jamk

Azure-ympäristön kovennus

Lauri Ranta

Opinnäytetyö, AMK
Toukokuu 2025
Insinööri (AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Ranta, Lauri

Azure-ympäristön kovennus

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2025, 33 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Opinnäytetyö keskittyi toimeksiantajan Qvantel Finland Oy:n Azure-ympäristön kovennukseen liittyviin osa-alueisiin. Työ tehtiin tarpeesta kehittää olemassa olevaa järjestelmää vastaamaan kehittyviä tietoturvavaatimuksia. Tehtävänä oli tutkia salasanattoman autentikaation käyttöönottoa ja roolipohjaisen käyttäjienhallinnan uudistusta. Tavoitteena oli kehittää selvitys käsitellyistä aiheista, jotta niitä voitaisiin hyödyntää tulevassa toteutuksessa.

Selvitystyö toteutettiin kokonaan Microsoftin Azure-pilvipalvelussa hyödyntäen sen sisäistä EntraID-palvelua. Salasanattomaa kirjautumista käsiteltiin pääosin fyysisten avainten käyttöönoton puolesta ja roolipohjaista käyttäjien hallintaa sen ominaisuuksien parantamisen puolesta.

Työn tuloksena luotiin selvitys käsiteltyjen aiheiden toteuttamisesta ja sen perusteella tietoturvan parantamisesta. Salasanaton kirjautuminen mahdollisti Microsoftin suositusten mukaisen turvallisemman autentikaation. Fyysisten avainten käyttöönotto lisäsi korkean riskin käyttäjien tietoturvaa vielä enemmän. Roolipohjaisen käyttäjienhallinnan muutoksen toteuttaminen mahdollistaa turvallisemman roolien aktivoinnin prosessin.

Avainsanat (asiasanat)

Azure, kovennus, autentikaatio, FIDO2, PIM, tietoturva

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Ranta, Lauri

Azure-environment hardening

Jyväskylä: JAMK University of Applied Sciences, May 2025, 33 pages

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Thesis focused on hardendening different sections of the Azure environment of the client Qvantel Finland Oy. Research was done from a need to improve an existing system to changing information security requirements. The assignment included exploring the adoption of passwordless authentication and renewing role based access control configuration. Target was to create a report on the covered topics so they could be used in a coming implementation.

Investigative work was implemented in in its entirety on Microsoft Azure cloud computing platform by utilizing its EntraID service. Passwordless authentication mainly covered the adoption of physical security keys and role based access control covered improving its properties.

As a result of the work, a report was created for implementation of the covered topics and based on that, improvement of information security. Passwordless authentication enabled a more secure authentication based on Microsofts recommendations. Physical security keys increased the security further for higher risk users. Role based access control configuration renewal enables a safer way for users to activate their roles.

Keywords/tags (subjects)

Azure, hardening, authentication, FIDO2, PIM, information security

Miscellaneous (Confidential information)

Sisältö

Kuviot

1 Johdanto

1.1 Toimeksiantaja

Työn toimeksiantaja Qvantel perustettiin Finder yrityshakusivuston (Qvantel Finland Oy n.d) mukaan vuonna 1995. Yritys toimittaa nykyään BSS (Business Support System) -palveluita internet- ja mobiilipalveluntarjoajille. Tarjotut palvelut auttavat yrityksiä parantamaan omaa myyntiä ja asiakaskokemusta. Asiakaskuntaan sisältyy sekä pieniä, että suuria yrityksiä maailmanlaajuisesti. (Qvantel Flex BSS: The Next Evolution of BSS N.d.)

Koska Qvantel työskentelee operaattorien kanssa, heidän omaama data kiinnostaa monia toimijoita. Tämä käy ilmi tutkimalla vuoden kyberuhkaraportteja. Hyökkäykset teleoperaattoreja ja teknologiayrityksiä vastaan ovat nousseet jopa 5 prosenttiyksikköä 2024 viimeisimmän neljänneksen aikana ja kaksi prosenttiyksikköä verraten vuoden ensimmäiseen neljännekseen. Nopeat nousut tarkoittavat sitä, että yritysten täytyy pitää järjestelmänsä aina valmiina ja kehitystä ei tulisi lykätä myöhemmälle ajankohdalle esimerkiksi kustannusten takia. (Iacono, Glass & Wojcieszek 2024.)

1.2 Kehittämistehtävä ja sen tavoite

Jotta yrityksen tietoturvaa voidaan pitää yllä, käytössä tulee olla erilaisia tekniikoita ja metodeja sen tukemiseen. Tietoturva on aiheena jatkuvasti kasvava ja laaja-alainen. Turvattavaa informaatiota on kahdenlaista, fyysistä ja digitaalista. Informaation turva on muuttunut nykyajan maailmassa. Dokumentteja ei enää pidetä turvattuna fyysisissä paikoissa, vaan käytössä on digitaalisia ympäristöjä. Tämän takia ympäristöjä täytyy turvata esimerkiksi turvallisuuden asiantuntijoiden puolesta. Yrityksen tietoturvan ylläpitäminen ja kehittäminen on tärkeää, koska erilaiset hyökkäykset yrityksen ympäristöihin heikentävät asiakkaiden uskoa palveluntarjoajaan. Uudet asiakkaat eivät myöskään välttämättä halua ottaa riskiä, jos he ovat tietoisia suuresta tietovuodosta. Uudet uhat kehittyvät jatkuvasti ja yritysten pitää pysyä niiden yläpuolella minimoidakseen riskin. (What is information security and why is it important? 2022.)

Tutkimustyön tarkoituksena oli toteuttaa selvitys autentikaatio- ja PIM (Käyttäjätietojen erityisoikeuksien hallinta) uudistuksesta Azure ympäristössä. Käsiteltävät aiheet perustuivat toimeksiantajan Qvantel Finland Oy:n vaatimuksiin tarpeesta parantaa tämänhetkistä järjestelmää. Tavoitteena

oli luoda selvä perusta käsiteltyjen aiheiden toteuttamiseksi ja hyödyntämiseksi yrityksen toiminnassa. Työssä käsiteltävien tehtävien konfiguraatiot perustuivat Microsoftin parhaisiin käytänteisiin kustakin tutkitusta osa alueesta.

1.3 Tutkimusasetelma

Kehitystyössä hyödynnettiin kehittävän tutkimustyön menetelmiä. Tutkijoiden mukaan se ei ole yksittäinen määritelmä vaan laaja käsite eri tutkintatavoille. Menetelmän kutsumanimi vaihtelee teetetystä työstä ja ne voidaan jakaa kolmeen pääaiheeseen keskustelua edistävänä, osallistavana tai esittävänä. Kuitenkin jokaisella tavalla yhteistä on käytännönläheisyys tavoitteiden saavuttamiseksi. Menetelmät vaihtelevat kulloinkin kyseessä olevan kehittämisprosessin vaiheen mukaan. Osa metodeista tuovat hyötyä esille yksittäisissä kohdissa, kun taas toisia pystytään hyödyntämään laajemmin. (Salonen, Eloranta, Hautala & Kinos 2017, 55-56.) Tämän työn tarkoituksena on toteuttaa selvitystä olemassa olevan järjestelmän parantamisesta ja hyödyntää täten kyseisiä metodeja.

Aihe rajattiin toteutuksen suunnitteluun ja selvityksen tekemiseen. Selvitys sisälsi rajattua henkilökohtaista testausta, mutta varsinaista pilotointia tai koko yrityksen laajuista käyttöönottoa ei tehty. Itse palveluiden osia käytiin läpi mahdollisimman tarkasti, jotta jatkossa tapahtuva toteutus olisi mahdollisimman yksinkertaista. Selvityksen tavoitteena oli kehittää keinoja, joilla yrityksen tietoturvaa voidaan parantaa olemassa olevissa järjestelmissä. Täten työn tarkoituksena oli vastata tutkimuskysymyksiin:

- Miten järjestelmänvalvojien ja käyttäjien autentikaatiota voidaan kehittää?
- Miten roolipohjaista oikeuksien hallintaa voidaan parantaa?

2 Microsoft Azure

2.1 Pilvialusta

Azure on Microsoftin luoma pilvialusta, joka tarjoaa erilaisia palveluita yrityksille ja yksityishenkilöille. Palveluita löytyy lähes jokaiseen tarpeeseen. Oli kyseessä sitten virtuaalikone, tietokanta tai sovelluskehitys sen voi toteuttaa Azuressa tai sen avulla. Microsoft on suuri toimija ja heillä konesaleja maailmanlaajuisesti, joka mahdollistaa toiminnan pienille kuin suurillekin yrityksille. Konesalien määrä mahdollistaa myös palveluiden helpon monistamisen useaan eri alueeseen. Tällä tavalla on lähes mahdotonta, että konesalionnettomuus aiheuttaa palveluiden seisokkeja. Azure mahdollistaa palveluiden joustavaa hyödyntämistä. Laskutustyyli, jossa maksetaan vain käytetystä resurssista voi luoda yritykselle säästöjä. Resurssien kokoa tai määrää pystytään myös muokkaamaan helposti, joka tarjoaa vaihtoehtoja. Palveluita pystytään tarvittaessa skaalaamaan ylös tai alas helposti. (Microsoft Azure: what it is and how it works 2018.)

Microsoft on suoraan vastuussa osasta palvelumallista. IaaS (Infrastructure as a Service) mallissa Microsoft on vastuussa laitteistosta ja yrityksen vastuu on ainoastaan laitteistolla käytettävästä ohjelmistosta. Osa palveluista on täysin Microsoftin vastuualueella. Tähän kuuluu SaaS (Software as a Service) -malli, jossa palvelu myydään valmiina pakettina. Näiden välissä on myös PaaS (Platform as a Service), jossa yritys kontrolloi ainoastaan sovellusta ja sen dataa. Tällä jaetulla vastuulla yrityksen ei tarvitse huolehtia esimerkiksi kalliista laitteistokuluista tai konesalien tai verkkojen turvallisuudesta. (Shared responsibility in the cloud 2019.)

2.2 EntraID

EntraID on Microsoftin SaaS pohjainen identiteetin ja pääsyn hallintapalvelu. Palvelulla voi hallita sekä Azuren sisäisiä sovelluksia, että käyttäjäresursseja. Se tarjoaa ominaisuuksia organisaation eri jäsenille, kuten IT järjestelmänvalvojille ja sovelluskehittäjille. (What is Microsoft Entra ID? 2023.)

