinnin prosessiin liittyviä haasteita työkalujen, kuten automaation ja visuaalisen käyttöliittymän avulla. Akateemisten lähteiden vähäisyyden takia, tässä luvussa hyödynnetään myös kaupallisia lähteitä kuten asiantuntijaraportteja (engl. *white paper*), jotka tarjoavat erilaisia näkökulmia aiheeseen. Kaupallisten lähteiden käyttö on myös perusteltua, koska pääsyoikeuksien katselmointi ulkoistetaan monissa organisaatioissa IT-konsulttiyrityksille tai muille kumppaneille. Tässä luvussa käytetään kaupallisina lähteinä Ramaseshanin (2019), Security Compliance Corporationin (2024), Onoraton (2023) ja Imprivatan (2023) julkaisuja.

3.1 Mitä pääsyoikeuksien katselmointi on

Pääsyoikeuksien katselmointi tunnetaan englanniksi yleisesti termillä *’access review’*. Kirjallisuudessa esiintyvät myös termit *’access recertification’* ja *’access audit’*, mutta niitä käytetään harvemmin. Tässä tutkielmassa käytetään termiä *’access review’*, joka on suomennettu pääsyoikeuksien katselmoinniksi. Valinta perustuu siihen, että kyseinen termi on yleisimmin käytetty ja korostaa organisaation sisäistä pääsyoikeuksien tarkastelua.

Pääsyoikeuksien katselmointi on säännöllinen prosessi, jonka avulla pyritään varmistamaan, että organisaation käyttäjillä on pääsyoikeudet vain niihin resursseihin, jotka ovat heidän työtehtäviensä kannalta välttämättömiä. Sen avulla pyritään havaitsemaan tunnistamattomia ja hallinnoimattomia tilejä (Jaferian, Rashtian ja Beznosov 2014). Samalla prosessi pyrkii

parantamaan organisaation tiedon laatua ja tunnistamaan puuttuvia oikeuksia, jotka saattavat häiritä työn sujuvuutta (Baumer ym. 2024).

Katselmointi on keskeinen osa tietoturvastandardeja ja -säädöksiä, sillä se edistää vähimmäisoikeuksien periaatteen toteutumista. Tämä periaate on olennainen osa NIST-suosituksia (2020) ja ISO/IEC 27001 -standardia (2013). Baumer ym. (2024) painottavat, että katselmointi on säädösten ja standardien ohjaama prosessi, joka tekee siitä tärkeän osan organisaation tietoturvan ylläpitoa. Lisäksi NIST:in (2020) ja ISO/IEC 27001 -standardin (2013) suositukset alleviivaavat prosessin säännöllisyyden merkitystä tietoturvan tehokkaassa varmistamisessa. Myös Euroopan unionin NIS2-direktiivi (2022) velvoittaa organisaatioita toteuttamaan kyberturvallisuuteen liittyviä riskienhallintatoimenpiteitä, joihin sisältyy pääsyoikeuksien hallinta ja katselmointi.

Jaferianin, Rashtianin ja Beznosovin (2014) mukaan pääsyoikeuksien katselmointi on erityisen tärkeä organisaatioissa, joissa esihenkilöt määrittelevät pääsyoikeudet, mutta tietoturva-asiantuntijat vastaavat niiden toteuttamisesta. Heidän mukaansa prosessi vaatii useiden toimijoiden kuten esihenkilöiden, sovellusten omistajien sekä tietoturva- ja järjestelmävalvojien kesken. Kern ym. (2022) korostavat, että katselmointi vaatii vähintään kaksi vastuuhenkilöä: yhden, joka johtaa katselmointia, ja toisen, joka vastaa arvioitavasta järjestelmästä. Vaikka artikkelit eivät ole yksimielisiä prosessin osallistujista, ovat ne yhtä mieltä siitä, että prosessin onnistunut toteutus vaatii useamman osapuolen aktiivista osallistumista ja yhteistyötä.

