OULUN AMMATTIKORKEAKOULU

Mika Lindberg

MONIVAIHEISEN TODENTAMISEN TOTEUTUS PK-YRITYKSESSÄ

MONIVAIHEISEN TODENTAMISEN TOTEUTUS PK-YRITYKSESSÄ

Mika Lindberg
Opinnäytetyö
Kevät 2020
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Informaatioteknologia, Tietojenkäsittelyn tutkinto-ohjelma

Tekijä: Mika Lindberg
Opinnäytetyön nimi: Monivaiheisen todentamisen toteutus PK-yrityksessä
Työn ohjaaja: Ilkka Mikkonen
Työn valmistumislukukausi ja -vuosi: Kevät 2020 Sivumäärä: 37 + 7

Opinnäytetyön tavoitteena oli kuvata yleisellä tasolla pk-yrityksen it-ympäristö, vaatimukset todentamiselle ja vertailla erityyppisiä ratkaisuja todentamisen toteutukseen vaatimuksiin pohjautuen. Työn tavoitteena ei ollut tehdä yksityiskohtaista analyysia todentamisesta ja sen teknisistä ratkaisuista vaan löytää yleinen määritelmä ja ratkaisuvaihtoehtoja todentamisen vaatimuksille tyypillisessä pk-yrityksessä opinnäytetyön teon ajankohtana. Työlle ei ollut varsinaista toimeksiantajaa ja se tehtiinkin työelämässä havaittujen tarpeiden perusteella.

Työssä määriteltiin aluksi tietoturvallisuus ja mikä rooli todentamisella on sen toteuttamisessa. Tämän jälkeen selvitettiin todentamisen menetelmät, joista tarkemmin käytiin läpi monivaiheisen todentamisen tapoja. Seuraavassa vaiheessa pyrittiin määrittelemään tavanomainen pk-yrityksen it-infrastruktuuri ja liiketoiminnan sekä käyttäjän vaatimukset todentamiselle. Tässä vaiheessa havaittiin, että vaikka yleisellä tasolla vaatimukset pystyttiin kirjaamaan, ovat ne silti niin yrityskohtaisia, että toteutuksen vertailuun tulisi valita erilaisia ratkaisuja niin tekniseltä toteutuksen kuin kustannustenkin kannalta.

Vaatimuksiin pohjaten tehtiin markkinakartoitusta ja valittiin neljä erilaista ratkaisua vertailuun. Vertailuun valittujen ratkaisujen osalta käytiin läpi ominaisuudet ja kustannukset, sillä tasolla millä vaatimusmäärittely tehtiin. Vertailun perusteella valittiin yksi ratkaisu minkä käyttöönotto tehtiin testiympäristöön ja vaiheistus kirjattiin liitteeseen tehtävälistaksi eikä niinkään asennusoppaaksi, sillä asennuksesta on saatavissa runsaasti valmistajan tukimateriaaleista. Vaihtoehtoisen toteutustavan käyttöönotto kuvattiin myös liitteellä yleisellä tasolla.

Työn tulokset ovat hyödynnettävissä pk-yrityksen tietoturvatyössä sen pohtiessa omia vaatimuksiaan ja ratkaisujaan todentamiselle sekä etenkin monivaiheiselle todentamiselle.

Työn perusteella voidaan todeta, että vaikka pk-yritys ei olisi riskienhallinnan menettelyin määrittänyt monivaiheisen todennuksen vaatimusta, niin kaikkia organisaatioita koskevien lakisääteisten vaatimusten, yleisten suositusten ja ajankohtaisten uhkakuvien vuoksi monivaiheisen todennuksen tulisi olla yksi käyttöönotettavista tietoturvan hallintakeinoista. Markkinoilla on tällä hetkellä tarjolla laaja kirjo erilaisia ratkaisuja, joiden soveltuvuus pk-yritykselle vaihtelee merkittävästi ja markkinoiden tarjonta lisääntyy sekä kehittyy koko ajan. Ratkaisuja pohtivan kannattaakin aktiivisesti seurata tarjonnan kehitystä.

Asiasanat: Tietoturva, luottamuksellisuus, tunnistaminen, todennus, monivaiheinen todennus

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author: Mika Lindberg
Title of thesis: Multifactor authentication in small business.
Supervisor: Ilkka Mikkonen
Term and year when the thesis was submitted: Spring 2020 Number of pages: 37 + 7

The goal of this thesis was to determine and describe typical small business IT infrastructure, demands for authentication and compare solutions for authentication based on demands. Thesis scope was not to make a deep dive to technical details or create to create an installation guide.

First part of thesis describes the very basics of information security and how authentication is related to them. Second part is an overview to authentication methods and especially to multifactor authentication.

Next part focus to determine how small business IT infrastructure is built and how it uses cloud services as part of it. This part also includes demands for authentication from user and business perspective. Demands are described at high level and more detailed should be made before choosing and implementing multifactor authentication solutions for specific company.

Market offering was studied to find few different kinds of solutions based on demands. Solutions was compared and one solution was chosen to be installed to testing system. Installation was documented to task list.

Study shows that multifactor authentication is a must to be implemented feature for many companies even without formative risk analysis. Thesis determines basic demands for multifactor authentication and helps to compare solutions from the market now and in future. It should be noted that properly managed risk analysis gives best overcome to the needs of information security controls.

Keywords: Information security, confidentiality, identification, authentication, multi factor authentication

SISÄLLYS

1 JOHDANTO

Käyttäjien todentamiseen liittyvät haasteet ovat olleet pitkään yksi tietoturvallisuuden ongelmakohtia. Työn tavoitteena on kuvata, miten vastataan tällä hetkellä pk-yrityksissä it-ympäristön käyttäjän turvallisen todentamisen haasteeseen. Pk-yritykset ovat viime vuosina siirtyneet kohti pilvipalveluiden käyttöä säilyttäen kuitenkin omaa it-infrastruktuuria (Työ- ja elinkeinoministeriö, 2019). Tässä toimintamallissa osa palveluista toteutetaan paikallisesti ja osa pilvipalveluina. Tämän vuoksi todentamisenkin tulee ottaa kantaa niin paikallisesti kuin pilvestä käytettävien järjestelmien kannalta. Aiheen ajankohtaisuudesta esimerkkinä mainittakoon, että Kyberturvallisuuskeskus on viimeisen kahden vuoden aikana tarttunut voimakkaasti aiheeseen ohjeistamalla etenkin pk-yritysten suosiman Office 365-palvelun käyttäjiä tunnistamaan käyttäjätunnusten ja salasanojen kalastelun sekä ottamaan käyttöön monivaiheinen todennus estämään tietomurtoja (Kyberturvallisuuskeskus, 2018). Aihe on siis ajankohtainen ja samalla siihen liittyy aitoa tarvetta pk-yrityksissä.

Työn tarkoituksena on kuvata todentamiseen liittyvät seikat ensin yleisesti ja tarkentaa siitä pk-yritysten tarpeisiin niin liiketoiminnan kuin myös käyttäjän kannalta. Nämä näkökulmat on valittu koska kaikessa yritysten tietoturvallisuuden kehittämisessä tulee palvella ensisijaisesti liiketoiminnan tarpeita unohtamatta tietoturvallisuuden varsinaisen lopullisen toteuttajan, käyttäjien, roolia. Teoreettisen taustan ja tarvekartoitusten jälkeen kartoitetaan markkinoilla olevia vaihtoehtoja ja valitaan niistä soveltuvin aikaisemmin kuvattuihin vaatimuksiin. Työ palvelee tulosten myötä laajaa kohderyhmää antaen opastusta, miten kartoittaa pk-yrityksen tarpeita todentamiseen ja miten valita soveltuva toteutuskeino monista tarjolla olevista vaihtoehdoista.

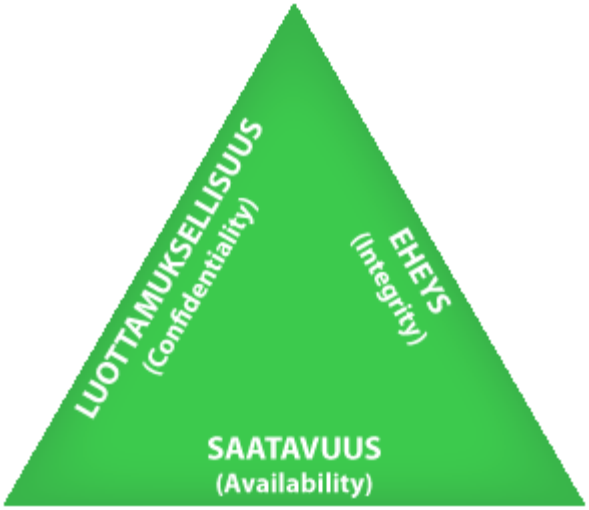
Työllä ei ole varsinaista toimeksiantajaa. Aihe kiinnostaa minua myös ammatillisesti ja koen sen siten palvelevan omaa ammatillista kehittymistäni sekä yritykseni tarpeita sen omassa toiminnassa kuin myös asiakkaille tehtävässä työssä osana tietoturvallisuuden asiantuntijapalveluita.