Työssä hyödynnettiin seuraavia EntraIDn alaisia osa-alueita:

- Identiteetinhallinta (Identity governance)
- Ehdollinen pääsy (Conditional access)
- Autentikaatio (Authentication).

Identiteetinhallinnan kautta pystytään hallitsemaan kaikkea käyttäjiin pääsyyn liittyvää. Se mahdollistaa myös automaattisen oikeuksien hallinnan, jonka avulla esimerkiksi työtehtävien vaihtuessa henkilön roolit vaihtuvat samalla. (What is Microsoft Entra ID Governance? 2023.) Työlle olennaisin osa-alue oli PIM, jonka ominaisuuksia käsiteltiin tarkemmin osiossa 3. Ehdollinen pääsy mahdollistaa hallinnan käyttäjä ja laiteidentiteetille. Sen pääasiallinen käyttötarkoitus on antaa tai kieltää pääsy tiettyihin resursseihin määritetyillä perusteilla. (What is Conditional Access? 2022.) Työn kannalta tärkeä käytäntö on tietyn autentikaatiovahvuuden vaatimus kirjautumisessa, jota käsitellään toteutuksen 5.1 osioissa Ehdollinen pääsy. Käyttäjän tulee aina todentaa kirjautumisensa jollakin tavalla ja näitä tapoja voidaan hallita autentikaation osa alueella (What is Microsoft Entra authentication? 2019). Monivaiheinen tunnistus ja salasanaton kirjautuminen olivat työn kannalta tärkeimpiä osioita.

Kaikki järjestelmänvalvojan tehtävät ovat roolipohjaisesti hallittuja. Koska aiheeseen liittyy ympäristön ylläpidon hallintaa, tiettyjä rooleja tarvitaan (Microsoft Entra built-in roles 2024). Työssä hyödynnettävät roolit olivat:

- Conditional Access Administrator
- Authentication Policy Administrator
- Privileged Role Administrator.

Käytetyt roolit ovat oikeutettuja, joka tarkoittaa, että ne mahdollistavat korkeiden oikeuksien tehtävien tekemisen, kuten käyttäjien kirjautumistietojen muuttamisen tai pääsyn rajattuun dataan (Privileged roles and permissions in Microsoft Entra ID (preview) 2023). Conditional access Administrator antaa täyden pääsyn muokkaamaan ehdollisen pääsyn konfiguraatiota. Authentication Policy Administrator antaa pääsyn muokata kaikkea autentikaatiometodeihin liittyvää paitsi käyttäjätason konfiguraatiota. Privileged Role Administrator antaa pääsyn kaikkeen rooleihin liittyvään, käyttäjätietojen erityisoikeuksien hallinnan (PIM) mukaan lukien. (Microsoft Entra built-in roles 2024.) PIM on tarkemmassa käsittelyssä osiossa 3.

2.3 Korkeiden käyttöoikeuksien etiikka

Työn aiheet keskittyivät osaksi etuoikeutetun datan käsittelyyn, kuten osiossa 2.2 kerrottiin. Oikeuksien laajuudesta ja omasta vastuusta eettiseen toimintaan tuli siis olla tietoinen käyttäessä kyseisiä rooleja.

Yksityisyyden kunnioittaminen on tärkeää, oli sitten kyseessä yksittäinen käyttäjä tai yrityksen laaja tieto. Kaiken etuoikeutetun tiedon käsittelyssä tulee olla tarkka ja sitä tulee pitää turvassa. Avoimuuden ja rehellisyyden periaatteina on, että luottamuksellista dataa ei väärinkäytetä tai manipuloida epäeettisiin tarkoituksiin. Vaikka kyseiseen dataan olisi pääsy, se ei tarkoita, että sitä voi tutkia ilman erillistä vaatimusta. Jos ympäristössä huomataan poikkeamia, niistä tulee informoida tarvittavia tahoja. Kaikista teoistaan tulee kantaa vastuu, se tarkoittaa työn läpinäkyvyyttä, prosessien dokumentointia ja virheiden korjaamista sekä niistä oppimista. Ammattimaisuus tarkoittaa kunnioittavaa käytöstä, standardien ja ohjeistusten mukaan toimimista ja omien taitojensa kehitystä. (Andersen 2024.)

Kun etiikkaa kunnioitetaan sekä työntekijät, että yritys hyötyvät. Maine ja luottamus yrityksen toimintaan paranee sekä sisäisesti, että asiakkaiden keskuudessa. Asiakkaat luottavat yrityksen toimintaan enemmän ja työntekijöiden moraali paranee, kun he tietävät omien arvojensa olevan yhteydessä yritykseen. Myös oikeudelliset riskit ja niihin liittyvät kulut ja haitat vähenevät. (Andersen 2024.)

3 PIM

Jokaisella käyttäjällä täytyy olla pääsy ainoastaan hänelle tarpeellisiin resursseihin ja palveluihin. Jos käyttäjätili vaarantuu, tarkat pääsyoikeudet voivat vähentävää aiheutuvaa haittaa. Organisaatioissa on myös aina henkilöitä, joilla on järjestelmävalvojatason oikeuksia. Näiden henkilöiden riskitaso on sen seurauksena korkeampi. Jotta korkean tason oikeuksia pystytään hallitsemaan tarkemmin, Microsoft on kehittänyt palvelun Käyttäjätietojen erityisoikeuksien hallinta (PIM). Sen avulla korkeampien oikeuksien aktivointi voidaan pyytää erikseen käyttäjältä. Jokaisesta oikeusaktivoinnista jää jälki järjestelmään ja se helpottaa tutkimusta väärinkäyttötilanteissa. Aktivointii täytyy myös esimerkiksi kirjata syy, miksi kyseinen aktivointi tehdään. (What is Microsoft Entra Privileged Identity Management? 2023.) PIM on jo laajassa käytössä, mutta toimeksiantajalla on vaatimus sen konfiguraation uudistamisen selvityksestä. Työssä käsiteltiin PIM:n eri osa alueita ja niiden parhaita käyttötapoja.

Permiso securityn blogikirjoituksen mukaan, vaikka PIM:n tarkoituksena on antaa tarkempi kontrolli pääsyoikeuksien hallintaan, se voi johtaa väärään turvallisuuden tuntemukseen. Teoreettisesti PIM antaa laajat mahdollisuudet hallintaan. Vähimpien etuoikeuksien periaate on PIM:n pohja. Käyttäjillä tulee aina olla vain tarvitsemansa roolit ja PIM antaa mahdollisuuden hallita niitä dynaamisesti. Oikeuksia ei tarvitse antaa pysyvästi, vaan niitä voidaan aktivoida tarvittaessa. Juuri ajoissa -käyttöoikeus on kyseisen periaate. Teoreettisesti riski sisäisille ja ulkoisille tietomurroille vähenee, kun laajemmat oikeudet eivät ole suoraan käytössä. Kontrolli antaa myös mahdollisuuden valvoa oikeuksia ja niiden aktivointeja. Valvonnalla pystytään huomaamaan poikkeuksellisia aktivointeja ja tutkimaan niitä. Kaikki mainitut ominaisuudet auttavat yritystä pysymään sääntelyvaatimuksien yläpuolella ja lisäävät henkilökohtaista vastuuta rooliaktivointien perusteluiden kautta. (Eades 2023.)

Kuitenkin todellisuudessa toteutuksella on käytännön haasteita. Oikeuksia saatetaan myöntää henkilöille ilman suurempia perusteita, koska ne eivät ole aktiivisina jatkuvasti. Tämä voi kuitenkin johtaa suurempaan määrään käyttämättömiä ja liian kattavia oikeuksia. Oikeuksien tarkempi laajuus nähdään joidenkin tahojen mielestä hyvänä asiana. Käyttäjät voivat valita vain tarvitsemansa roolit ja täten vahinkojen määrä konfiguraatioissa vähenee. Tämä ei kuitenkaan ole kirjoittajan mielestä erityisen hyvä syy, koska käyttäjällä ei tulisi olla laajaa pääsyä, jos hän tekee helposti vir-

heitä. Roolien aktivointien perustelut ovat myös useasti merkityksettömiä, joka tekee mahdollisten väärinkäytösten tutkimisesta haasteellisempaa. Erityisesti, jos käyttäjälle on asetettu Global Administrator -rooli eli täysi pääsy koko ympäristöön, hän voisi tässä tilanteessa aktivoida sen ilman mitään erityistä perustetta. Permison tutkimuksen mukaan Global Administrator -roolia aktivoitiin myös liian usein. Jos rooli aktivoidaan enemmän kuin 5 kertaa kuukaudessa, käyttäjä joko hyödyntää roolia tarpeettomasti tai hänellä voisi olla tarve aktivoida rooli pysyvästi. MFA vahvistuksen toteutus ei myöskään ole kattava oletuksena. Koska vahvistus tehdään jo alkuperäisen kirjautumisen aikana, sitä ei kysytä uudestaan. (Eades 2023.)