3.2 Pääsyoikeuksien katselmoinnin prosessi

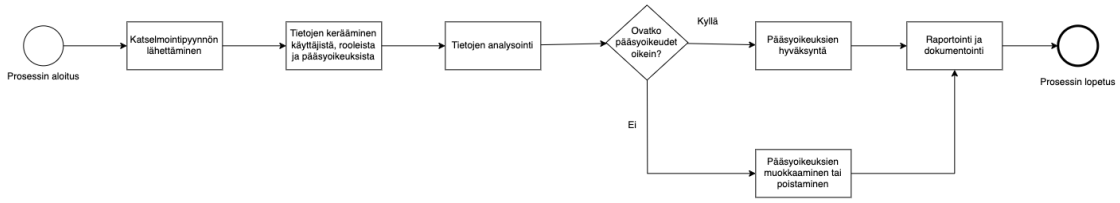
Pääsyoikeuksien katselmointi määriteltiin alaluvussa 3.1. Grollin ym. (2021) mukaan katselmointiprosessi voidaan tiivistää kahteen vaiheeseen, jotka ovat käyttäjän identiteetin tarkistaminen ja pääsyoikeuden myöntämistä koskevan päätöksen tekeminen. Imprivata (2023) ja Onorato (2023) suosittelevat pääsyoikeuksien hallinnassa käytettäväksi alaluvussa 2.2.3 esiteltyä RBAC-mallia sen organisaatioroolien takia. Tässä alaluvussa esitetty katselmoinnin prosessi ja siihen liittyvä kuvio 2 perustuvat Grollin ym. (2021) yksinkertaistettuun katselmointiin ja RBAC-malliin. Muiden hallintamallien, kuten ABAC:in ja PBAC:in, yhteydessä katselmointiprosessia on muokattava huomioimaan niiden erityispiirteet, kuten attribuuttien

ja sääntöjen tarkastelu.

Jaferianin, Rashtianin ja Beznosovin (2014) mukaan prosessi käynnistyy, kun tietoturvavastaava (engl. *security administrator*) lähettää pääsyoikeuksien katselmointipyynnön katselmoijalle (engl. *reviewer*). Heidän mukaansa pääsyoikeuksien katselmoija on organisaation esihenkilö, tietoturvavastaava tai sovellusomistaja. Hänelle kerätään katselmoinnin käynnistämisen yhteydessä tarvittavat tiedot katselmoinnin kohteena olevan järjestelmän käyttäjistä, rooleista ja pääsyoikeuksista. Näihin tietoihin sisältyvät muun muassa tiedot käyttäjän identiteetistä, työtehtävistä ja osastosta (Jaferian, Rashtian ja Beznosov 2014). Jaferianin, Rashtianin ja Beznosovin (2014) mukaan katselmoijan rooli vaikuttaa tarkastuksen painopisteeseen, sillä siinä missä esihenkilö ja tietoturvavastaava keskittyvät käyttäjille annettujen roolien tarkasteluun, arvioi sovellusomistaja rooleihin liitettyjä käyttäjiä.

Katselmoija analysoi kerätyt tiedot, tarkistaa käyttäjien nykyiset roolit ja niihin liittyvät pääsyoikeudet sekä arvioi, ovatko löytyneet pääsyoikeudet käyttäjän työtehtävien kannalta tarpeellisia (Jaferian, Rashtian ja Beznosov 2014). Kerättyjen tietojen perusteella hän tekee päätökset, säilytetäänkö löytyneet pääsyoikeudet vai tuleeko niitä muokata tai poistaa (Kern ym. 2022). Jaferian, Rashtian ja Beznosov (2014) korostavat, että prosessin aikana katselmoija voi myös konsultoida sidosryhmiä, kuten sovellusomistajia ja tietoturvatiimiä, varmistaakseen päätösten oikeellisuuden. Kernin ym. (2022) mukaan yhteistyö on erityisen tärkeää, sillä katselmoija käsittelee suuria tietomääriä rajallisen informaation avulla.

Prosessi päättyy raportointivaiheeseen, jossa dokumentoidaan tehdyt muutokset ja tehdyt havainnot. Akateeminen tutkimus ei mainitse raportointivaihetta, mutta kaupallisissa lähteissä, kuten Security Compliance Corporationin (2024) se korostuu. Katselmoinnin raportointi ja dokumentointi ovat olennaisia, sillä ne varmistavat prosessin läpinäkyvyyden, mahdollistavat tarkastettavuuden, jäljitettävyyden ja tarjoavat arvokasta tietoa tulevien katselmointien tueksi (Security Compliance Corporation 2024).