2 TODENTAMINEN OSANA TIETOTURVALLISUUTTA

Tietoturvallisuus on laaja kokonaisuus minkä perimmäisenä tarkoituksena on varmistaa tietojen turvallisuus kaikissa tilanteissa liiketoiminnan vaatimalla tasolla. Tietoturvallisuuden ja etenkin tietojen luottamuksellisuuden yhtenä perustekijänä on tietoja ja järjestelmiä käyttävien käyttäjien tunnistaminen ja todentaminen.

2.1 Tietoturvallisuuden perusteet

Klassisen tietoturvallisuuden perusteet määrittelevät tietoturvallisuuden koostuvan luottamuksellisuudesta (confidentiality), eheydestä (integrity) ja käytettävyydestä (availability). Termien englanninkielisten versioiden perusteella muodostuu niin kutsuttu CIA kolmio (CIA triad), mitä käytetään usein kuvaamaan tietoturvallisuuden määritelmää graafisesti.



KUVIO 1. CIA kolmio (Mattila, A-L. 2014)

Luottamuksellisuuden tarkoituksena on varmistaa, että tiedot ovat vain sellaisten tahojen käytettävissä, joilla on niihin oikeus. Tietojen luottamuksellisuus pyritään varmistamaan teknisin keinoin kuten todentaminen ja salaus, ohjeistuksella ja henkilöstön koulutuksella sekä oikealla tiedon käsittelyllä. Eheydellä tarkoitetaan sitä, että tiedoissa ei ole virheitä joko tahallisesti tai tahattomasti tai ne eivät ole muuttuneet hallitsemattomasti. Tietojen eheyttä pyritään turvaamaan järjestelmien tarkistusten ja valvonnan kautta. Turvatoimien ja ohjeistuksen tavoitteena on ehkäistä virheitä ja

laiminlyöntejä tietojen käsittelyssä. Saatavuus merkitsee sitä, että tiedot ovat saatavilla häiriöttömästi silloin kun niitä tarvitaan. Tietojen saatavuutta pyritään lisäämään toimilla, joilla vaikutetaan järjestelmien toiminnan jatkuvuuteen ja tiedon saatavuuteen poikkeusoloissa kuten sähkö- tai tietoliikennekatkokset ja laiteviat. Tietoturvallisuuden riskejä ja niihin kohdistuvia kontrolleja arvioidaan usein sen kautta, miten hyvin ne vastaavat yhteen tai useampaan edellä mainituista perustekijöistä. (Hakala, Vainio & Vuorinen, 2006, 4 - 5; Stewart, Chapple & Gibson, 2015, 3 - 7)

2.2 Todentamisen rooli tietoturvallisuudessa

Tietoturvallisuuden määritelmää on laajennettu, sillä kolmen edellä esitellyn on katsottu olevan riittämättömiä huomioimaan kaikkia tarpeellisia tietoturvallisuuden tarpeita. Laajennuksen myötä edellä mainittujen kolmen osion lisäksi määritelmä sisältää kiistämättömyyden (nonrepudiation) ja pääsynvalvonnan (access control). Kiistämättömyydellä tarkoitetaan sitä, että toimenpiteen tai tapahtuman tekijä ei voi kiistää tapahtunutta. Kiistämättömyyden osatekijöitä ovat tunnistaminen (identification), todentaminen (authentication), valtuuttaminen (authorization), osoitusvelvollisuus (accountability) ja valvonta (auditing). (Stewart, 2015, 11-12). Pääsynvalvonnan tehtävänä on rajoittaa tietojärjestelmien käyttöä, kun luottamuksellisuudella varmistettiin itse tietoon pääsyn oikeus. Pääsynvalvonnan tarkoituksena on siis varmistaa, ettei organisaation tietojärjestelmäresursseja käytetä luvatta. (Hakala, 2006, 5 – 6)

Kiistämättömyyden osatekijöitä kutsutaan myös AAA-palveluiksi. Näistä ensimmäisenä olevan tunnistamisen tarkoituksena on tunnistaa tietoon tai järjestelmään pääsyä haluava taho. Tunnistaminen voi tapahtua useilla tavoilla, joista tutuin on kaikilla kirjoittamalla annettu käyttäjätunnus (username). Muita tunnistamisen tapoja voivat olla toimikortit (smart card), sormenjälki (finger print) tai kasvot (face recognition) taikka äänitunniste (voice recognition). Tunnistamisen tarkoituksena on erottaa käyttäjät toisistaan ja kytkeä myöhemmät tapahtumat tunnistuksen kohteeseen. Toisena AAA-palveluista on todentaminen, missä tunnistettu taho todennetaan olevan se kuka hän väittää olevansa. Tämä tapahtuu pyytämällä jokin lisätieto minkä tulee yksiselitteisesti kytkeytyä väitettyyn tunnisteeseen. Yleisin tapa todentamiseen on salasana (password). Annettua tunnistetta ja todennustietoa verrataan tietokantaan tai muuhun tunnisteet ja todentamisen tiedot sisältävään tietokokoelmaan minkä tuloksena koko prosessi onnistuu tai epäonnistuu. Todentamisen tieto on lähtökohtaisesti vain tunnisteen haltijan tiedossa eli yksityinen. Todentamiseen käytettävät tekniset me-

netelmät ja todentamisen salaisten tietojen suojaaminen ovat ratkaisevassa asemassa koko prosessin turvallisuuden kannalta. Mikäli tunnistaminen ja etenkin todentaminen ovat toteutukseltaan heikkoja, niin järjestelmään tai tietoon oikeudettoman pääsyn saaminen on helppoa tietoturvan mittapuulla. Mikäli taasen nämä on toteutettu hyvä tasoisesti, on järjestelmän tai tiedon luvaton käyttö vaikeaa ja tietoturvallisuuden taso siten korkeampi. Tunnistaminen ja todentaminen ovatkin siten tietoturvallisuuden ja etenkin luottamuksellisuuden kulmakiviä. (Stewart, 2015, 8-9).

Tunnistamista ja todentamista käytetään aina yhdessä ja turvallisuuden tason parantamiseksi todentamiseen on lisätty muita vaiheita. Tällöin muodostuu monivaiheisen todentamisen menetelmä missä sen lisäksi, että on jotain minkä tiedät, kuten salasana, sinulla voi olla jotain sellaista hallussasi tai voit olla taikka tehdä jotain mikä voidaan kytkeä osaksi todentamista. Tämä hallussa oleva voi olla esimerkiksi toimikortti, tunnisteväline tai puhelin ja mitä olet taikka teet voi olla sormenjälki, ääni, ele tai muu liike. Viimeiseksi mainittuja kutsutaan käyttämiseen pohjautuviksi tunnisteiksi. (Stewart, 2015, 563)

Valtuuttaminen tapahtuu onnistuneen tunnistamisen ja todentamisen jälkeen. Valtuutuksessa annetaan tunnistetulle taholle pääsy resursseihin sen mukaan mitä oikeuksia tunnisteeseen on kytketty. Osoitusvelvollisuus ja valvonta ovat menettelyitä millä valvotaan ja tarkastetaan valtuutusten käyttöä ja niiden avulla tehtyjä resursseihin kohdennettuja toimia.

3 TODENTAMISEN TYYPIT JA MENETELMIÄ

Tunnistaminen ja siihen kiinteästi liittyvä todentaminen ovat keino varmistaa tietoon ja järjestelmiin pyrkivä käyttäjä. Todentamisen tyyppejä on kolmea eri tyyppiä mitkä on esitelty seuraavissa kappaleissa. Korkeampaa tyyppiä pidetään lähtökohtaisesti matalampaa turvallisempana ja useamman tason yhdistelmää kaikkein turvallisimpana ratkaisuna.

3.1 Tyypit

Todentamiseen käytetyt menetelmät jaetaan kolmeen tyyppiin. Näitä ovat:

- Tyyppi 1 on jotain mitä tiedät kuten salasana tai PIN-koodi.
- Tyyppi 2 on jotain mitä sinulla on kuten fyysinen laite.
- Tyyppi 3 on jotain mitä sinä olet, kuten biometriset tunnisteet, tai jotain sellaista miten sinä toimit, kuten käsiala tai ele.

(Stewart, 2015, 563)

3.2 Käyttäjätunnus ja salasana

Yleisimmin ja yksinkertaisin tunnistamisen ja todentamisen menetelmä on käyttäjätunnuksen ja salasanan yhdistelmä. Salasana on tyypin 1 todentamisen menetelmä. Tietoresursseihin pääsyä haluava taho tunnistautuu antamalla käyttäjätunnuksen ja sen oikeellisuuden todentamiseksi antaa käyttäjätunnukseen kytketyn salasanan.