Tässä vaiheessa voisi siis pohtia, mitä hyötyä koko palvelusta on. Kaikki hyöty, jota tähän asti on saatu, on lisävalikko oikeuksien aktivointiin. Sitä voisi periaatteessa kutsua turvaksi epäselvyyden kautta (security through obscurity), jossa turvallisuutta pyritään lisäämään piilottamalla järjestelmän elementtejä (Borges 2024). Eadesin (2023) sanoin” In all seriousness, the process has been reduced to a procedural formality, where “just-in-time” access becomes scarcely distinguishable from “all-the-time” access”. Hänen mukaansa tämä kuitenkin tarkoittaa, että konfiguraatio tulee ottaa uudelleen käsittelyyn ja sitä tulee parantaa oletusarvoista. Vaatimalla tarkempia aktivointien syitä, poikkeustilanteiden auditointia voidaan parantaa. Perusteluille voisi olla myös käytössä tietty formaatti, jotta aktivointeja varten voidaan luoda monitorointia. MFA vahvistusta voidaan parantaa hyödyntämällä EntraID:n ehdollisen pääsyn käytäntöä, jonka avulla erillisen vahvistusmetodin käyttö voidaan pakottaa. On kuitenkin mahdollista, että käyttäjä aktivoi roolin ja tulee kaapatuksi sen jälkeen. Tätä varten voidaan esimerkiksi asettaa laitevaatimuksia, jotka estävät kirjautumisen muilta kuin yrityksen laitteilta. Roolien aktivointiin voidaan myös sisällyttää hyväksyjiä, joka parantaa kontrollia ja turvallisuutta. Tämä kuitenkin toimii PIM:n juuri ajoissa-käyttöoikeuden periaatetta vastaan, koska aktivointi on toisesta henkilöstä kiinni. (Eades 2023.) Myös Sørensenin (2024) mukaan, aktivointien vahvistaminen toisella henkilöllä on kaksipuoleinen aihe. Se antaa samalla paremman turvallisuuden tason, koska toinen työntekijä tulee aktivoinnin väliin. Se voi kuitenkin johtaa myös huonoon käyttäjäkokemukseen, koska roolien aktivoinnissa voi kestää pitkään. Tämä huomioiden roolien tärkeys ja vaaditun turvallisuuden taso tulee ottaa huomioon, sillä jokainen rooli ei välttämättä tarvitse erillistä vahvistusta. (Sørensen 2024.) Aktivointien monitorointi on myös tarpeellinen ominaisuus, sitä ei kuitenkaan voida toteuttaa PIM:n kautta, vaan tarvitsee jonkin toisen palvelun tueksi. Yleisellä tasolla roolien konfiguraatio tulisi olla mahdollisimman tarkka ja työtehtäviä vastaava. Pääsyoikeuksia tulee myös auditoida säännöllisesti ja ylimääräisiä oikeuksia ottaa pois käytöstä. (Eades 2023.)

4 Autentikaatio

4.1 Salasanaton kirjautuminen

Autentikaatiolla on suuri merkitys missä tahansa organisaatiossa. Salasanaton kirjautuminen on Microsoftin suositusten mukaan turvallisin tapa toteuttaa se. Kirjautumisprosessi muuttuu myös yksinkertaisemmaksi käyttäjän näkökulmasta. Toteutustapana voisi olla esimerkiksi sormenjälki ensimmäisenä ja puhelin toisena autentikaatio-tapana. Tällä tavalla salasana poistetaan yhtälöstä, joka samalla myös estää sen vuotamisen ulos organisaatiosta. (What authentication and verification methods are available in Microsoft Entra ID? 2024.) Yleisellä tasolla monivaiheisen tunnistamisen periaatteena on hyödyntää ainakin kahta kolmeen kategoriaan kuuluvista metodeista. Jokin käyttäjän tiedossa oleva asia, jotakin hänen omistamaansa ja jotain, jota hän on. Näistä esimerkkejä voisi olla, PIN-koodi, fyysinen laite ja sormenjälki. (How it works: Microsoft Entra multifactor authentication 2020.)

Salasanojen käyttöön sisältyy paljon ongelmia. Kenties merkittävin ongelma on saman salasanan käyttäminen usean eri palvelun kesken. Käyttäjä voi mukavuuden nimissä käyttää samaa salasanaa kaikilla tileillään, jotta useaa salasanaa ei tarvitsisi muistaa. Vahvojen salasanojen periaatteet liittyvät myös samaan aiheeseen. Siinä vaiheessa, kun salasanan tulee olla pitkä ja sen tulee sisältää kirjaimia numeroita ja merkkejä, muistamisesta tulee yhä vaikeampaa. Tämä johtaa yhä helpommin niiden kirjoittamista esimerkiksi paperille tai muuhun turvattomaan muotoon. Vaikka vahva salasana estäisikin tietojenkalastelijoita suoraan arvaamasta niitä, käyttäjä on silti haavoittuva tietojen kalasteluyrityksille ja haittaohjelmille, jotka monitoroivat näppäimenpainalluksia. (Why Going Passwordless is the Future of Cybersecurity n.d.)

4.2 FIDO2

Jos turvallisuutta halutaan vielä yksi askel eteenpäin, FIDO2 avaimet ovat yksi mahdollisuuksista turvaamaan korkean riskin käyttäjiä. Microsoftin mukaan muiden autentikaatiometodien hyödyntäminen sisältää ulkoisia riskejä. Puhelimen soitto- ja viestiominaisuudet ovat riippuvaisia puhelinyhteydestä. Esimerkiksi laaja palvelukatkos voi estää kirjautumisen täysin. Ne ovat myös altistuneita yhteyden kaappaamiselle. Lähes jokainen saatavilla oleva metodi on myös haavoittuvainen reaaliaikaiselle tietojenkalastelulle. Tästä poikkeuksia ovat kuitenkin FIDO2 avaimet ja Windows Hello (Privileged access: Accounts 2024.)

FIDO2 on avoin autentikaatio-standardi ja on FIDO Allianssin kehittämä. Allianssi koostuu eri yritys- ja valtiotoimijoista. Standardi perustuu julkisen ja yksityisen avaimen pariin, joka parantaa samalla turvallisuutta ja käyttäjäkokemusta yksinkertaistamalla kirjautumisprosessia. Kun FIDO2-laite rekisteröidään palveluun, uniikki avainpari luodaan. Julkinen avain jaetaan palvelulle ja yksityinen avain pysyy laitteessa. Kirjautumisprosessissa palvelu lähettää haasteen laitteelle, joka vahvistetaan yksityisellä avaimella. Koska avainparit ovat uniikkeja jokaiselle rekisteröidylle palvelulle, sillä ei voida vahingossakaan kirjautua tietojenkalastelu-sivustolle. Jotta laite pystyy varmistumaan käytättäjän identiteetistä, se tulee vahvistaa esimerkiksi PIN-koodilla tai fyysisellä tunnisteella, kuten sormenjäljellä. FIDO2 kykeneviä laitteita on kahdenlaisia, erillisiä fyysisiä avaimia ja johonkin toiseen laitteeseen, kuten puhelimeen liitettyjä. (What is FIDO2? N.d.)

Koska kaikki autentikaatioon liittyvä tapahtuu FIDO2-laitteessa, sen on oltava fyysisesti yhteydessä esimerkiksi tietokoneeseen tai sen lähellä. Tämän avulla kukaan ei voi kirjautua laitteelle ilman kyseistä avainta. Avain ei myöskään jaa luottamuksellista autentikaatio-tietoa palveluun, johon kirjautumista ollaan tekemässä (What Is FIDO2 and How Does It Work? Passwordless Authentication Advantages & Disadvantages 2025). Tämän perusteella kirjautumisprosessissa ei ole mitään, mikä voisi vuotaa ulos käyttäjältä digitaalisesti. Tätä tukee myös Mehtälän (2024, 45-46, 50, 52-53.) tutkimus, jonka mukaan FIDO2 standardia hyödyntävät avaimet ovat immuuneja testatuille tietojenkalasteluohjelmille. Testeissä käytettiin ohjelmia, joiden avulla luotiin väärennettyjä sivuja tietojenkalastelua varten. FIDO2 autentikaatio ei antanut missään esimerkissä hyökkääjälle pääsyä testattavaan käyttäjään. (Mehtälä 2024, 45-46, 50, 52-53.)

4.3 Fyysiset avaimet

Työ keskittyi Yubicon valmistamiin YubiKey 5C NFC ja YubiKey 5 NFC avaimiin. Näiden ainoa ero on liitäntäportti, USB-A tai USB-C. Ne tukevat esimerkiksi FIDO2, PIV, OTP ja NFC ominaisuuksia, jotka ovat toimeksiantajan vaatimuksissa. Avaimet ovat myös suoraan yhteensopivia Google Account, AWS Identity and Access Management (IAM) ja Microsoft Azure AD kanssa. Yksittäisen avaimen hinta on noin 60 €, joten se rajoittaa laajentamista suurelle määrälle työntekijöitä (YubiKey 5 NFC N.d.) Tämä työ keskittyi kuitenkin ainoastaan Azuren toimintaan. Eri valmistajien välistä vertailua ei tulla toteuttamaan, koska Yubikey on jo rajoitetussa käytössä yrityksessä ja todettu toimivaksi.

PIN-koodin vahvuutta ei voi erikseen määrittää toisten palveluiden kuten EntraIDn kautta. Tämä johtuu FIDO2 avaimen arkkitehtuurista, jossa kaikki autentikaatio tapahtuu itse avaimessa, kuten edellä mainittiin. Sen takia avainten kyvyistä tulee olla tietoinen ennen niiden valintaa. Yubikey 5 sarjan avaimissa PIN-vaatimus on neljämerkkinen, saatavilla on myös esimerkiksi FIPS sarjan avaimia, joissa vaatimus on kuusi merkkiä ja käytössä on myös kiellettyjen PIN-koodien lista. (Bucy 2021). Käyttöönottajalla tulee siis olla selvä suunnitelma omista tarpeistaan ja valita tällä perusteella sopiva avaintyyppi.

PIN-koodien vaatimuksista puhuttaessa, esimerkiksi NIST vaatii kuusimerkkistä koodia (Temoshok, Fenton, Choon, Lefkovitz, Regenscheid, Galluzzo, Richer 2024, 38). Kuitenkin Markert, Bailey, Golla, Dürmuth & Aviv (2021, 2-3) osoittavat, että kuusinumeroinen PIN-koodi ei tuo lisää turvallisuutta, koska käyttäjä valitsee suuremmalla todennäköisyydellä helpommin arvattavan koodin. Koska jopa kuusinumeroiset PIN-koodit ovat heikkoja ilman muuta rajoitusta, niitä tulee käyttää jonkinlaisen lukitus tai viiveominaisuuden kanssa. Puhelimissa tämä voi olla rajoitus, kuinka monta koodia voidaan asettaa tietyssä aikamäärässä. (Markert ym. 2021, 2-3). Yubikeyn PIN-koodista puhuessa, avaimesta tulee käyttökelvoton kahdeksan väärän yrityksen jälkeen ja se tulee resetoida. Resetoinnin jälkeen avain tulee rekisteröidä uudestaan käyttäjälle. (Bucy 2021.)