Kuvio 2. Pääsyoikeuksien katselmoinnin prosessi

3.3 Pääsyoikeuksien katselmoinnin haasteet

Vaikka pääsyoikeuksien katselmointi on tärkeä osa tietoturvan hallintaa, prosessiin liittyy merkittäviä haasteita, jotka voivat hankaloittaa sen toteuttamista ja vaikuttaa katselmoinnin laatuun. Laadun heikentyminen voi vähentää katselmoinnin hyötyä ja heikentää pääsyoikeuksien hallintaa. Jaferianin, Rashtianin ja Beznosovin (2014) mukaan katselmointiin liittyviä haasteita ovat katselmoinnin laajuus, sen toteuttajien puutteellinen tietämys pääsyoikeuksista, manuaalinen työmäärä, säännöllisyys sekä poikkeustilanteiden hallinta.

Kernin ym. (2022) mukaan katselmoinnin suurin haaste on prosessin manuaalisuus. Groll ym. (2021) sekä Jaferian, Rashtian ja Beznosov (2014) eivät kommentoi sitä, onko manuaalisuus prosessin suurin haaste, mutta nostavat kuitenkin tutkimuksessaan manuaalisuuden yhdeksi katselmointiin liittyväksi haasteeksi. Kern ym. (2022), Groll ym. (2021) ja Jaferian, Rashtian ja Beznosov (2014) ovat kuitenkin yhtä mieltä siitä, että katselmoinnissa kaikkien pääsyoikeuksien läpi käyminen vaatii paljon manuaalista työtä, joka on aikaa ja resursseja vievää. Manuaalinen työ tekee katselmoinnista myös virhealttiin (Groll ym. 2021).

Toisena merkittävänä haasteena on katselmoijan puutteellinen ymmärrys pääsyoikeuksista ja niiden merkityksestä (Kern ym. 2022). Jos pääsyoikeuksien katselmoinnin toteuttaa henkilö, joka ei ole riittävän perehtynyt tarkastuksen kohteena olevien roolien ja pääsyoikeuksien sisältöön, seurauksena voi olla virheellisiä pääsyoikeuksiin liittyviä päätöksiä. Puutteellisen tiedon takia katselmoija saattaa vahvistaa pääsyoikeudet kykenemättä arvioimaan niiden tarpeellisuutta, joka voi johtaa ylimääräisten pääsyoikeuksien säilymiseen (Kern ym. 2022). Jaferian, Rashtian ja Beznosov (2014) esittävätkin, että pääsyoikeuksien katselmointia to-

teuttaville henkilöille tulisi tarjota koulutusta ja tukea pääsyoikeuksiin liittyviin päätöksiin.

Myös poikkeustapaukset voivat aiheuttaa haasteita katselmoinnissa. Pääsyoikeus ei aina vastaa käyttäjän toimenkuvaa, mikä voi johtaa siihen, että oikeuksia jää järjestelmään esimerkiksi tilapäisten roolimuutosten, kuten sijaisuuksien vuoksi. Tämä voi lisätä ylimääräisten pääsyoikeuksien määrää ja heikentää järjestelmän tietoturvaa. Tämän haasteen vähentämiseksi katselmoinnissa tulisi kiinnittää huomiota poikkeustilanteisiin sekä varmistaa, että pääsyoikeuksia päivitetään säännöllisesti (Jaferian, Rashtian ja Beznosov 2014).

Lisäksi Grollin ym. (2021) tutkimuksessa korostetaan, että pääsyoikeuksien katselmoinnin laadun mittaaminen on haastavaa, eikä prosessin onnistumisen arviointiin ole kehitetty kattavia menetelmiä. Ilman tehokkaita laatumittareita organisaatiolla voi olla vaikeuksia tunnistaa, onko katselmointi saavuttanut halutut tietoturvatavoitteet. Näiden haasteiden lisäksi myös katselmoinnin säännöllinen toteuttaminen aiheuttaa organisaatioissa ongelmia (Jaferian, Rashtian ja Beznosov 2014).

Näiden haasteiden ratkaisemiseksi Kern ym. (2022), Baumer ym. (2024) ja Jaferian, Rashtian ja Beznosov (2014) esittelevät erilaisia ratkaisuja. Parannuksina tarjotaan muun muassa automaatiotyökalujen hyödyntämistä ja pääsyoikeuksien arviontiin liittyvien visuaalisten käyttöliittymien parantamista (Jaferian, Rashtian ja Beznosov 2014). Baumer ym. (2024) ehdottavat myös katselmoijan päätöksenteon ohjaamista digitaalisten ohjauskeinojen (engl. *digital nudges*) kuten oletusvalintojen ja muistutusten avulla. Näiden ratkaisujen lisäksi katselmointiin liittyviä haasteita voidaan helpottaa myös Jaferianin, Rashtianin ja Beznosovin (2014) mukaan organisaation sisäisen yhteistyön parantamisella ja henkilöstön kouluttamisella.