Käyttäjätunnuksen tulee aina olla yksilöllinen ja erotettava kaikki järjestelmään kirjautuvat tahot toisistaan sillä kaikki muut toiminnot nojaavat siihen. Käyttäjätunnusta ei pidetä useinkaan salaisena tietona mutta sen julkistamista tai esillä pitämistä ei voida mitenkään suositella. Salasana on, kuten nimestäkin voi päätellä, salainen ja tarkoitettu vain haltijansa tietoon. Salasanat tulisi aina tallentaa niin kutsutun yksisuuntaisen funktion avulla. Tällöin salasanaa ei voida missään tilanteessa palauttaa selkokieliseen muotoon mutta sitä voidaan verrata käyttäjän syötteeseen ja suorittaa todentaminen. (OWASP, 2020)

Salasanat ovat yleisin mutta myös heikoin todentamisen menetelmä. Salasanoista tekee heikkoja useat eri syyt kuten:

- Käyttäjät valitsevat liian helppoja ja arvattavia salasanoja.
- Satunnaisesti luodut salasanat ovat vaikeita ja ne kirjoitetaan muistiin heikosti suojatulla tavalla.
- Salasanoja on liian monta ja ne kirjoitetaan muistiin heikosti suojatulla tavalla.
- Salasanoja saatetaan välittää selkokielisinä salaamattoman tietoliikenneyhteyden kautta, jolloin ne ovat hyökkääjän urkittavissa.
- Salasanatietokanta voidaan murtaa kokeilemalla kaikkia mahdollisia yhdistelmiä ja löytämällä oikea salasana. Menetelmää kutsutaan brute-force hyökkäykseksi. Se paljastaa etenkin heikot salasanat tai salasanat mitkä on tallennettu heikolla suojauksella tietokantaan.

(Stewart, 2015, 564)

Turvallisiin salasanakäytäntöihin on julkaistu lukuisia suosituksia ja oppaita. Kyberturvallisuuskeskus suosittelee käyttämään jokaisessa palvelussa ja järjestelmässä eri salasanaa, salasanan tulee olla riittävän pitkä ja monimutkainen, kuten lause, ja salasanojen suuren määrän vuoksi suositellaan käytettäväksi salasanojen hallintaan tarkoitettua ohjelmaa. Salasanojen lisäksi suositellaan käytettäväksi kaksi- tai monivaiheista todentamista. (Kyberturvallisuuskeskus, 2019)

3.3 Monivaiheinen todentaminen

Monivaiheinen todentaminen hyödyntää salasanan lisäksi yhtä tai useampaa menetelmää mitkä ovat tyypin 2 tai 3 menetelmiä. Tällä tavoin saadaan nostettua turvallisuuden tasoa verrattuna vain yhden menetelmän hyödyntämiseen. On huomioitava, ettei useamman saman tyypin todentamisen yhteisvaikutus nosta turvallisuuden tasoa vaan siihen vaaditaan yhdistelmä eri menetelmiä. (Stewart, 2015, 572). Monivaiheista todentamista kutsutaan usein myös kaksivaiheiseksi todentamiseksi tai vahvaksi todentamiseksi. Vaikka termit eivät ole täysin yhdenmukaisia, niin yleisesti kaikilla näillä viitataan edellä kuvattuun useamman tyypin yhdistävää todentamisen tapaa.

Monivaiheisessa todentamisessa käyttäjän tunnistamisen jälkeen syöttää salasanan minkä onnistuneen todennuksen jälkeen hänet todennetaan myös toisella tavalla (tyyppi 2 tai 3). Tämä toinen

todentaminen on otettu käyttöön järjestelmän tai verkkopalvelun asetuksista tai käyttöönoton yhteydessä. Tyypin 2 menetelmiä ovat USB-avaimet, puhelimeen asennettavat avainkoodi- tai tunnistautumissovellukset, tekstiviestit tai erilliset avainkoodilaitteet. (Kyberturvallisuuskeskus, 2019).

3.3.1 Tekstiviesti

Järjestelmä lähettää tekstiviestin käyttäjätunnukseen kytkettyyn puhelinnumeroon ja käyttäjä syöttää viestin sisältämän tunnisteen järjestelmään. Tekstiviesti on yksinkertainen mutta myös osin haavoittuvainen monivaiheisen todentamisen menetelmä (Duo, 2020). Todettuja haavoittuvuuksia on havaittu tekstiviestipalvelimissa (iSynergy, 2020) ja SIM-korttien identiteettivarkauksilla (Millman, 2020).

3.3.2 Aikaan perustuva TOTP

Monivaiheisen todentamisen menetelmä missä käytetään aikaan perustuva vaihtuvaa tunnistetta. Tunnisteen luomiseksi puhelimen sovellus yhdistetään palveluun yleensä lukemalla QR-koodi palvelun asetuksista. Tämän jälkeen kirjautumisen yhteydessä puhelimen sovelluksesta luetaan voimassa oleva tunniste. Tunnisteen vaihto perustuu aikaan. (Duo, 2020)

3.3.3 Push-viesti

Push-viestissä puhelimen sovellus kysyy käyttäjältä lupaa kirjautua. Puhelimen sovellus on ensin rekisteröity palveluun kuten edellä esitelty TOTP menetelmä (Duo, 2020).

3.3.4 U2F laitteet

U2F-laitteet ovat USB-porttiin kytkettäviä laitteita, avaimia. Avain rekisteröidään palveluun ja kirjautumisen yhteydessä käyttäjää pyydetään kytkemään avain tietokoneeseen ja painamaan avaimessa olevaa aktivointinappia. Tämän jälkeen käyttäjä yleensä syöttää avaimen PIN-koodin ja kirjautuminen tapahtuu tämän jälkeen. (Duo, 2020)

3.4 Kertakirjautuminen

Kertakirjautumisella (Single Sign-On) tarkoitetaan keskitettyä järjestelmää minkä avulla käyttäjän tunnistus ja todentaminen suoritetaan yhden kerran ja sen avulla annetaan pääsy useampaan järjestelmään. Kertakirjautuminen helpottaa käyttäjän toimintaa vähentämällä tarvittavia tunnistamisen ja todentamisen kertoja. Samalla voidaan parantaa tietoturvan tasoa vaatimalla yhteen tunnistamiseen ja todentamiseen useampia menetelmiä (Stewart, 2015, 573). Nykyisin useat tunnetut palvelut mahdollistavat kertakirjautumispalvelunsa hyödyntämisen muissa verkkopalveluissa. Tällaisia palveluita tarjoavat mm. Microsoft, Google, Facebook ja Twitter. Yritysten IT-ympäristöihin on myös tarjolla useita kertakirjautumisen järjestelmiä. Yksi käytetyimpiä on Microsoftin Active Directoryyn perustuva ratkaisu.

3.5 Muut menetelmät

Muut todentamisen menetelmät ovat tyypin 3 menetelmiä. Näitä ovat biometriset tunnisteet tai käyttäytymiseen perustuvat menetelmät. Biometrisistä tunnisteista tunnetuin on sormenjälki ja kasvojen tunnistus. Käyttäytymiseen perustuvista menetelmistä esimerkkinä voidaan mainita käsialan tunnistus. (Stewart, 2015, 568-570)

4 VAATIMUKSET TODENTAMISELLE

Tietoturvallisuudelle ja siten myös todentamiselle asetettavat tavoitteet ja vaatimukset tulisi aina johtaa liiketoiminnan vaatimuksista sekä niiden perusteella tehdyistä riskiarvioista. Todentamisen osalta on myös laadittu suosituksia mitkä perustuvat yleisiin uhka-arvioihin. Jokaisen yrityksen liiketoiminta ja IT-infrastruktuuri ovat erilaisia ja siksi niiden tulisikin arvioida omia tavoitteitaan tietoturvalle ja tietoriskejään ennen uusien tietoturvakontrollien käyttöönottoa.