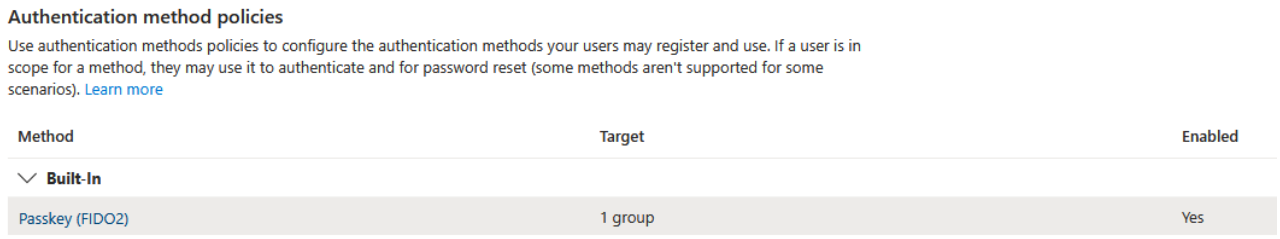
PIN-koodien estoluettelojen tarpeellisuus on myös tärkeä kysymys. Markert ja muut (2021 2-3.) käsittelivät tutkimuksessaan myös kyseistä aihetta. Testauksessa käytettiin useita pieniä ja laajempia listoja. Tuloksien mukaan turvallisuus ei parantunut merkittävästi. Simuloitu hyökkääjä pystyi arvaamaan koodin melkein yhtä hyvin, vaikka estolista oli käytössä. Tämän tuloksen johtopäätöksenä listojen tulisi olla huomattavasti pidempiä, jotta niistä olisi varsinaista hyötyä. Kuitenkin, jos listojen pituutta jatkettaisiin suuremmiksi, käyttäjäkokemuksesta huononee samaa tahtia. (Markert ym. 2021, 2-3).

Yubicon suositus on, että henkilöllä olisi kaksi fyysistä avainta esimerkiksi tapauksessa, jossa toinen avain katoaa (Spare YubiKeys. N.d.) Tämä ei ole kuitenkaan merkittävä ongelma organisaatiossa, sillä henkilökohtaisia autentikaatiometodeja ja -laitteita pystytään resetoimaan helposti. (Manage user authentication methods for Microsoft Entra multifactor authentication 2024.) Tässä tilanteessa tulee kuitenkin olla varma henkilön identiteetistä ja se täytyy varmistaa toimeksiantajan määrittämän prosessin kautta.

5 Toteutus

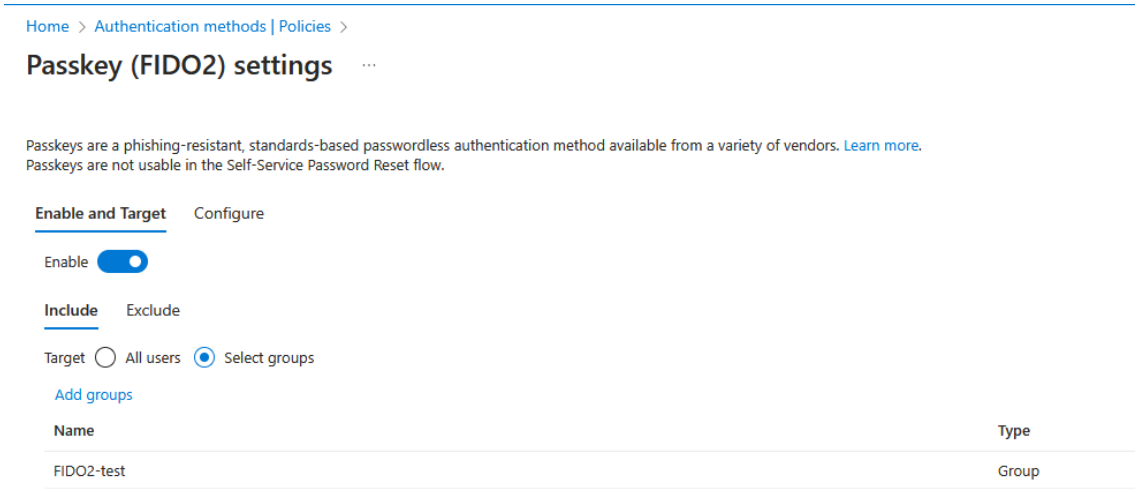
5.1 Salasanaton kirjautuminen

Jotta FIDO2 avaimet voitiin ottaa käyttöön, käyttäjille saatavilla olevia autentikaatiometodeja tulee muokata EntraID:n ”Authentication methods” -valikosta, joka on kuvattuna Kuviossa 1. FIDO2 metodiin tuli lisätä haluttu käyttäjäryhmä, jotta avaimen pystyi lisäämään omalle käyttäjälle.



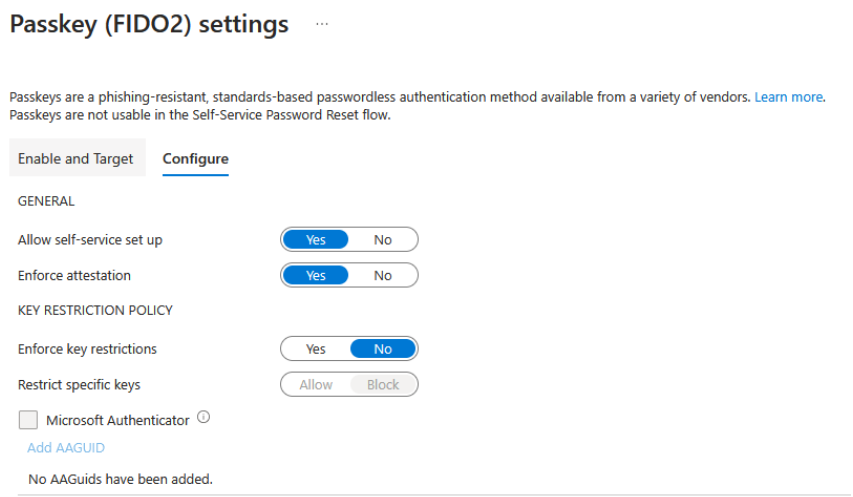
Kuvio 1. Autentikaatiotapojen valikko.

Haluttu käyttäjäryhmä tulee valita autentikaatiometodille, jotta se voidaan ottaa käyttöön. Tässä tapauksessa testiryhmä, jossa oma käyttäjä on ainut jäsen. (Kuvio 2)



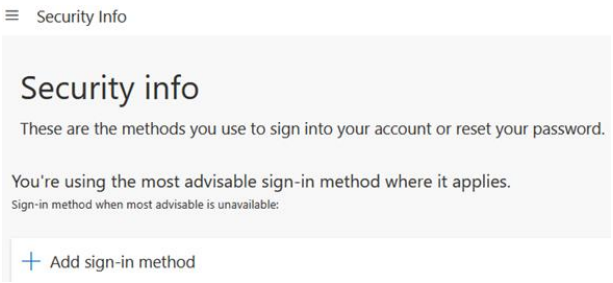
Kuvio 2. Azure-ympäristön FIDO2 konfiguraatioon sisältyvät ryhmät.

Asetuksia voi myös konfiguroida tarkemmin turvallisuusvaatimusten mukaisesti, kuten Kuviossa 3. on kuvattu. ”Enforce attestation” vaatii avainta ilmoittamaan tunnistekoodin, jonka avulla sen alkuperäisyydestä voidaan varmistua. Jos halutaan rajoittaa vain tiettyjen avainten käyttöä, niitä voidaan estää tai hyväksyä ”Restrict specific keys” – valikosta (Enable passkeys (FIDO2) for your organization 2024.)

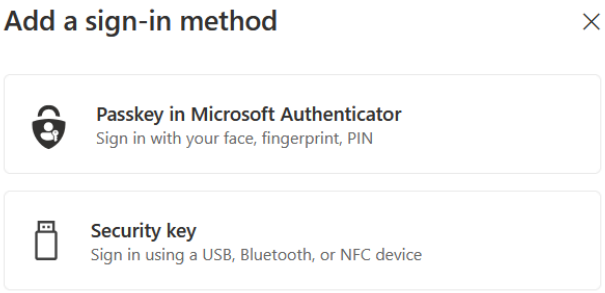


Kuvio 3. Azure-ympäristön FIDO2 konfiguraatio.

Avaimen käyttöönotto tapahtui lisäämällä se sisäänkirjautumismetodiksi käyttäjän profiilista, joka on saatavilla osoitteessa https://mysignins.microsoft.com/security-info. Fyysistä avainta lisättäessä tuli valita vaihtoehto ”Security key” (Kuviot 4 ja 5).

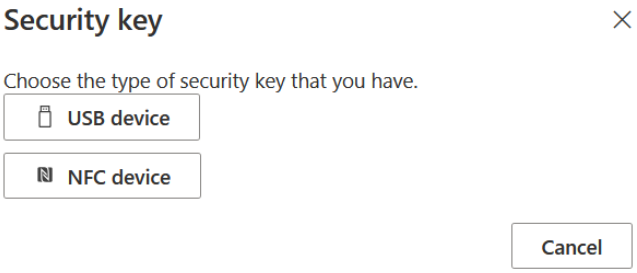


Kuvio 4. Autentikaatiometodin lisääminen käyttäjälle.



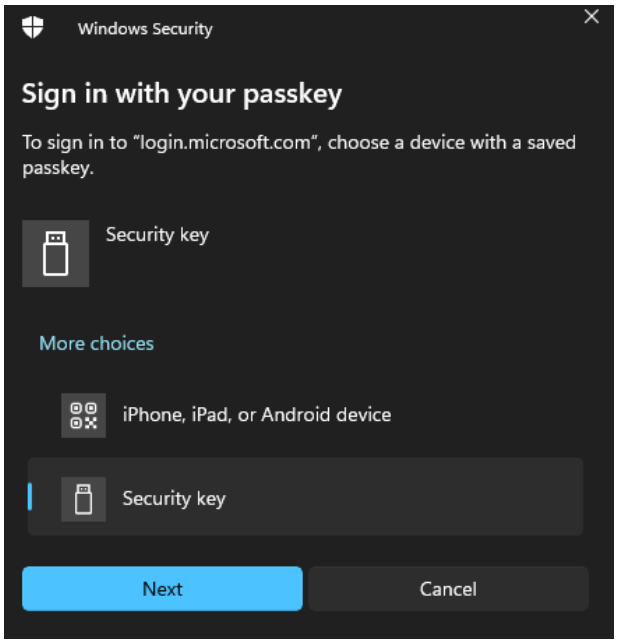
Kuvio 5. FIDO2-avaimen lisääminen käyttäjälle.