3.4 Miksi pääsyoikeuksien katselmointeja kannattaa toteuttaa säännöllisesti

Akateemiset ja kaupalliset lähteet ovat samaa mieltä siitä, että säännöllisesti toteutettu pääsyoikeuksien katselmointi auttaa varmistamaan, että organisaatio noudattaa erilaisia tietoturvaan liittyviä säädöksiä ja ohjeita. Esimerkiksi Sarbanes-Oxley-laki (SOX), Yhdysvaltojen terveysvakuutusten siirrettävyys- ja vastuullisuuslaki (engl. *Health Insurance Portability and*

Accountability Act, HIPAA) ja Euroopan unionin yleinen tietoturvalaki (GDPR) edellyttävät organisaatiolta pääsyoikeuksien säännöllistä tarkistusta (Baumer ym. 2024; Jaferian, Rashtian ja Beznosov 2014; Groll ym. 2021; Security Compliance Corporation 2024; Ramaseshan 2019; Imprivata, Inc. 2023). Ulkoisten säädösten lisäksi pääsyoikeuksien katselmointi tukee myös organisaation sisäisten säädösten ja tietoturvakäytänteiden noudattamista (Security Compliance Corporation 2024).

Säännöllisesti toteutettu pääsyoikeuksien katselmointi voi auttaa tunnistamaan ja korjaamaan pääsyoikeuksien hallinnan puutteita, mikä voi vähentää järjestelmistä löytyviä ylimääräisiä oikeuksia ja parantaa hallinnan kattavuutta. Katselmoinnin keskeinen tehtävä on turvata organisaation arvokkaat resurssit ja vähentää pääsyoikeuksiin liittyviä tietoturvariskejä (Security Compliance Corporation 2024). Molemmat lähdetyypit korostavat säännöllisyyden merkitystä, sillä se auttaa pienentämään puutteelliseen pääsyoikeuksien hallintaan liittyvää uhkaikkunaa vähentämällä alaluvussa 2.4 esiteltyjä ylimääräisiin pääsyoikeuksiin liittyviä riskejä (Baumer ym. 2024; Jaferian, Rashtian ja Beznosov 2014; Groll ym. 2021; Security Compliance Corporation 2024; Ramaseshan 2019; Imprivata, Inc. 2023).

Edellä mainittujen hyötyjen lisäksi kaupallisissa lähteissä painotetaan, että säännöllinen pääsyoikeuksien katselmointi tarjoaa myös taloudellisia hyötyjä. Imprivata, Inc. (2023), Ramaseshan (2019) ja Security Compliance Corporation (2024) ovat samaa mieltä siitä, että säännöllinen katselmointi auttaa poistamaan ylimääräisiä pääsyoikeuksia, joka vähentää lisensseihin liittyviä kustannuksia. Akateeminen kirjallisuus ei kuitenkaan käsittele pääsyoikeuksien katselmoinnin taloudellisia hyötyjä.

3.5 Pääsyoikeuksien katselmoinnin hyvät käytänteet

Hyvin toteutettu pääsyoikeuksien katselmointi varmistaa, että kaikki pääsyoikeudet ovat linjassa organisaation tarpeiden kanssa, eikä käyttäjillä ole tarpeettomia oikeuksia. Säädökset ja lait, kuten SOX, HIPAA ja NIST tarjoavat ohjeita ja vaatimuksia pääsyoikeuksien hallinnan ja katselmoinnin toteuttamiseen. Säädösten ja lakien lisäksi hyviä käytänteitä esiintyy akateemisissa lähteissä ja organisaatioiden materiaaleissa kuten Ramaseshanin (2019), Imprivatan (2023) ja Security Compliance Corporationin (2024) julkaisuissa.

Pääsyoikeuksien tarkastaminen säännöllisesti on yksi tehokkaan pääsyoikeuksien hallinnan kulmakivistä. Säännöllisyydellä voidaan varmistaa, että pääsyoikeudet ovat ajan tasalla, ylimääräisiä oikeuksia ei löydy ja oikeudet vastaavat organisaation nykytilannetta (NIST 2020; Security Compliance Corporation 2024). Säännöllisyyttä voidaan Ramaseshan (2019) mukaan tukea lisäämällä katselmointi osaksi organisaation tietoturva- ja arviointiohjelmaa.