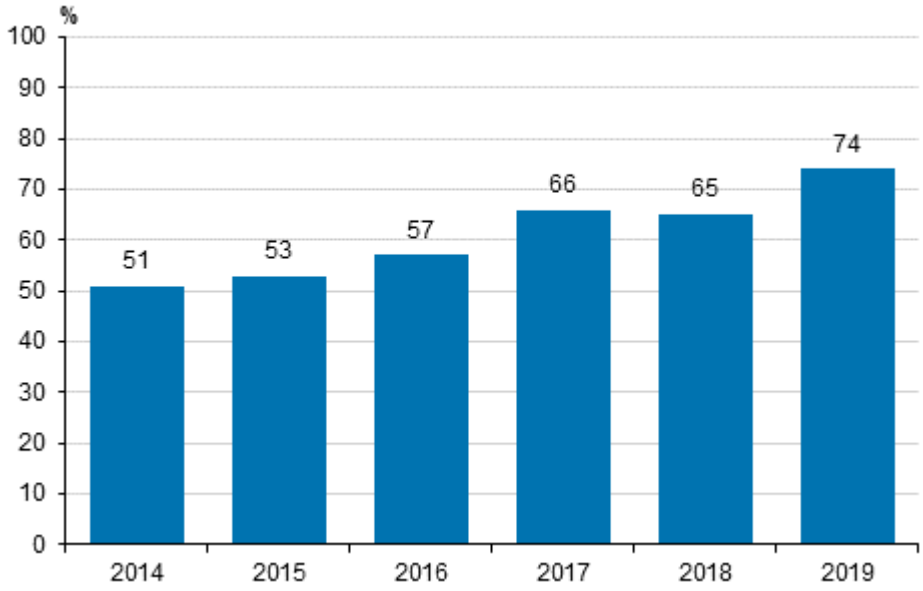
4.1 PK-yrityksen IT-infrastruktuuri

Pk-yrityksen määritelmä tilastokeskuksen mukaan on:
Pienet ja keskisuuret yritykset (PK-yritykset) määritellään yrityksiksi, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa (40 miljoonaa euroa ennen vuotta 2003) tai taseen loppusumma on enintään 43 miljoonaa (27 miljoonaa euroa ennen vuotta 2003) euroa ja jotka täyttävät alla määritellyn perusteen riippumattomuudesta.
(Tilastokeskus, Käsitteet, PK-yritys. Viitattu 13.2.2020)

Riippumattomia yrityksiä ovat ne yritykset, joiden pääomasta tai äänivaltaisista osakkeista 25 prosenttia tai enemmän ei ole yhden sellaisen yrityksen omistuksessa tai sellaisten yritysten yhteisomistuksessa, joihin ei voida soveltaa tilanteen mukaan joko PK-yrityksen tai pienen yrityksen määritelmää.
(Tilastokeskus, Käsitteet, PK-yritys. Viitattu 13.2.2020)

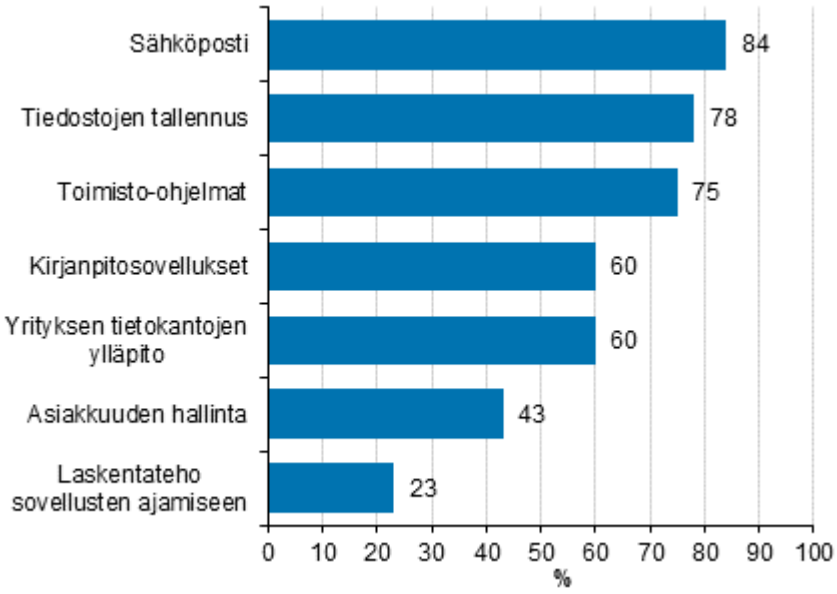
Pk-yritysten IT-infrastruktuuri on moninainen ja vaihteleva. Usein se kuitenkin rakentuu jonkin tyyppisestä paikallisesta verkosta, missä Microsoftin Active Directory hakemistopalvelua hallinnoiva palvelin vastaa tunnistamisesta ja todentamisesta. Lisäksi paikallisessa verkossa oleville palvelimille on usein sijoitettuna tietoresursseja ja järjestelmiä. Paikallisten resurssien lisäksi osa yritysten käyttämistä palveluista hankitaan pilvipalveluina. Varsinainen työskentely tapahtuu kiinteällä työasemalla tai kannettavalla tietokoneilla, joiden suosio on kasvanut vuosi vuodelta. Käyttöjärjestelmistä Windows on edelleen selkeästi suurimmassa osassa yritysten tietokoneita mutta Applen Mac tietokoneiden yleistyminen on lisännyt myös macOS käyttöjärjestelmän käyttöä yrityksissä. Nykyään onkin tavanomaista, että yrityksen verkossa on käytössä molempia.

Tilastokeskuksen tutkimus Tietotekniikan käyttö kertoo, että suomalaisten yritysten pilvipalveluiden käyttöaste on kasvanut viimeisten vuosien aikana ollen vuonna 2019 74% kun huomioidaan yli 10 henkilöä työllistävät yritykset.



KUVIO 2. Pilvipalvelun käyttö yrityksissä 2014-2019. Osuus kaikista vähintään kymmenen henkilöä työllistävistä yrityksistä. (Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä [verkko-julkaisu]. 2019)

Samainen tilasto kertoo käytettyjen pilvipalveluiden sisältävän sähköposteja, tiedostoja, kirjanpito-tietoa, yritysten tietokantoja ja asiakkuuden hallinnan tietoja. Voidaankin todeta yritysten käyttävän pilvipalveluita laajasti erilaisiin toimintoihin, jotka sisältävät liiketoiminta- ja henkilötietoa. (Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä [verkkojulkaisu]. 2019)



KUVIO 3. Käytetyt pilvipalvelut 2014-2019. Osuus kaikista vähintään kymmenen henkilöä työllistävistä yrityksistä. (Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä [verkkojulkaisu]. 2019)

Pilvipalveluiden markkinaosuuksia ei ole palveluntarjoajien taholta julkaistu vertailtavissa olevin luvuin. Yhdysvaltalainen pilvipalveluiden tietoturvallisuuteen keskittyvät Bitglass teki vuonna 2018 selvityksen missä todettiin, että noin 56 % pilvipalveluita käyttävistä yrityksistä hyödyntää Microsoftin Office 365 palvelua ja noin 25% Googlen G suite palvelua. (Serpa, 2018). Luvut eivät suoraan kerro suomalaisten yritysten jakaumaa mutta antavat riittävän kuvan tilanteesta. Luvuista voidaankin päätellä, että karkeasti vähintään noin puolet yrityksiä hyödyntää Office 365 tai G Suite palveluita sähköpostiin ja tiedostojen käsittelyyn.

PK-yritysten IT-infrastruktuurin ylläpitämiseen ja kehittämiseen varatut resurssit ja toteutustapa vaihtelevat merkittävästi. Pienemmissä, lähellä mikroyrityksiä, on usein käytössä kevyitä ulkoistettuja palveluita tai joku henkilökunnasta toimii IT-vastuullisena oman toimensa ohella. PK-yritysten suuremmassa kokoluokassa, keskisuurissa, on usein jo oma IT-asiantuntija tai käytetään merkittävässä määrin ulkoistettuja asiantuntijapalveluita.

4.2 Liiketoiminnan vaatimukset todentamiselle

Tietoturvallisuudelle ja siten todentamiselle asetettavien vaatimusten perusteena tulisi aina olla liiketoiminnalliset tavoitteet ja vaatimukset. Ne tavanomaisesti kuvataan tietoturvallisuuden hallinta-

järjestelmän määrittelemällä tavalla. Tavanomaisesti hallintajärjestelmä rakentuu ylätason politiikoissa, joista ne johdetaan ohjeisiin ja käytäntöihin sekä tallenteiksi, joilla hallintajärjestelmässä asetettujen tavoitteiden toteutumista voidaan mitata. Liiketoiminnallisten tavoitteiden lisäksi tietoturvallisuuden vaatimuksiin vaikuttavat lait, asetukset ja sopimukset. Näiden kautta yritykselle voi tulla erityisiä tietoturvavelvoitteita noudatettavaksi ja niiden tunnistamisen prosessi on osa tietoturvallisuuden hallintajärjestelmää.