Avaimen tyyppi tuli valita seuraavaksi. Tällä valinnalla ei ollut merkitystä työn kannalta, koska avain saadaan lisättyä kummallakin vaihtoehdolla. Kuitenkin, jos tarpeena olisi hyödyntää NFC ominaisuutta tulee valita se vaihtoehto, jotka ovat kuvattuna Kuviosta 6.



Kuvio 6. FIDO2-avaimen tyypin valinta.

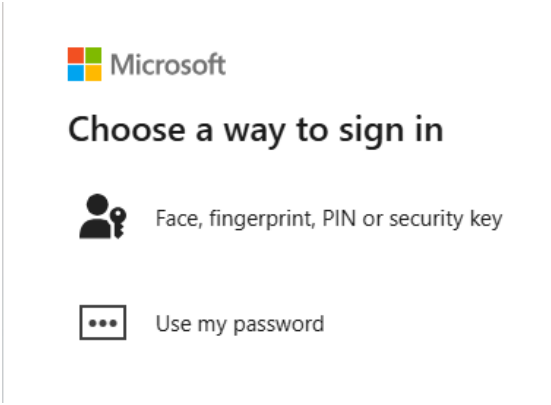
Kun uusi avain otettiin käyttöön, tuli määrittää PIN-koodi. Seuraavaksi avaimen sensoria tuli painaa, jonka jälkeen lisäys oli valmis. Avaimelle tuli myös asettaa nimi, jolla sen pystyi tunnistamaan. Avain oli saatavilla seuraavan kirjautumisen yhteydessä (Kuvio 7). Avain pyysi myös PIN-koodin, ja sensorin painamisen vahvistukseksi.



Kuvio 7. FIDO2-avaimen hyödyntäminen kirjautumisessa.

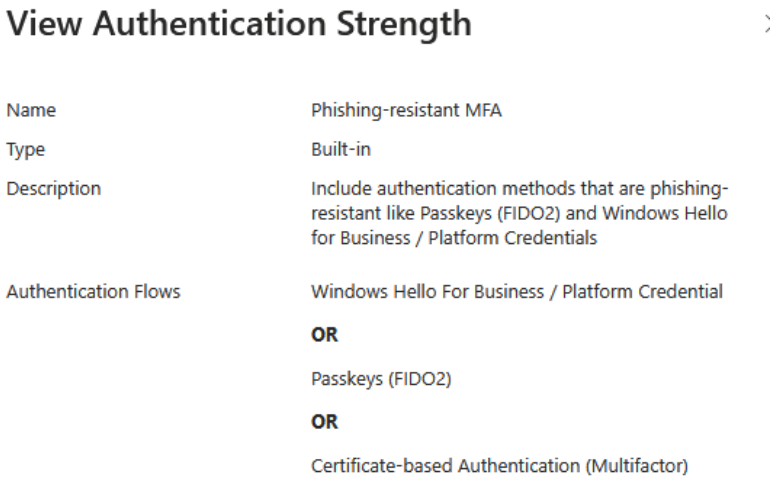
Conditional access policy

Jos konfiguraatio jätetään tähän, kuviosta 8 näkee, että salasanan käyttäminen on vielä mahdollista. Tämä halutaan estää, joten uusi käytäntö tulee luoda EntraID:n autentikaatiovahvuuksiin.

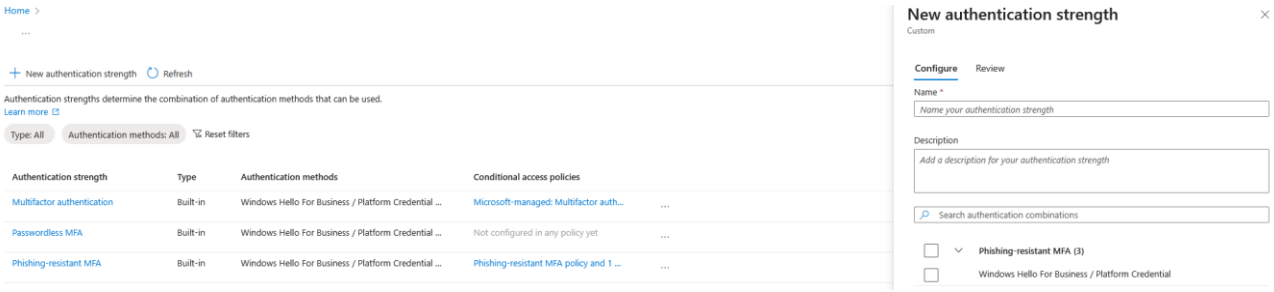


Kuvio 8. Salasana on vielä mahdollinen vaihtoehto.

Tiettyä autentikaation vahvuuskonfiguraatiota tuli hyödyntää, jotta vain halutut autentikaatiometodit saatiin käyttöön. Tätä opinnäytetyötä varten esimerkkinä hyödynnettiin Microsoftin sisäänrakennettua ”Phishing-resistant MFA” vahvuutta (Kuvio 9). Konfiguraatio normaalille salasanattomalle autentikaatiolle toimii samalla periaatteella, silloin vahvuutena tulisi käyttää vaihtoehtoisesti ”Passwordless MFA”. Uuden vahvuuden voi myös määrittää vastaamaan juuri niitä metodeja kohtaan mitä halutaan käytettävän (Kuvio 10).

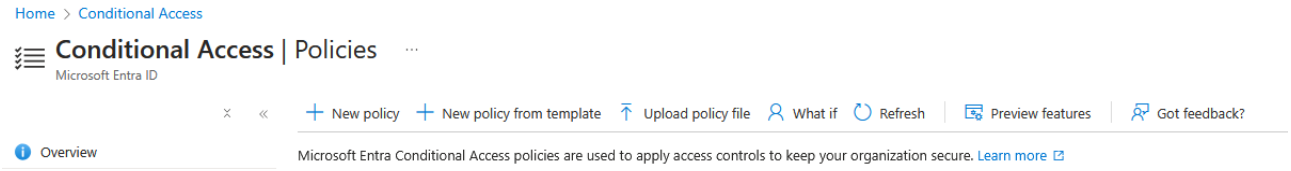


Kuvio 9. Esimerkissä hyödynnettävän autentikaation vahvuus.



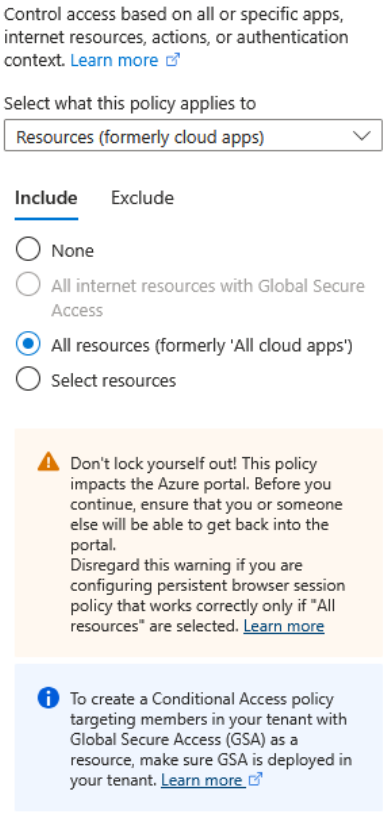
Kuvio 10. Uuden autentikaatiovahvuuden määrittäminen.

Työssä käsitellyllä konfiguraatiolla mahdollistetaan perustason autentikaatio. Muita mahdollisia konfiguraatioita, kuten riskikäyttäjiin liittyviä ei käsitelty tässä työssä. Uusi käytäntö tuli luoda hyödyntäen edellä mainittua autentikaatiovahvuutta. Käytäntöjen lisääminen on esitettynä kuviossa 11.

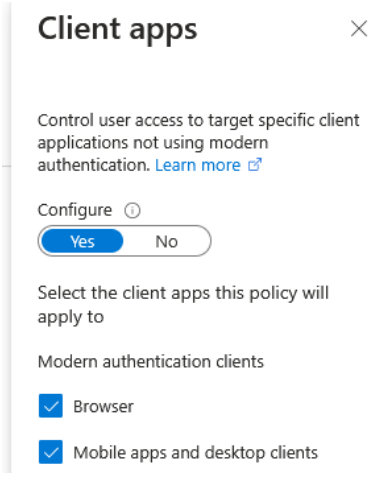


Kuvio 11. Uusien käytäntojen luonti.

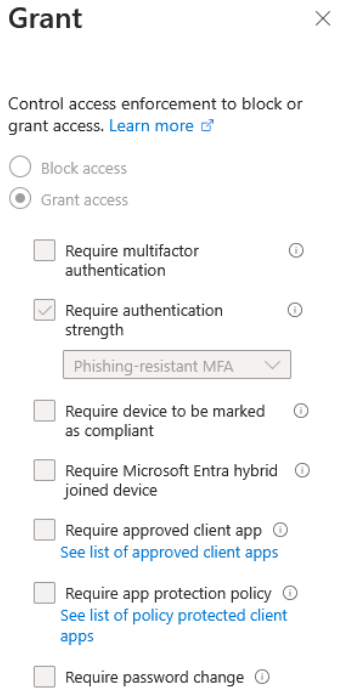
Kuvioissa 12, 13 ja 14 kuvataan käytännön asetusten määrittäminen. Käytäntöön tuli määrittää halutut resurssit. Koska kyseessä on organisaation laajuinen autentikaatio, kaikki resurssit tuli sisällyttää. Kaikki sovellukset otetaan käytännön alle samasta syytä. Itse käytännön vaatimuksiin tulee määrittää käytettävä autentikaatiovahvuus, joka mainittiin kuviossa 9.



Kuvio 12. Resurssien pääsynhallinta.