Kuten alaluvussa 3.3 todettiin, pääsyoikeuksien katselmoinnin haasteena on prosessin manuaalisuus. Lähteet suosittelevatkin katselmoinnin osittaista tai kokonaista automatisointia. Automatisoinnilla voidaan vähentää manuaalisen työn määrää ja siitä johtuvia inhimillisiä virheitä sekä parantaa laadunvalvontaa ja päätöksien laatua. Automatisointi voi myös tukea pääsyoikeuksien katselmoinnin säännöllisyyttä (Security Compliance Corporation 2024; Groll ym. 2021; Jaferian, Rashtian ja Beznosov 2014; NIST 2020; Ramaseshan 2019).

Imprivata, Inc. (2023) ja Onorato (2023) listaavat pääsyoikeuksien katselmoinnin hyviin käytänteisiin RBAC-mallin hyödyntämisen pääsyoikeuksien hallinnassa. Imprivatan (2023) mukaan RBAC-malli ja vähimmäisoikeuksien periaate täydentävät toisiaan ja varmistavat, että käyttäjillä on vain tarvittavat oikeudet. Kaupalliset ja akateemiset lähteet eivät kommentoi, miten pääsyoikeuksien katselmointi tulee toteuttaa muille pääsyoikeuksien hallinnan malleille. Katselmoinnissa voisi kuitenkin olla perusteltua huomioida kohdejärjestelmässä käytettyjen pääsyoikeuksien hallinnan mallien erityispiirteet kuten ABAC-mallin attribuutit ja PBAC-mallin politiikat.

Edellä mainittujen hyvien käytänteiden lisäksi työntekijöiden kouluttaminen ja perehdyttäminen ovat tärkeitä tekijöitä pääsyoikeuksien katselmoinnin toteuttamisessa ja sen onnistumisessa. Henkilöstön ymmärrys oikeiden käytäntöjen ja oikeuksien merkityksestä tukee katselmointiprosessin onnistumista ja vahvistaa organisaation tietoturvan parantamista (Ramaseshan 2019).

4 Yhteenveto

Tutkielmassa tarkasteltiin pääsyoikeuksien hallintaa ja sen vahvistamista säännöllisellä pääsyoikeuksien katselmoinnilla. Tutkielmaan tulokset osoittivat, että säännöllisesti toteutettu pääsyoikeuksien katselmointi auttaa tunnistamaan kohdejärjestelmästä löytyviä ylimääräisiä pääsyoikeuksia ja hallinnan puutteita, mikä vahvistaa organisaation tietoturvaa.

Tutkielmassa esiteltiin viisi pääsyoikeuksien hallinnan mallia ja tultiin siihen tulokseen, että pääsyoikeuksien hallinnan keskeisimmät haasteet liittyvät sen monimutkaisuuteen, skaalautuvuuden puutteeseen sekä manuaaliseen työhön ja siihen liittyviin inhimillisiin virheisiin. Näiden haasteiden arvioitiin heikentävän pääsyoikeuksien hallinnan tehokkuutta ja kattavuutta. Tutkielmassa ratkaisuna ehdotettiin koulutuksen ja automatisoinnin lisäksi säännöllisesti toteutettavaa pääsyoikeuksien katselmointia.

Vaikka tutkielmassa havaittiin, että pääsyoikeuksien katselmointi tukee tietoturvaa ja pääsyoikeuksien hallintaa, sen hyötyjä olisi mahdollista kasvattaa. Tutkielman mukaan pääsyoikeuksien katselmointi painottuu ensisijaisesti hallinnan puutteista johtuvien seurausten korjaamiseen, vaikka juurisyiden analysointiin keskittyminen voisi tehdä katselmoinnista tehokkaamman ja merkityksellisemmän työkalun. Juurisyiden lisäksi katselmoinnin tulisi tuottaa tarkempaa informaatiota pääsyoikeuksien hallinnan puutteista ja tukea pääsyoikeuksien hallinnan kehittämistä.