Kaikilla organisaatioilla ei ole varsinaista tietoturvanhallintajärjestelmää sillä esimerkiksi kyberturvallisuusstrategia puuttuu 60% yrityksistä. (Pervilä, M. 2019. Tekniikka ja talous). Tämän kaltaisissa tilanteissa tukeudutaan yleiseen uhkakäsitykseen ja niihin perustuviin suosituksiin. Näitä molempia laatii Kyberturvallisuuskeskus, joka suosittaa voimakkaasti käytettäväksi kaksi- tai monivaiheista todentamista. (Kyberturvallisuuskeskus, 2019). Monivaiheisen todentamisen hyödyllisyyttä tietoturvallisuuden tasoa nostavana keinona tukee myös Microsoftin tekemä tutkimus, jonka mukaan 99,9 % pilvipalveluiden käyttäjiin kohdistuneista automaattisista hyökkäyksistä voidaan estää. Tämä perustuu siihen, että pelkästään salasanaan perustuva todentaminen ei riitä edes laadukkaalla salasanalla estämään hyökkäyksien vaikuttavuutta. Microsoft suosittelee monivaiheisen todentamisen käyttöä kaikissa verkkopalveluissa, ei pelkästään heidän tuottamissa. (Cimpanu, 2019)

Jokaisen Euroopassa toimivan yrityksen tulee noudattaa tietosuoja-asetusta ja tarkentavaa kansallista lainsäädäntöä. Tietosuoja-asetus asettaa pakolliseksi henkilötietoon kohdistuvien riskien arvioinnin. Yhtenä esimerkkinä riskistä mainitaan luvaton henkilötietoihin pääsy minkä yhtenä kontrollikeinona on riittävä tunnistus ja todentaminen. (EU yleinen tietosuoja-asetus 2016/679)

Tietoturva- ja lakisääteisten vaatimusten lisäksi tulee huomioida PK-yrityksen tietohallinnon taloudelliset ja henkilöresurssit. Niiden osalta tulee varmistaa, että niiden puitteissa voidaan käyttöönottaa ja ylläpitää monivaiheisen todentamisen ratkaisua. Kuten kohdassa 4.1 todettiin, ovat nämä resurssit hyvin erilaisia PK-yrityksissä ja yleensä asettavat reunaehtoja ratkaisun kustannuksille ja monimutkaisuudelle. Tavanomaisesti pyritään ratkaisuun missä hyödynnetään olemassa olevaa infrastruktuuria ja vaaditut investoinnit pysyvät siten vähäisinä sekä ratkaisun tekninen ylläpito pysyy mahdollisimman kevyenä.

Yhteenvetona todettakoon, että vaikka yrityksellä ei olisi varsinaista tietoturvallisuudenhallintajärjestelmää tai muuta menettelyä millä tunnistetaan tietoturvaan ja todentamiseen kohdistuvat vaati-

mukset, niin yleiset uhkakuvat, niihin annetut toimintasuositukset ja tietosuoja-asetuksen vaatimukset henkilötietojen suojaamiseksi luvattomalta pääsyltä määrittävät monivaiheisen todentamisen käyttöönotettavaksi useimmissa yrityksissä vähintäänkin tärkeimpien järjestelmien osalta toteutuksen mahdollisuuksien mukaan. Monivaiheisen todentamisen toteutuksen tulee käyttöönotto- ja elinkaarikustannuksiltaan suhteutua yrityksen taloudellisiin resursseihin ja arvioituun riskitasoon.

4.3 Käyttäjän vaatimukset todentamiselle

Keskiverto yrityskäyttäjällä on kokonaisuudessaan muistettavanaan noin 90-200 salasanaa. Käytännössä kenenkään on mahdotonta muistaa näin suurta määrää 3.2 kohdan suositusten mukaisia salasanoja ja tämän vuoksi niistä annettuja ohjeita usein rikotaankin mistä aiheutuu tietoturvauhkia heikkojen tai useissa palveluissa käytettyjen salasanojen vuoksi (Child, 2019). Käyttäjien piittaamattomuus myös nimettiin suurimmaksi esteeksi tehokkaan kyberturvallisuuden toteuttamiseksi (Vesterinen, 2019).

Organisaatiot ovat pyrkineet suojautumaan käyttäjän ohjeiden ja suositusten vastaisella toiminnalla aiheuttamaan uhkaan muutamin eri tavoin. Helsingin seudun kauppakamarin Yrityksiin kohdistuvat kyberuhat 2019 selvityksessä 26% yrityksistä nimesi henkilökunnan kouluttamisen kohdistetuksi toimenpiteeksi (Vesterinen, 2019).

Todentamisen turvallisuustason parantamiseen käytetään koulutusten lisäksi teknisiä keinoja. Yleisimmin ja pisimpään on käytetty salasanaan kohdistuneita vaatimuksia kuten pituus, monimutkaisuus ja vanheneminen. Näillä pyrittiin pakottamaan käyttäjät noudattamaan salasanoista annettuja ohjeita. Etenkin salasanan vanheneminen ja siten pakotettu vaihto johti siihen, että useat käyttäjät käyttivät ennustettavia salasanoja (Alexander, 2018). Salasanaan itsessään kohdistuvien vaatimusten jälkeen yritykset ottivat käyttöön salasanojen hallintaan tarkoitettuja sovelluksia, monivaiheista todentamista eri keinoin ja yhdenkertaisen kirjautumisen menettelyitä. Kaikilla näillä kolmella tavoitellaan parempaa turvallisuutta ja käyttäjäkokemusta vähentämällä käyttäjälle kohdistuvaa salasanojen muistamisen vaikeutta ja määrää sekä nopeuttamalla tai jopa poistamalla käyttäjän vastuulta osa todentamisen vaiheista ja vapauttamaan heidät keskittymään omaan työtehtäväänsä. (Child, 2019)

Yhteenvetona todettakoon, että vaikka käyttäjät tiedostavat todentamisen merkityksen ja yritysten siihen kohdentamat vaatimukset, toimitaan kuitenkin heikkolaatuisesti tietoturvan kannalta. Todentamisen tulee olla käyttäjälle mahdollisimman helppoa ja yksinkertaista täyttäen kuitenkin organisaation vaatimukset kohdan 4.2 mukaisesti.

4.4 Yhteenveto vaatimuksista

Vaatimuksia todentamiselle pohdittiin edellisissä luvussa ja niistä voidaan johtaa yhteenveto seuraaviin ominaisuuksiin:

1. Helppokäyttöinen – Käyttäjän näkökulmasta käyttöön ei liity merkittävässä määrin työtä haittaavia ja teknisesti hankalia vaiheita.
2. Teknisesti turvallinen – Yrityksen kannalta tärkeää on, että todentaminen järjestetään teknisesti riittävällä turvallisuustasolla tunnetuilla ja mahdollisimman hyvin standardeihin tai alan yleisiin käytäntöihin perustuen.
3. Kustannuksiltaan soveltuva pk-yritykselle – Kustannusten tulee olla koko elinkaaren ajalta, hankinta- ja ylläpitovaiheen ajan, soveltuva PK-yrityksen tietoturvabudjetille ja vastata liiketoiminnan asettamiin vaatimuksiin turvallisuudesta.
4. Integroituu käytössä olevaan teknologiaan– Integraatio käytössä olevaan teknologiaan tukee kaikkia edellä mainittuja muita vaatimuksia todentamiselle. Tässä yhteydessä integraation tasoksi määritellään PK-yrityksissä yleisesti käytössä olevat palvelut, todentamiseen Microsoft Active Directorya vasten lähiverkon työasemilla sekä palvelimella ja sähköposti sekä työryhmätoimintoihin Microsoft Office 365 palveluun kaikilla päätelaitteilla.
5. Yhteensopivuus – Ratkaisun tulee olla käytettävissä yleisesti yritysten käytössä Windows ja macOS käyttöjärjestelmien versioissa. Windowsin osalta tämä voidaan rajata 10 versioon, sillä aikaisempien versioiden tuki on loppunut ja macOS:n osalta uusimpaan sekä kahteen edelliseen versioon.