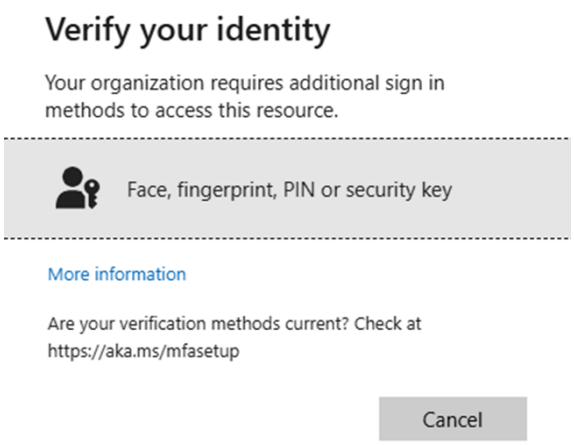


Kuvio 13. Hallinta, mihin sovelluksiin sääntö vaikuttaa.



Kuvio 14. Autentikaation vahvuuden valinta.

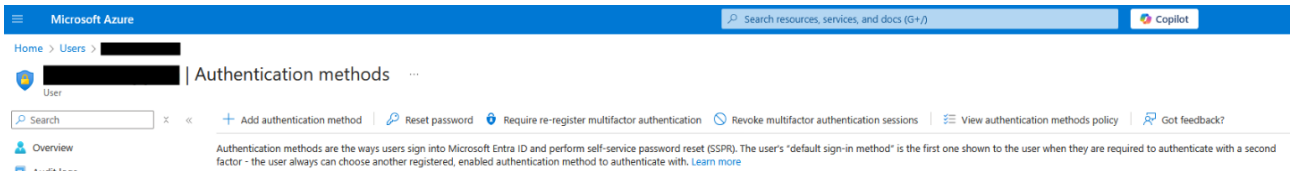
Testauksessa käytetyt käyttäjät tuli myös sulkea pois olemassa olevista MFA-konfiguraatiosta, jotta ainoastaan uudet tulivat käyttöön. Muutoksen jälkeen salasanaa tai muita määrittämättömiä metodeja ei voida enää käyttää kirjautumiseen, kuten kuviosta 15. nähdään.



Kuvio 15. Uusi konfiguraatio toiminnassa.

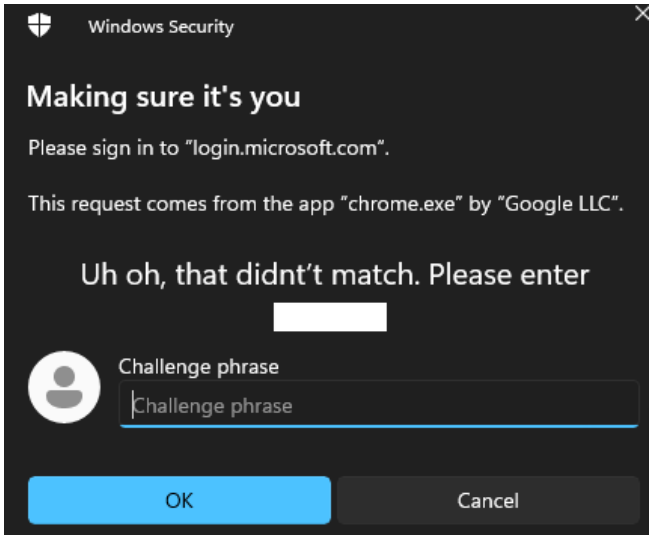
Poikkeustilanteissa toiminta

Järjestelmänvalvojien konfiguraatiosta puhuessa, jos FIDO2 avain on ainoa tapa kirjautua käyttäjälle, voidaan päätyä tilanteeseen, jossa käyttäjä lukkiutuu ulos. Mahdollisia tapauksia voisi olla esimerkiksi PIN-koodin unohtuminen tai avaimen kadottaminen. Tämänlaisessa tapauksessa metodeja voidaan hallita käyttäjäkohtaisesti. Kuviossa 16. on esitetty Azuren valikko hallintaan. Vanha avain voidaan poistaa ja uusi lisätä.



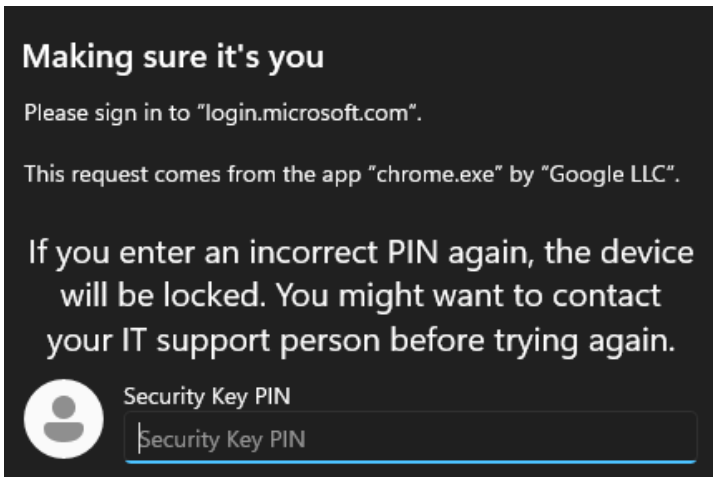
Kuvio 16. Henkilökohtaisten autentikaatiometodien hallinta.

Kun avaimen PIN-koodi oli kirjoitettu väärin seitsemän kertaa, esiin tuli näkymä, joka vaati kirjoittamaan haastelauseen. Näkymä on kuvattuna kuviossa 17. Tässä vaiheessa PIN-koodi on kirjoitettu väärin seitsemän kertaa ja tämä pysäyttää käyttäjän lukitsemasta avaintaan.



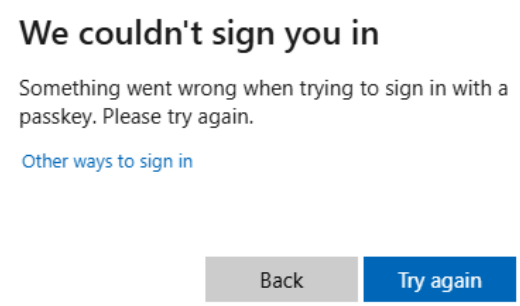
Kuvio 17. Haastelause kirjautumisen yhteydessä.

Haastelauseen kirjoittamisen jälkeen, ruutuun ilmestyi varoitus viimeisestä yrityksestä, joka on kuvattuna kuviossa 18. Kun PIN-koodi kirjoitettiin vielä kerran väärin, avain lukitsi itsensä.



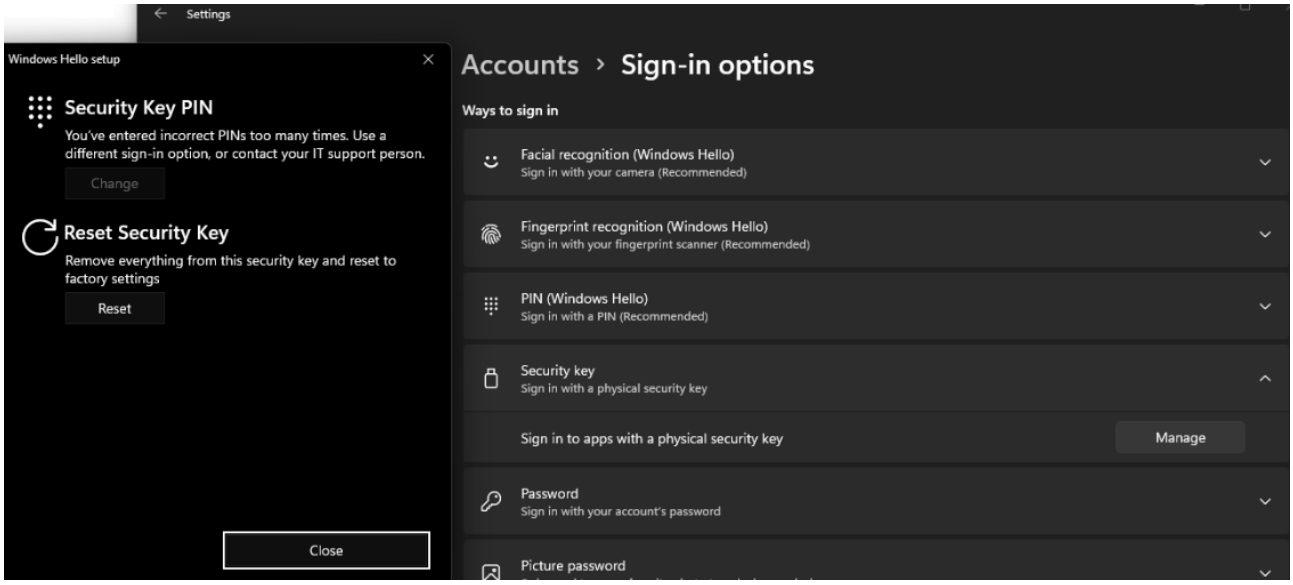
Kuvio 18. Varoitus avaimen lukkiutumisesta.

Kun avain lukkiutui, sitä ei voitu enää käyttää kirjautumaan käyttäjille. Prosessi pyysi koskettamaan avaimen sensoria, mutta sen jälkeen PIN-koodin ruutu ei tullut näkymiin vaan prosessi keskeytyi (Kuvio 19).



Kuvio 19. Kirjautumisen yritys avaimen lukkiuduttua.

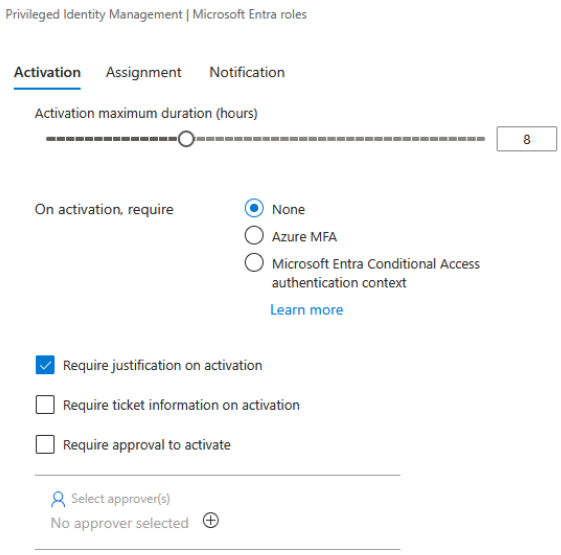
Tässä vaiheessa ainoa mahdollisuus oli resetoida avain, jotta sen pystyisi lisäämään takaisin käyttäjälle. Resetointi tyhjentää avaimeen tallennetut käyttäjät kokonaan ja mahdollistaa sen rekisteröinnin uudestaan. Prosessi on kuvattuna kuviossa 20.