Tutkielmassa tunnistettiin, että säännöllisesti toteutettava katselmointi vaatii paljon resursseja. Riskiperusteinen lähestymistapa voisi tehostaa pääsyoikeuksien katselmointia ja auttaa resurssien keskittämisessä. Tämä voitaisiin toteuttaa arvioimalla organisaation järjestelmien ja roolien riskisyydet, sekä luomalla riskiperusteiset priorisointikriteerit. Näiden kriteerien avulla katselmoinnit ja organisaation resurssit voitaisiin kohdentaa tehokkaammin korkeamman riskin järjestelmiin ja rooleihin, joka lisäisi tietoturvaa ja resurssien strategisempaa käyttöä.

Laajemmassa kuvassa katselmointi tulisi nähdä strategisena työkaluna, joka tukee organisaation pääsyoikeuksien hallinnan pitkäjänteistä kehittämistä. Järjestelmällinen katselmoinnin löytämien poikkeamien kerääminen ja analysointi voisivat auttaa luomaan kattavampaa

kokonaiskuvaa organisaation pääsyoikeuksien hallinnasta ja auttaa tunnistamaan siihen liittyviä kehityslinjoja ja ongelmakohtia. Pitkäjänteinen ja strategisesti nähty katselmointi voisi nostaa katselmoinnin rutiininomaisesta säädösten vaatimasta tehtävästä keskeiseksi osaksi organisaation turvallisuuskulttuuria ja pääsyoikeuksien hallinnan jatkuvaa kehittämistä.

Tutkielmassa korostuu pääsyoikeuksien katselmointiin liittyvän laajemman perustutkimuksen tarve, sillä aihetta on tutkittu erittäin vähän. Vajaan tutkimuksen takia aiheeseen liittyy useita tutkimusaukkoja, jotka voivat tarjota mahdollisuuksia kehittää prosessia ja lisätä kaupallisen ja akateemisen maailman yhteistyötä. Jatkotutkimuksena olisi olennaista tutkia, miten pääsyoikeuksien hallinnan prosesseja ja katselmointia voitaisiin kehittää kohti ennakoivaa riskienhallintaa. Lisäksi olisi hyvä tutkia, miten moderneja teknologioita, kuten tekoälyä ja koneoppimista, voidaan hyödyntää katselmoinnin tukena ja onko teknologioiden avulla mahdollista toteuttaa reaaliaikaista pääsyoikeuksien katselmointia. Myös eri pääsyoikeuksien hallintamallien vaikutusta katselmointiprosessin sujuvuuteen ja tehokkuuteen tulisi tarkastella. Näitä tutkimusehdotuksia olisi hyvä tarkastella tapaustutkimusten avulla, sillä sen avulla toteutettava tutkimus ja tutkimuksen tulokset voisivat laajentaa aihepiirin akateemista tutkimusta ja hyödyttää organisaatioita ja niiden pääsyoikeuksien hallinnan kehittämistä.

Lähteet

Aftab, Muhammad Umar, Ali Hamza, Ariyo Oluwasanmi, Xuyun Nie, Muhammad Sarfraz, Danish Shehzad, Zhiguang Qin ja Ammar Rafiq. 2022. "Traditional and Hybrid Access Control Models: A Detailed Survey". *Security and Communication Networks* 2022 (helmikuu): 1–12. https://doi.org/10.1155/2022/1560885.

Ahn, Gail-Joon. 2018. "Discretionary Access Control". Teoksessa *Encyclopedia of Database Systems,* toimittanut Ling Liu ja M. Tamer Özsu, 1140–1143. New York, NY: Springer New York. ISBN: 978-1-4614-8265-9. https://doi.org/10.1007/978-1-4614-8265-9_135. https://doi.org/10.1007/978-1-4614-8265-9_135.

Baracaldo, Nathalie ja James Joshi. 2013. "An adaptive risk management and access control framework to mitigate insider threats". *Computers Security* 39:237–254. ISSN: 0167-4048. https://doi.org/https://doi.org/10.1016/j.cose.2013.08.001.

Baumer, Thomas, Tobias Reittinger, Sascha Kern ja Günther Pernul. 2024. "Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations", 239–258. USENIX Association, elokuu. https://www.usenix.org/conference/soups2024/presentation/baumer.

Bertino, Elisa. 2003. "RBAC models — concepts and trends". *Computers Security* 22 (6): 511–514. ISSN: 0167-4048. https://doi.org/https://doi.org/10.1016/S0167-4048(03)00609-6.

Capital One. 2019. *2019 Cyber Incident.* Viitattu 15.12.2024. https://www.capitalone.com/digital/facts2019/.