5 MONIVAIHEISEN TODENTAMISEN TOTEUTUS

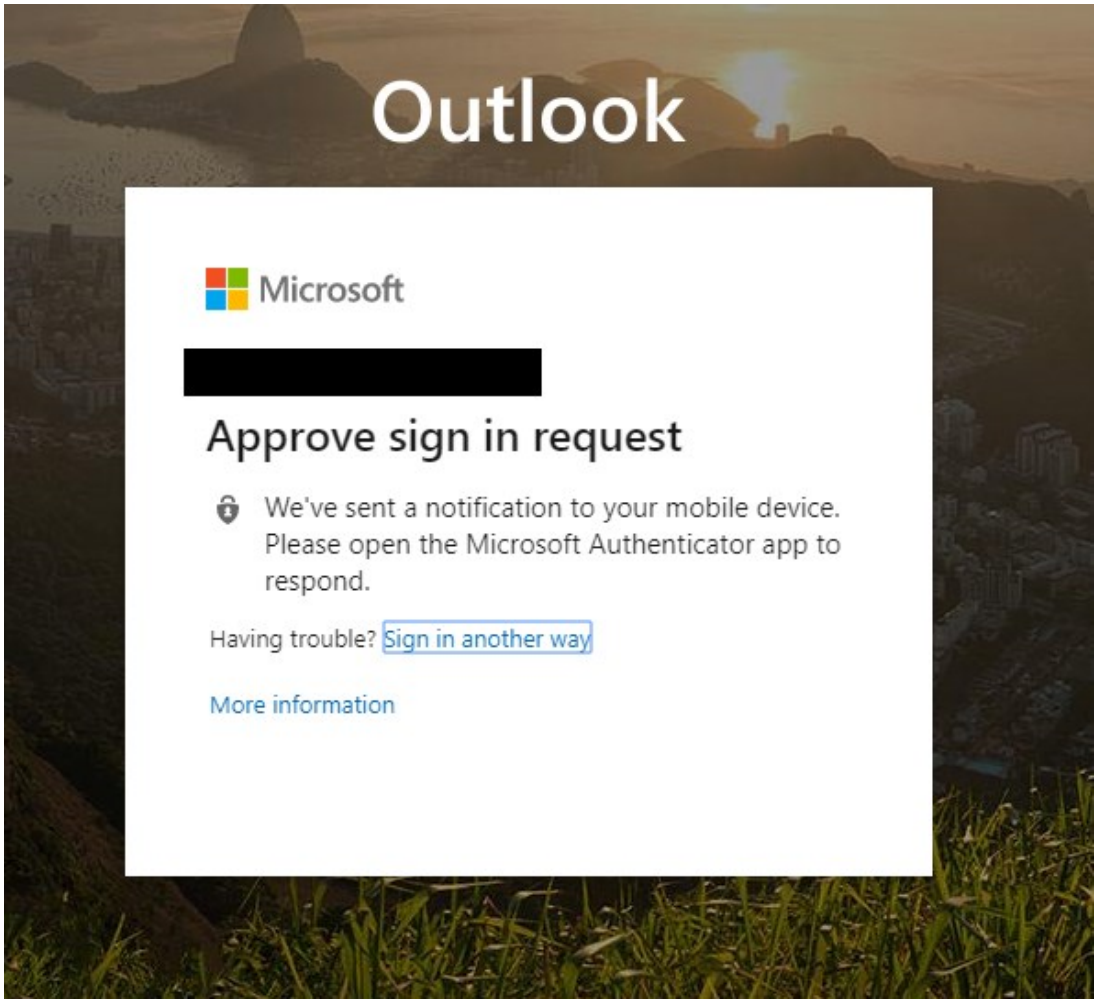
Monivaiheisen todentamisen toteuttamiseen on tarjolla useita ratkaisuja, joiden käyttötapa, teknin-en toteutus, kustannukset ja integraatio PK-yritysten järjestelmiin vaihtelevat merkittävästi. Tässä osiossa pyritään tarjolla olevia ratkaisuja vertailemalla löytämään potentiaalisia vaihtoehtoja PK-yritykselle ja kuvaamaan niistä perustellusti valitun käyttöönotto yleisellä tasolla. Lisäksi ehdotettiin vaihtoehtoinen valinta ja kerrottiin sen käyttöönoton vaiheet.

5.1 Markkinoiden tarjonta

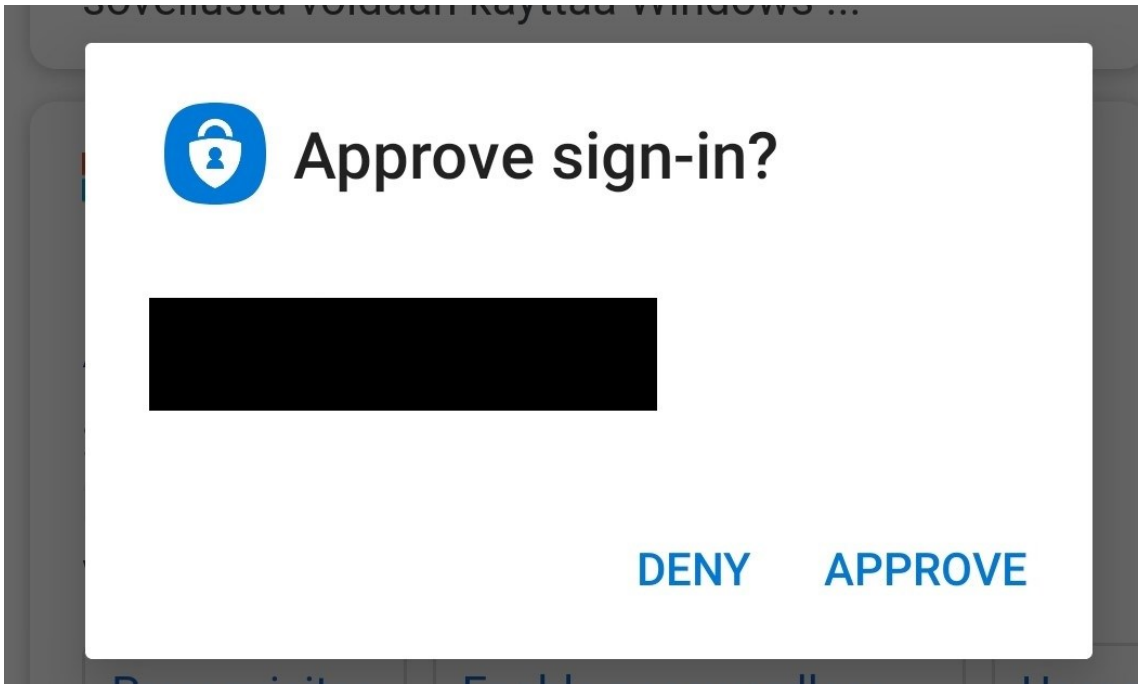
Markkinoilla on tarjolla erilaisiin teknologioihin ja eri toimitusmalleihin perustuvia monivaiheisen to-dentamisen ratkaisuja. Eri toteutusmallit näkyvät myös käyttäjälle erilaisina käyttökokemuksina. Esimerkkeinä käyttötavoista mainittakoon, että osa ratkaisuista perustuu puhelimeen asennetta-vaan sovellukseen ja osa fyysiseen avaimen tyyppiseen USB-väylään kytkettävään laitteeseen. Markkinoiden tarjontaa kartoitettiin erilaisiin lähteisiin, kuten Gartner Magic Quadrant, perustuen ja valmistajien julkisesti internet-sivuilla antamien tietojen avulla. Tästä tarjonnasta seulottiin luvun 4 vaatimuksiin perustuen erilaisia vaihtoehtoja kuitenkin siten, että vertailuun saadaan erilaisia toteu-tustapoja niin teknisesti kuin myös kustannusten osalta. Kustannusten vertailemiseksi yhtenä kri-teerinä olikin julkisesti ilmoitettu hinta valmistajan internet-sivuilla.

5.1.1 Autentikaattorisovellukset puhelimiin

Tekstiviestien jälkeen puhelimeen asennettavat sovellukset ovat suurelle yleisölle tutuin monivai-heisen todennuksen tapa. Puhelimen sovellukseen rekisteröidään todennusta käyttävä tili, kuten Office 365 tai G Suite, ja kirjauduttaessa salasanan lisäksi sovelluksesta katsotaan voimassa oleva numerokoodi. Nykyisin suositumpi menettely on hyväksyä sovelluksen pyyntö kirjautumisesta. Au-tentikaattorisovellukset ja niiden hyödyntäminen kirjautumiseen on Microsoftilla ja Googlella mak-sutonta kokonaisuudessaan eikä siten vaadi laitteiden tai lisenssien hankintaa. Käyttöönoton kus-tannukset koostuvat teknisesti kohtuullisen yksinkertaisesta asetusten määrittelystä ja käyttäjille ohjeiden laatimisesta ja heidän kouluttamisestaan. Autentikaattorisovellukset eivät kuitenkaan täytä kohdan 4.4 vaatimusta 4 järjestelmien kattavuudesta, sillä niitä ei voida hyödyntää kirjau-duttaessa työasemille ilman lisäsovelluksia kuten myöhemmin esitelty Duo tai Authlite.



KUVIO 4. Ilmoitus Office 365 palveluun kirjautuessa, kun monivaiheinen todentaminen on käytössä.