Kuvio 20. FIDO2-avaimen hallinta Windows-asetuksista.

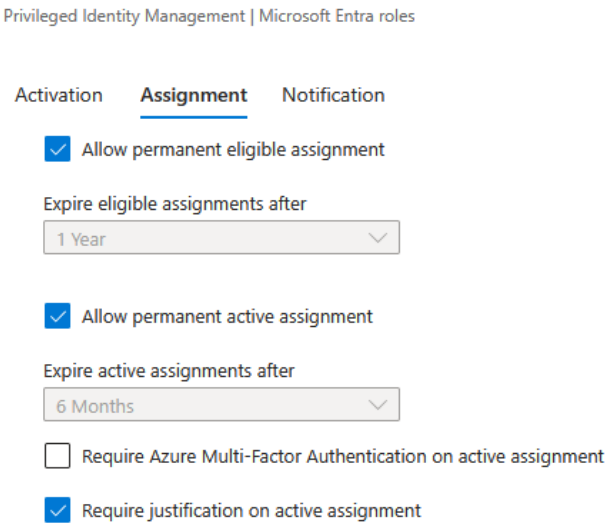
5.2 PIM

Roolien asetuksia voidaan hallita tarkasti, kuviossa 21 kuvatusta valikosta. Eri rooleilla on erilaisia vaatimuksia niiden laajuuden mukaan. Jotkut roolit tarvitsevat erillisen MFA vahvistuksen ja esimerkiksi tietoa aktivoinnista. Nämä ovat määritettynä yrityksen puolesta. Tästä näkymästä voitiin myös valita halutut hyväksyjät.



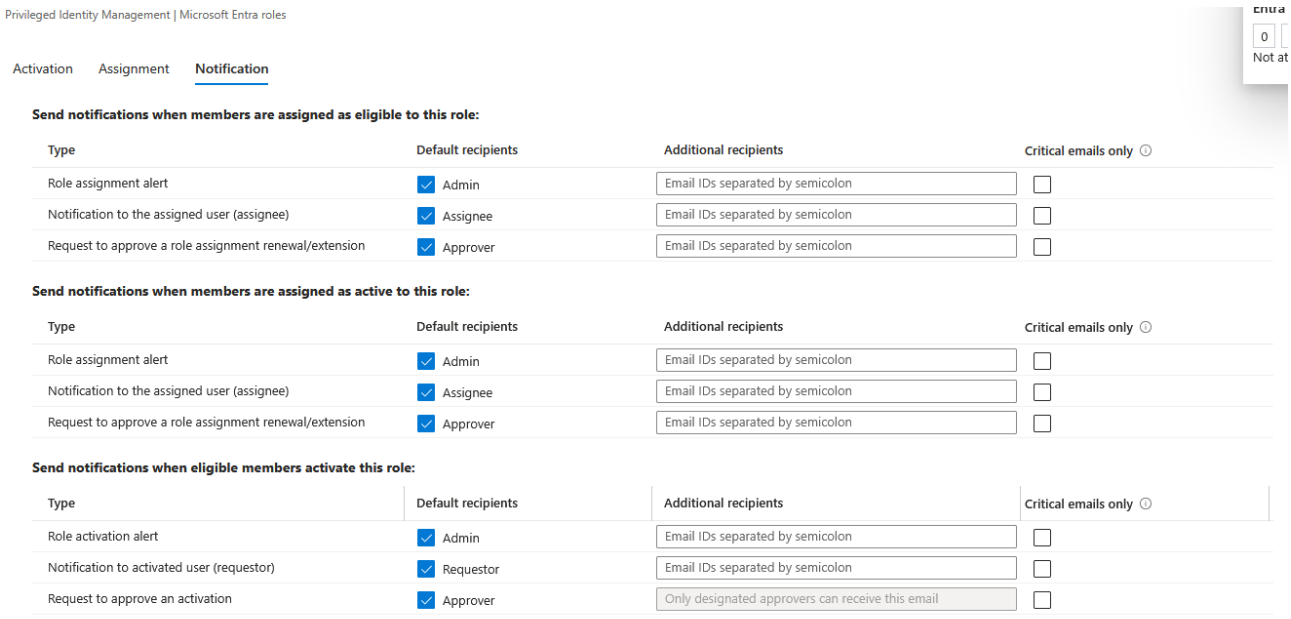
Kuvio 21. PIM roolien aktivointiasetukset.

Roolien aktivointipituuksia voidaan toimeksiantovälilehdeltä, joka on kuvattuna kuviossa 22. Ensimmäinen valinta määrittää kuinka pitkäksi ajaksi rooli voidaan asettaa käyttäjälle. Toisessa valinnassa asetetaan, kuinka pitkään rooli voidaan asettaa aktiiviseksi käyttäjälle. Aktiiviseen aktivointiin voidaan myös vaatia erikseen MFA-vahvistus ja erillinen syy.



Kuvio 22. PIM-roolien aktivointien pituuksien hallinta.

Ilmoitus-välilehdeltä voidaan hallita kuka saa ilmoituksia mistäkin rooleihin liittyvistä tapahtumista, joka on kuvitettuna kuviossa 23. Ilmoituksiin kuuluu roolien aktivointi ja asettaminen käyttäjälle. Jokaisessa ilmoituksessa on erikseen määritetyt oletus vastaanottajat, niihin voidaan kuitenkin lisätä myös muita henkilöitä sähköpostien kautta.



Kuvio 23. PIM-roolien ilmoitusasetukset.

6 Pohdinta

Autentikaation muutos keskittyi salasanattoman kirjautumismetodien käyttöönottoon ja sen tuomiin hyötyihin. Normaalien käyttäjien tilanteessa Microsoft autentikaattori toimii riittävän hyvänä tapana, mutta järjestelmänvalvojat, joilla on pääsy oikeutettuihin rooleihin tarvitsevat turvallisemman, tietojenkalastelulle immuunin tavan, kuten fyysisen FIDO2 avaimen. Fyysiset avaimet helpottavat myös kirjautumisprosessia, joten syitä olla ottamatta niitä käyttöön yrityksessä on vähän. Hinta on yksi tekijä erityisesti, jos yrityksellä on paljon työntekijöitä. Avaimet tekevät kaiken autentikaatioon liittyvän sisäisesti, joka voidaan nähdä sekä hyvänä, että huonona asiana. Hyvänä puolena on, että mikään autentikaatio-prosessiin liittyvä yksityinen tieto ei voi vuotaa ulos avaimelta, kuitenkin huonoa on se, että esimerkiksi PIN-vaatimukset ovat täysin laitekohtaisia. Tämän takia ostettavan avaimen kyvyistä tulee olla tietoinen etukäteen. PIN-koodi on siis täysin laitekohtainen, joten sen unohtuminen tekee kirjautumisesta mahdotonta sen unohtuessa. Tämä on pääasiallisesti hyvä asia ja ei ole haittanakaan merkittävä yritysympäristössä, koska metodeja voidaan hallita toisten järjestelmänvalvojien puolesta. Vastaten ensimmäiseen tutkimuskysymykseen salasanattomalla kirjautumisella ja erityisesti FIDO2 avaimilla voidaan parantaa autentikaatiota ja työn mukaan, valitut Yubikey 5 -avaimet vastaavat tarpeita.

Autentikaatioon liittyen muutamaa asiaa ei käsitelty työssä. Yksi tärkeä kysymys on, mitä tapahtuu, kun käyttäjän autentikaatiometodit resetoidaan. Jos käyttäjällä on mahdollista kirjautua sisään ainoastaan FIDO2 avaimella ja kyseinen metodi poistetaan käyttäjältä, pystyykö hän lisäämään uuden avaimen itsenäisesti. Samaan aiheeseen liittyy myös tilanne, jossa käyttäjän vaatimus FIDO2 avaimesta otetaan käyttöön ennen kuin hän on rekisteröinyt avainta omalle käyttäjälleen. Tämä vaatii lisätutkimusta varsinaiseen toteutukseen. Pohdintana on myös, halutaanko tämänlaista vapautta käyttäjälle, vai pitäisikö tämänlaisissa tilanteissa mennä aina järjestelmänvalvojan kautta.

Roolipohjaisten oikeuksien hallinnan puolesta, pohdintana on, minkälainen PIM konfiguraatio vastaa parhaiten yrityksen tietoturva-vaatimuksia. Vaikka erillisten aktivointien vaatimus lisää teoriassa turvallisuutta, se voi tarkoittaa, että työntekijät hyväksyvät niitä ajattelematta asiaa sen enempää, koska henkilökohtainen työtaakka lisääntyy. Voisi jopa sanoa, että tästä tulee uusi työtehtävä, varsinkin jos aktivointien vahvistuksia tulee paljon yksittäiselle henkilölle. Muiden käyttä-

jien kokemus huononee myös hieman tämän muutoksen kautta, koska roolien aktivoinnissa menee pidempään. Kuitenkin vahvistus on kuitenkin hyvä tapa lisätä välikäsi erityisesti korkeiden oikeuksien rooleihin, jotta mahdollisia väärinkäyttötilanteita voitaisiin saada kiinni. Koska roolien hyväksyjien valitsemiseen ei ole erityisiä määritettyjä käytäntöjä Microsoftin puolesta, se riippuu yrityksen asettamista vaatimuksista ja ohjeistuksesta. Mahdollisuuksina tässä on, että yksi tiimi on vastuussa kaikista hyväksymisistä tai jokainen tiimi vastaa omista rooleistaan. Mukaan tulee myös huomioida esimerkiksi työntekijöiden loma-ajat ja mahdolliset omat poissaolot. Aktivoinneissa vaatimuksena tulisi olla myös selvä selitys siitä, mihin roolia ollaan käyttämässä. Tämä lisää käyttäjän vastuuta tekemistään muutoksista ja parantaa väärinkäyttötilanteiden auditointia. Auditoinnin tulisi myös olla säännöllisesti tehtävä asia, jotta poikkeavia tilanteita voidaan havaita. Vastaten toiseen tutkimuskysymykseen, roolipohjaista oikeuksien hallintaa voidaan parantaa määrittämällä tarkka prosessi kunkin roolin aktivointiin, hyväksyjien tarpeeseen ja roolien yleiseen konfiguraatioon.