"Department of Defense Trusted Computer System Evaluation Criteria". 1985. Teoksessa *The 'Orange Book' Series,* 1–129. London: Palgrave Macmillan UK. ISBN: 978-1-349-12020-8. https://doi.org/10.1007/978-1-349-12020-8_1.

Euroopan unioni. 2022. *Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS2-direktiivi).* https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi. EUVL L 333, 27.12.2022, s. 80–152 (FI). Viitattu 6. joulukuuta 2024.

Fan, Yanfang, Zhen Han, Jiqiang Liu ja Yong Zhao. 2009. "A Mandatory Access Control Model with Enhanced Flexibility". Teoksessa *2009 International Conference on Multimedia Information Networking and Security,* 1:120–124. https://doi.org/10.1109/MINES.2009.267.

Groll, Sebastian, Sascha Kern, Ludwig Fuchs ja Günther Pernul. 2021. "Monitoring Access Reviews by Crowd Labelling". Teoksessa *Trust, Privacy and Security in Digital Business,* toimittanut Simone Fischer-Hübner, Costas Lambrinoudakis, Gabriele Kotsis, A. Min Tjoa ja Ismail Khalil, 3–17. Cham: Springer International Publishing.

Hummer, Matthias, Michael Kunz, Michael Netter, Ludwig Fuchs ja Günther Pernul. 2016. "Adaptive identity and access management—contextual data based policies". *EURASIP Journal on Information Security* 2016 (elokuu). https://doi.org/10.1186/s13635-016-0043-2.

Imprivata, Inc. 2023. *Top User Access Review Best Practices.* https://www.imprivata.com/uk/node/103704. Vierailtu 17. marraskuuta 2024.

ISO/IEC27001. 2013. *ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO/IEC 27001:2022. Vierailtu 17. joulukuuta 2024. International Organization for Standardization. https://www.iso.org/standard/82875.html.

Jaferian, Pooya, Hootan Rashtian ja Konstantin Beznosov. 2014. "To Authorize or Not Authorize: Helping Users Review Access Policies in Organizations". Teoksessa *10th Symposium On Usable Privacy and Security (SOUPS 2014),* 301–320. Menlo Park, CA: USENIX Association, heinäkuu. ISBN: 978-1-931971-13-3. https://www.usenix.org/conference/soups2014/proceedings/presentation/jaferian.

Kern, Sascha, Thomas Baumer, Ludwig Fuchs ja Günther Pernul. 2023. “Maintain High-Quality Access Control Policies: An Academic and Practice-Driven Approach”. Teoksessa *Data and Applications Security and Privacy XXXVII,* toimittanut Vijayalakshmi Atluri ja Anna Lisa Ferrara, 223–242. Cham: Springer Nature Switzerland. ISBN: 978-3-031-37586-6.

Kern, Sascha, Thomas Baumer, Sebastian Groll, Ludwig Fuchs ja Günther Pernul. 2022. “Optimization of Access Control Policies”. *Journal of Information Security and Applications* 70:103301. ISSN: 2214-2126. https://doi.org/https://doi.org/10.1016/j.jisa.2022.103301.

Kim, Sangsig, Dae-Kyoo Kim, Lunjin Lu ja Eunjee Song. 2014. “Building hybrid access control by configuring RBAC and MAC features”. *Information and Software Technology* 56 (7): 763–792. ISSN: 0950-5849. https://doi.org/https://doi.org/10.1016/j.infsof.2014.02.003.

Kukreti, Anil. 2022. “Access Control and Authentication for Secure Systems and Networks”. *NeuroQuantology* 20 (5): 5321–5329. https://doi.org/10.48047/nq.2022.20.5.nq22814.

Kunz, Michael, Alexander Puchta, Sebastian Groll, Ludwig Fuchs ja Günther Pernul. 2019. “Attribute quality management for dynamic identity and access management”. *Journal of Information Security and Applications* 44:64–79. ISSN: 2214-2126. https://doi.org/https://doi.org/10.1016/j.jisa.2018.11.004.

Long, Sun ja Li Yan. 2019. “RACAC: An Approach toward RBAC and ABAC Combining Access Control”. Teoksessa *2019 IEEE 5th International Conference on Computer and Communications (ICCC),* 1609–1616. https://doi.org/10.1109/ICCC47050.2019.9064301.

MacLennan, James ja Junjie Zhang. 2024. “Path-Safe: Enabling Dynamic Mandatory Access Controls Using Security Tokens”. Teoksessa *NAECON 2024 - IEEE National Aerospace and Electronics Conference,* 7–11. https://doi.org/10.1109/NAECON61878.2024.10670691.