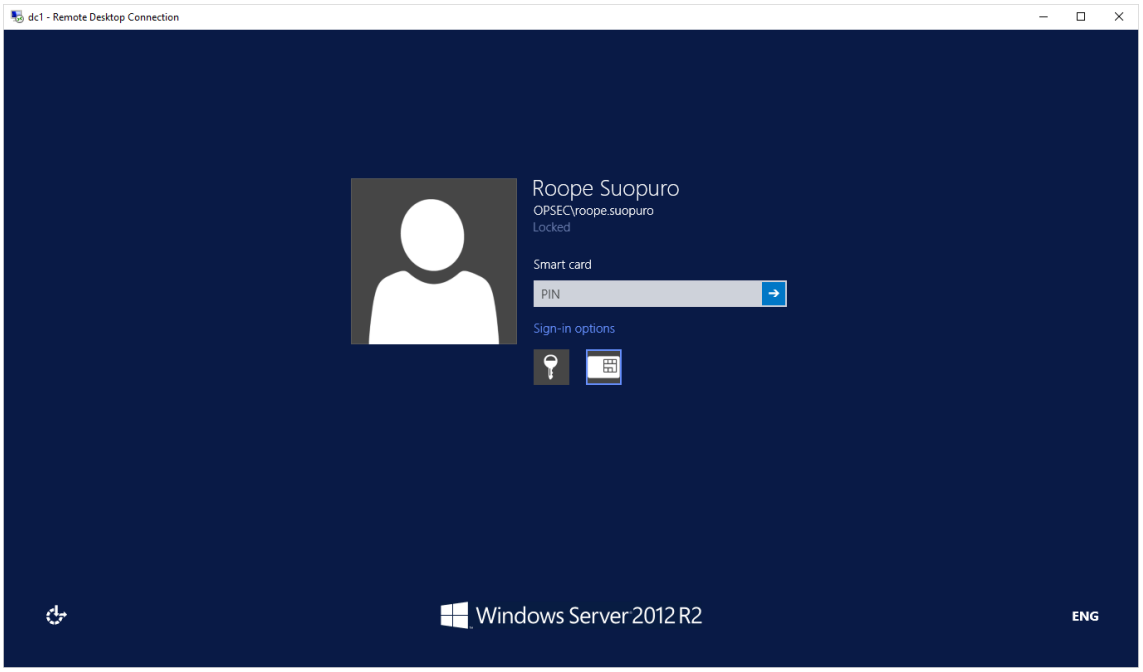


KUVIO 5. Autentikaattorisovelluksen toiminta puhelimessa kirjautumisen yhteydessä

5.1.2 Yubikey

Yubico on alun perin ruotsalainen yritys mikä valmistaa Yubikeyta. Yubikey on USB-porttiin kytkettävä ”avain” jota käytetään monivaiheiseen tunnistamiseen. Yubikey laitteet ovat fyysisesti yksinkertaisia ja rakenteeltaan kestäviä ja yksikköhinnaltaan kohtuullisia vaihdellen noin 30 – 50 € välillä mallista riippuen. Yubikey on käyttäjän kannalta yksinkertainen käyttää mutta selkeästi ylimääräinen huolehdittava laite mukaan. Vaikka kyse on pienestä ja muiden avainten mukana kulkevasta laitteesta, niin sen hukkaaminen saattaa estää tai vaikeuttaa kirjautumista laitteelle ja palveluun. Hukatun tai rikkoutuneen avaimen tilalle tulee ottaa käyttöön uusi avain. Tämä vaikeuttaa etenkin paljon matkustavien työntekijöiden tukemista vikatilanteissa heidän ollessa matkoilla. Pahimmillaan tämä voi tarkoittaa sitä, että tietokoneelle kirjautuminen estyy kokonaan, ellei heillä ole käytettävissään vara-avainta. Käyttöönotto Active Directory ympäristöön Yubikeyn käyttöönotto Active Directory ja Office 365 ympäristöön vaatii teknistä osaamista. Yubikeyn voidaan todeta vastaavan kaikkiin 4.4 kohdan vaatimuksiin. Google G Suite tukee kaikilta ominaisuuksiltaan Yubikeyta (Yubico, viitattu 7.3.2020).

KUVIO 6. Yubikey kytkettynä tietokoneeseen (Opsec Oy, viitattu 7.3.2020)

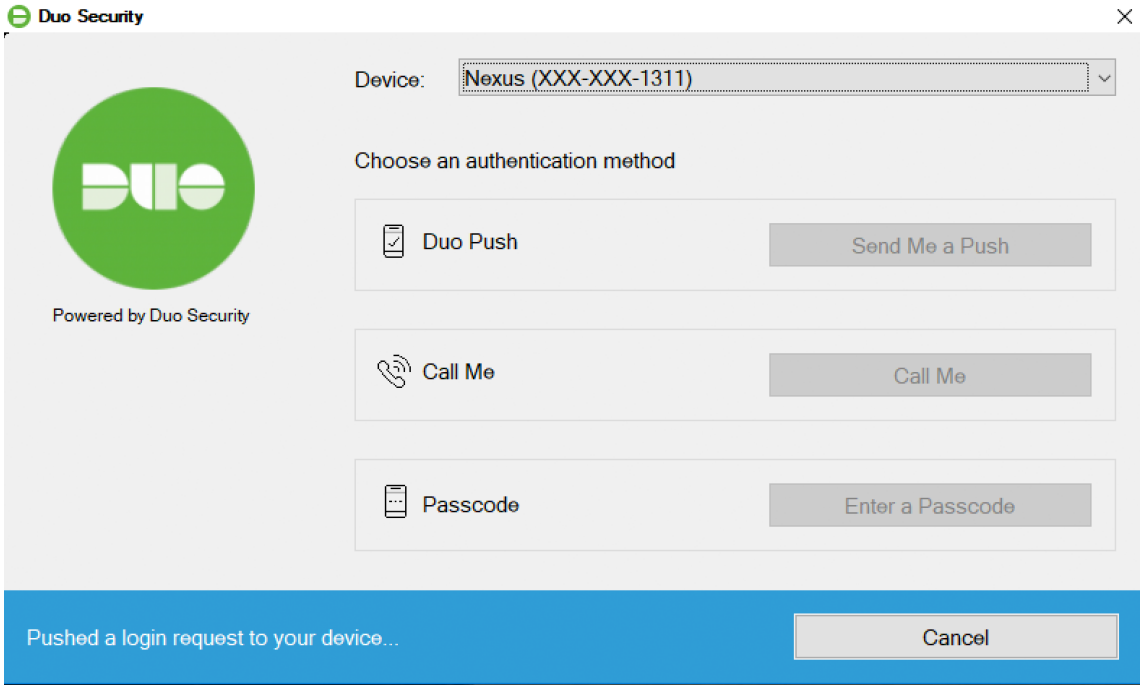


Kuvio 7. Yubikey kirjautuminen Windows tietokoneelle (Opsec Oy, viitattu 20.3.2020)

5.1.3 Duo

Duo valmistaa erilaisia tietoturvan ja etenkin todentamisen ja identiteetinhallinnan ratkaisuja. Duon monivaiheisen todentamisen ratkaisu kattaa kohdan 4.4 vaatimukset ja merkittävän määrän myös muita palveluntarjoajia sekä laitevalmistajia ja tekniikoita. Duon avulla voidaan monivaiheisen todentamisen piiriin tuoda siten määriteltyjen perusjärjestelmien lisäksi muitakin järjestelmiä. Duon

ratkaisua kuvataan käyttäjälle helpoksi ja vaivattomaksi käyttää. Duo mahdollistaa erilaisten todentamisen tapojen käyttämistä sillä Duo tukee puhelinsovelluksia ja USB-porttiin kytkettäviä laitteita kuten Yubikey avaimia. Duon käyttöönoton tekninen osuus vaatii teknistä osaamista mutta sitä ei voida pitää erityisen vaativana. Kustannusten muodostuminen Duossa on erilainen verrattuna kahteen edelliseen, sillä se perustuu käyttäjäkohtaiseen vajaan 10 € kuukausimaksuun. Tämä tekee siitä kalliimman kuin edelliset vaihtoehdot (Duo, viitattu 7.3.2020).



Kuvio 8. Duo kirjautuminen Windows tietokoneelle (Duo, viitattu 21.3.2020)

5.1.4 Authlite

Authlite on valmistaja, joka on keskittynyt toteuttamaan paikallisen lähiverkon monivaiheisen tunnistamisen Yubikey ja Microsoft Active Directory perusteisesti. Näiden lisäksi se tukee Office 365 monivaiheista todentamista sekä Windows etätyöpöytäyhteyksiä. Authlite ei tuo muita pilvipalveluita mutta VPN-yhteydet voidaan sen avulla saattaa monivaiheisen todentamisen piiriin. Authliten hinnoittelu on käyttäjämäärään perustuva kertahankintalisenssi. Yhden käyttäjän kustannus on noin 100 € ja minimihankinta on 5 käyttäjää. Käyttöönotto vaatii teknistä osaamista ja samoin käyttäjien koulutukseen tulee varautua kuten muissakin vaihtoehdoissa (Authlite, viitattu 7.3.2020).

5.2 Ratkaisujen vertailu

Kohdissa 5.21 – 5.2.4 on lyhyesti esitelty kunkin vaihtoehdon vastaavuus kohdan 4 vaatimuksiin. Vertailussa käytetyt tiedot ja hinnat perustuvat valmistajien www-sivujen tietoihin 20.3.2020.