Työssä ei käsitelty PIM toteutusta muun kuin konfiguraation kautta. Prosessit tulee määrittää erikseen yrityksen puolesta vastaamaan tarvittavia osa-alueita. Roolien aktivointia ei myöskään testattu työssä ja aktivointipyyntöjen toteutukseen liittyvät aiheet jäivät työn ulkopuolelle. Oletusarvona ilmoitukset tulevat käyttäjän sähköpostiin. Kuitenkin tehokkaampi tapa toiminnalle voisi olla, että viestit saataisiin ohjattua suoraan jollekin Teams-kanavalle, jotta ne olisivat paremmin näkyvissä.

7 Yhteenveto

Työn tarkoituksena oli luoda selvitys autentikaatio- ja PIM muutoksen toteuttamisesta Azure-ympäristössä. Työ tuotti tuloksia, mutta kaikkia eri osa alueita ei pystytty käsittelemään aikataulun vuoksi. Tutkimuskysymyksiin vastattiin ja tehdyn selvityksen pohjalta voidaan luoda varsinainen toteutus, mukaan tulee huomioida myös pohdinnassa ilmenneet kehittämiskohteet.

Autentikaation puolesta salasanaton kirjautuminen oli paras tapa toteuttaa kirjautuminen käyttäjätileille ja FIDO2 avaimet tuovat lisäturvan ja yksinkertaisuuden järjestelmänvalvojien kirjautumiseen. Fyysisten avainten hyödyt tulevat niiden tarpeesta olla kirjauduttavan laitteen lähellä. Avaimien arkkitehtuuri ei myöskään mahdollista kirjautumista kalasteluohjelmien luomille verkkosivuille. Avainten lisääminen ja hallinta oli simppeliä yrityksen näkökulmasta. Varsinaisen toteutuksen kannalta aiheesta tulee kehittää laaja suunnitelma ja pilotointi, jotta ongelmatilanteet eivät vaikuta negatiivisesti yrityksen toimintaan.

PIM-toteutus vaatii kuitenkin paljon erilaisia tehtäviä, jotta sen täysi potentiaali voidaan hyödyntää. Tarkat prosessit aktivointeihin ja niiden hyväksymiseen olivat keskeisiä aiheita. PIM on oletusasetuksillaan puutteellinen ja kuten työssä tutkittiin, sitä tulisi täydentää. Selvät aktivoijat niitä tarvitseviin rooleihin, jotta kyseisiä rooleja voidaan turvata paremmin. Informatiiviset syyt aktivointeihin helpottavat auditointia selventämällä aktivointien tarkoitusta.

Yleisellä tasolla työssä onnistuttiin, vaikka jokaista työn osaa ei keritty testaamaan tai käsittelemään täysin. Olennainen pohjatieto toteutukselle määriteltiin ja sen perusteelta pystytään luomaan lopullinen osien toteutus.

Lähteet

Andersen, G. 2024. Ethical Considerations in IT Technician Roles: Privacy and Data Protection. Artikkeli. Viitattu 30.04.2025. https://moldstud.com/articles/p-ethical-considerations-in-it-technician-roles-privacy-and-data-protection

Borges, E. 2024. Security Through Obscurity: A Critical Analysis of Hidden Dangers. Threat intelligence 101-blogi. Viitattu 30.04.2025. https://www.recordedfuture.com/threat-intelligence-101/legal-ethical-considerations/security-through-obscurity

Bucy, D. 2021. Understanding YubiKey PINs. Yubico verkkosivu. Päivitetty 1.8.2024 Viitattu 09.04.2025. https://support.yubico.com/hc/en-us/articles/4402836718866-Understanding-YubiKey-PINs

Eades, N. 2023. Privileged Identity Management (PIM): For Many, a False Sense of Security. Permison blogikirjoitus. Julkaistu 07.12.2023. Viitattu 20.04.2025. https://permiso.io/blog/privileged-identity-management-pim-for-many-a-false-sense-of-security

Enable passkeys (FIDO2) for your organization. 2024. Microsoftin dokumentaatiosivu. Päivitetty 05.03.2025. Viitattu 16.04.2025. https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2

How it works: Microsoft Entra multifactor authentication. 2020. Microsoftin dokumentaatiosivu. Päivitetty 04.03.2025. Viitattu 16.04.2025. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

Iacono, L., Glass, G. & Wojcieszek, K. 2024. Q3 2024 Threat Landscape Report: Rising Attacks on Tech and Telecoms Reinforce Need for Business Continuity Planning. Kroll-sivusto. Julkaistu 21.11.2024. Viitattu 18.03.2025. https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2024-threat-landscape-report-business-continuity-planning#sector

Manage user authentication methods for Microsoft Entra multifactor authentication. 2024. Microsoftin dokumentaatiosivu. Päivitetty 07.03.2025. Viitattu 09.04.2025. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userdevicesettings

Markert, P. Bailey, D. Golla, M. Durmuth, M. Aviv, A. 2021. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. Tutkimustyö. Viitattu 09.04.2025. https://arxiv.org/pdf/2003.04868

Mehtälä, H. 2024. The Cybercriminal Arsenal: MFA Attacks. Opinnäytetyö, AMK. Jyväskylän ammattikorkeakoulu, tieto- ja viestintätekniikan tutkinto-ohjelma. Viitattu 09.04.2025. https://www.theseus.fi/bitstream/handle/10024/875560/Mehtala_Herkko.pdf?sequence=2&isAllowed=y

Microsoft Azure: what it is and how it works. 2018. Intercept-blogi. Päivitetty 23.12.2024. Viitattu 08.04.2025. https://intercept.cloud/en-gb/blogs/what-is-microsoft-azure

Microsoft Entra built-in roles. 2024. Microsoftin dokumentaatiosivu. Päivitetty 08.01.2025. Viitattu 08.04.2025. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Privileged access: Accounts. 2024. Microsoftin dokumentaatiosivu. Viitattu 16.04.2025. https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-accounts

Privileged roles and permissions in Microsoft Entra ID (preview). 2023. Microsoftin dokumentaatiosivu. Päivitetty 15.10.2024. Viitattu 30.04.2025 https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-roles-permissions?tabs=admin-center

Qvantel Finland Oy. N.d. Finder yrityshaku. Viitattu 14.04.2025. https://www.finder.fi/Sovelluk-set+ja+ohjelmistot/Qvantel+Finland+Oy/Helsinki/yhteystiedot/175664

Qvantel Flex BSS: The Next Evolution of BSS. N.d. Qvantelin verkkosivu. Viitattu 14.04.2025. https://www.qvantel.com/

Salonen, K. Eloranta, S. Hautala, T & Kinos S. 2017. Kehittämistoiminta ja kehittämisen menetelmiä ammatillisessa korkeakoulutuksessa. Theseus-verkkosivu. Viitattu 08.04.2025. https://www.theseus.fi/bitstream/handle/10024/817817/isbn9789522166494.pdf?sequence=2&isAllowed=y

Shared responsibility in the cloud. 2019. Microsoftin dokumentaatiosivu. Päivitetty 29.09.2024. Viitattu 08.04.2025. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Sørensen, P. 2024. Entra ID PIM – Part 2: How to set it up and delegate permissions in a good way. Agderinthe verkkosivu. Viitattu 14.04.2025. https://agderinthe.cloud/2024/01/17/entra-id-pim-part-2-how-to-set-it-up-and-delegate-permissions-in-a-good-way/

Spare YubiKeys. N.d. Yubicon verkkosivu. Viitattu 09.04.2025. https://www.yubico.com/products/spare/

Temoshok, D. Fenton, J. Choon, Y. Lefkovitz, N. Regenscheid, A. Galluzzo, R. Richer, J. 2024. Digital Identity Guidelines. NIST-verkkojulkaisu. Viitattu 01.05.2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.ipd.pdf

What authentication and verification methods are available in Microsoft Entra ID?. 2023. Microsoftin dokumetaatiosivu. Päivitetty 04.03.2025. Viitattu 08.04.2025. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

What is Conditional Access?. 2022. Microsoftin dokumentaatiosivu. Päivitetty 04.03.2025. Viitattu 30.04.2025. https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

What is Microsoft Entra ID Governance?. 2023. Microsoftin dokumentaatiosivu. Päivitetty 09.04.2025. Viitattu 30.04.2025. https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview

What is FIDO2? N.d. Microsoftin blogipostaus. Viitattu 20.04.2025. https://www.microsoft.com/en-us/security/business/security-101/what-is-fido2

What Is FIDO2 and How Does It Work? Passwordless Authentication Advantages & Disadvantages. 2025. Hideez-verkkosivu. Viitattu 08.04.2025. https://hideez.com/en-int/blogs/news/fido2-explained

What is Microsoft Entra authentication?. 2019. Microsoftin dokumentaatiosivu. Päivitetty 04.03.2025. Viitattu 30.04.2025. https://learn.microsoft.com/en-us/entra/identity/authentication/overview-authentication

What is Microsoft Entra Privileged Identity Management?. 2023. Microsoftin dokumentaatiosivu. Päivitetty 07.01.2025. Viitattu 08.04.2025. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

What is information security and why is it important. 2022. Dataguard-verkkosivu. Päivitetty 10.2.2025. Viitattu 08.04.2025. https://www.dataguard.com/blog/importance-of-information-security

What is Microsoft Entra ID?. 2023. Microsoftin dokumentaatiosivu. Päivitetty 05.03.2025. Viitattu 08.04.2025. https://learn.microsoft.com/en-us/entra/fundamentals/whatis

Why Going Passwordless is the Future of Cybersecurity. N.d. SSH-verkkosivu. Viitattu 16.04.2025. https://www.ssh.com/academy/secrets-management/why-going-passwordless-is-future-of-cybersecurity

YubiKey 5 NFC. N.d. Yubicon verkkosivu. Viitattu 09.04.2025. https://www.yubico.com/fi/product/yubikey-5-nfc/