Onorato, Gerard. 2023. *Enhancing Information Security through Effective Access Reviews.* White Paper. Viitattu 17. marraskuuta 2024. Bridge Security Advisors. https://bridgesecurityadvisors.com/white-paper-enhancing-information-security-through-effective-access-reviews/.

Pal, Shantanu, Michael Hitchens, Vijay Varadharajan ja Tahiry Rabehaja. 2019. “Policy-based access control for constrained healthcare resources in the context of the Internet of Things”. *Journal of Network and Computer Applications* 139:57–74. ISSN: 1084-8045. https://doi.org/https://doi.org/10.1016/j.jnca.2019.04.013.

Puchta, Alexander, Fabian Böhm ja Günther Pernul. 2019. “Contributing to Current Challenges in Identity and Access Management with Visual Analytics”. Teoksessa *Data and Applications Security and Privacy XXXIII,* toimittanut Simon N. Foley, 221–239. Cham: Springer International Publishing.

Ramaseshan, Sundaresan. 2019. “Effective User Access Reviews”. Viitattu 17. marraskuuta 2024, *ISACA Journal* 4. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews.

Samarati, Pierangela ja Sabrina Capitani de Vimercati. 2001. “Access Control: Policies, Models, and Mechanisms”. Teoksessa *Foundations of Security Analysis and Design,* toimittanut Riccardo Focardi ja Roberto Gorrieri, 137–196. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-45608-7.

Sandhu, R.S. ja P. Samarati. 1994. “Access control: principle and practice”. *IEEE Communications Magazine* 32 (9): 40–48. https://doi.org/10.1109/35.312842.

Security Compliance Corporation. 2024. *User Access Reviews Best Practice for Success.* White Paper. Viitattu 17. marraskuuta 2024. Security Compliance Corporation. https://www.securitycompliancecorp.com/user-access-reviews-best-practice/.

Shen, Hai-bo ja Fan Hong. 2006. “An Attribute-Based Access Control Model for Web Services”. Teoksessa *2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT’06),* 74–79. https://doi.org/10.1109/PDCAT.2006.28.

Shi, Lei, Shouqian Sun ja Jun Yuan. 2008. “Research on improved RBAC model and its access control strategy”. Teoksessa *2008 9th International Conference on Computer-Aided Industrial Design and Conceptual Design,* 1067–1071. https://doi.org/10.1109/CAIDCD.2008.4730747.

Standards, National Institute of ja Technology. 2020. *Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Revision 5).* Teknінen raportti SP 800-53r5. Gaithersburg, MD: National Institute of Standards ja Technology. https://doi.org/10.6028/NIST.SP.800-53r5. https://doi.org/10.6028/NIST.SP.800-53r5.

Vahti. 2008. *Valtionhallinnon tietoturvasanasto.* VAHTI Publication 8/2008, Ministry of Finance, Finland, elokuu. https://dvv.fi/documents/2252790/13063677/2008_VAHTI_ohje_tietoturvasanasto.pdf/0cd599d4-e8c5-3e82-8f06-ae76cae7dd8a/2008_VAHTI_ohje_tietoturvasanasto.pdf.

Wei, Lau Kung ja S. Jarzabek. 1998. "A generic discretionary access control system for reuse frameworks". Teoksessa *Proceedings. The Twenty-Second Annual International Computer Software and Applications Conference (Compsac '98) (Cat. No.98CB 36241),* 356–361. https://doi.org/10.1109/CMPSAC.1998.716680.

Xu, Weize, Lei Kong, Nan Wang ja Jinzhong Liu. 2022. "Optimization of attribute-based access control policy with priority filtering". Teoksessa *2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology (ICCASIT),* 1045–1052. https://doi.org/10.1109/ICCASIT55263.2022.9986571.

Zhao, Xia ja M. Eric Johnson. 2010. "Access Governance: Flexibility with Escalation and Audit". Teoksessa *2010 43rd Hawaii International Conference on System Sciences,* 1–13. https://doi.org/10.1109/HICSS.2010.42.

Zhi, Lin, Wang Jing, Chen Xiao-su ja Jia Lian-xing. 2009. "Research on Policy-based Access Control Model". Teoksessa *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing,* 2:164–167. https://doi.org/10.1109/NSWCTC.2009.313.