Esitellyistä vaihtoehdoista varsinaiseen pisteytykseen valittiin kolme. Pelkällä autentikaattori sovelluksilla ei voida vastata esitettyihin turvallisuusvaatimuksiin sillä ne eivät yksistään integroidu Active Directoryyn ja mahdollista käyttäjän tunnistamista työasemalle kirjauduttaessa. Tästä syystä ne jätettiin pois lopullisesta vertailusta.

Ratkaisujen kustannukset on koottu vertailutaulukoon (taulukko 1). Kustannusten vertailussa on tehty esimerkkilaskelma suorista laite- ja lisenssikustannuksista 50 käyttäjälle 36 kk ajalla sellaisella kokoonpanolle millä voidaan toteuttaa kohdan 4 vaatimukset täyttävä kokonaisuus. Käyttöönottoon kuluvaa työtä ja käyttäjien koulutusta ei ole arvioitu eikä niiden osuutta huomioida vertailussa.

Ratkaisujen vertailemiseksi niiden vastaavuus vaatimuksiin pisteytettiin. Korkein mahdollinen pistemäärä oli 100. Ominaisuuksien painoarvoksi annettiin 60 pistettä jakautuen tasan ominaisuuksien kesken. Pisteitä annettiin seuraavasti muista kuin kustannuksista seuraavasti:
0 – ratkaisu ei vastaa vaatimusta
7,5 – ratkaisu vastaa vaatimukseen osin
15 – ratkaisu vastaa vaatimukseen kokonaisuudessaan

Kustannusten painoarvoksi annettiin 40 pistettä. Kustannusten pisteiden laskentaan käytettiin kaavaa missä halvin saa täydet pisteet ja muut suhteessa halvimpaan (Sihvola, 2017). Laskentakaava on

$$\frac{halvimman\ tarjoajan\ hinta}{tarjoajan\ hinta} * painoarvo$$

5.2.1 Autentikaattorisovellus

Helppokäyttöisyys

Älypuhelimen käyttö on käyttäjille rutiinia. Autentikaattorisovellukset tarjoavat lisäksi erilaisia tapoja kirjautumiseen.

Turvallisuus

Microsoft, Google ja muut suuret toimijat suosittelevat puhelimien sovelluksia niiden turvallisuuden vuoksi. Ei kuitenkaan tarjoa työasemalle kirjautumiseen

Kustannukset

Puhelimiin asennettavat sovellukset ovat lähestulkoon kaikki ilmaisia. Puhelimen vaihtuessa sovellus tulee asentaa myös uuteen puhelimeen, joten vaihtotilanteessa kuormittaa jonkin verran ylläpitoa tai käyttäjää. Kynnystä käyttöönottoon ja sen vaatimaan työkustannukseen madaltaa tarjolla oleva merkittävä määrä oppaita ja koulutusmateriaalia.

Integraatiot

Toimii erittäin hyvin Office 365 palvelun kanssa ja integroituu Active Directoryyn Office 365 toimintojen kautta. Ei kuitenkaan mahdollista monivaiheisen todentamisen toteutusta työasemille kirjautumiseen.

Yhteensopivuus

Yhteensopiva useimpien markkinoilla olevien päätelaitteiden ja käyttöjärjestelmien kanssa.

5.2.2 Yubico Yubikey

Helppokäyttöisyys

Paikalliselle työasemalle kirjautumiseen käytettynä USB-laite on helppo kytkeä tietokoneeseen mutta vaatii käyttäjältä lisätoimia ja yhden esineen lisää muistettavaksi ja kytkettäväksi laitteeseen. Office 365 kirjautumiseen vaaditaan USB-laitteen kytkennän lisäksi erillisen sovelluksen avaamisen ja sieltä numerokoodin kopioimisen kirjautumisen yhteydessä.

Turvallisuus

Yubikey on standardien mukaisesti toteutettu ja tarjoaa halutun turvallisuustason todentamiseen.

Kustannukset

30-50 € per avain. Käyttöönotto vaatii teknistä osaamista ja siihen tulee varata resursseja. Office 365 tunnistukseen tarvitaan lisäksi erillinen Azure AD Premium P1 lisenssi (Yubico, viitattu 20.3.202). Lisenssin kustannukset ovat 5,06 € / käyttäjä / kk (Microsoft, viitattu 20.3.2020).

Integraatiot

Toimii hyvin Microsoft Active Directoryn kanssa ilman lisäsovelluksia. Office 365 palvelun taustalla olevan Azure Active Directoryn käyttöön tarvitaan lisämaksullinen lisenssi. Mahdollista käyttää useiden U2F tukevien verkkopalveluiden kanssa.

Yhteensopivuus

Toimii Windows ja MacOs käyttöjärjestelmien kanssa.

5.2.3 Duo MFA

Helppokäyttöisyys

Duo mahdollistaa usean erilaisen tavan monivaiheiseen todentamiseen ja ne on suunniteltu helppokäyttöisiksi. Duoa voi käyttää autentikaattorisovelluksella tai avaimella kuten Yubikey.

Turvallisuus

Duon tuotteilla on arvioitu SOC 2 ja FIPS 140-2 vaatimusten mukaisesti. Tarjoaa halutun turvallisuustason todentamiseen.

Kustannukset

8,25 € / käyttäjä / kk ja haluttaessa Yubikeyt hankittava käyttäjille. Käyttöönottoon ja käyttäjien koulutukseen tulee varata resursseja.

Integraatiot

Autenkaattorisovellus toimii hyvin Microsoft Active Directoryn kanssa ja tukee Office 365 palvelua. Duo myös tukee merkittävää määrää muitakin verkkopalveluita. Duo-Yubikey yhdistelmää ei voida käyttää täysipainoisesti Active Directory kirjautumisiin (Duo. Viitattu 21.3.2020).

Yhteensopivuus

Toimii Windows ja MacOs käyttöjärjestelmien kanssa.

5.2.4 Authlite

Helppokäyttöisyys

USB-laite on helppo kytkeä tietokoneeseen mutta vaatii käyttäjältä lisätoimia ja yhden esineen lisää muistettavaksi. Tunnistautumiseen käytetty sovellus vaatii käyttäjältä yhden lisävaiheen kirjautumisen yhteydessä.

Turvallisuus

Authlite integroituu vahvasti paikalliseen Active Directoryyn ja tarjoaa halutun turvallisuustason todentamiseen. Sen yhteydessä on käytettävä Yubikeyta.

Kustannukset

Noin 100 € per käyttäjä hankinta ja Yubikeyt hankittava käyttäjille. Käyttöönottoon ja käyttäjien koulutukseen tulee varata resursseja.

Integraatiot

Toimii hyvin Microsoft Active Directoryn kanssa ja tukee Office 365 palvelua. Mahdollista käyttää myös etätyöpöytä ja VPN-yhteyksissä.

Yhteensopivuus

Toimii Windows ja MacOs käyttöjärjestelmien kanssa.

5.3 Ratkaisujen kustannusvertailu ja pisteytys

TAULUKKO 1. Kustannukset

	Hankintahinta	**Ylläpitomaksut**	**Yhteensä**
Yubico Yubikey	2062,00 € Yubikeyt	9108,00 € *	11 170,00 €
Duo puhelinsovelluksella	0 €	14 850,00 € **	14 850,00 €
Duo Yubikey avaimella	2062,00 € Yubikeyt	14 850,00 € **	16 912,00 €
Authlite	2296,00 € lisenssi 2062,00 € Yubikeyt	0 €	4358,00 €

* 5,06 € / käyttäjä / kuukausi Azure AD Premium P1 lisenssi

** 8,25 € / käyttäjä / kuukausi Duo Beyond lisenssi

TAULUKKO 2. Pisteytys

	Helppokäyt-töisyys	**Turvalli-suus**	**Kustannuk-set**	**Integraatio**	**Yhteensopi-vuus**	**Yhteensä**
Yubico Yubi-key	7,5	15	15,06	15	15	67,56
Duo puhelin-sovelluksella	15	15	11,74	15	15	71,74
Duo Yubikey avaimella	7,5	15	10,30	15	15	62,8
Authlite	7,5	15	40	15	15	92,5

5.4 Ratkaisun valinta

Tasapainoinen kokonaisuus osion 4 vaatimusten mukaisesti on Authliten ratkaisu. Se toteuttaa kaikki 4.4 kohdan vaatimukset ollen kuitenkin kustannuksiltaan kohtuullinen. Esimerkkilaskelman suorat laite- ja lisenssikustannuksista 50 käyttäjälle 36 kk ajalle ovat 4358,00 €. Authlite saa myös vertailussa eniten pisteitä ja siten ratkaisuksi tässä esimerkkitapauksessa päädytään Authliten ratkaisuun.

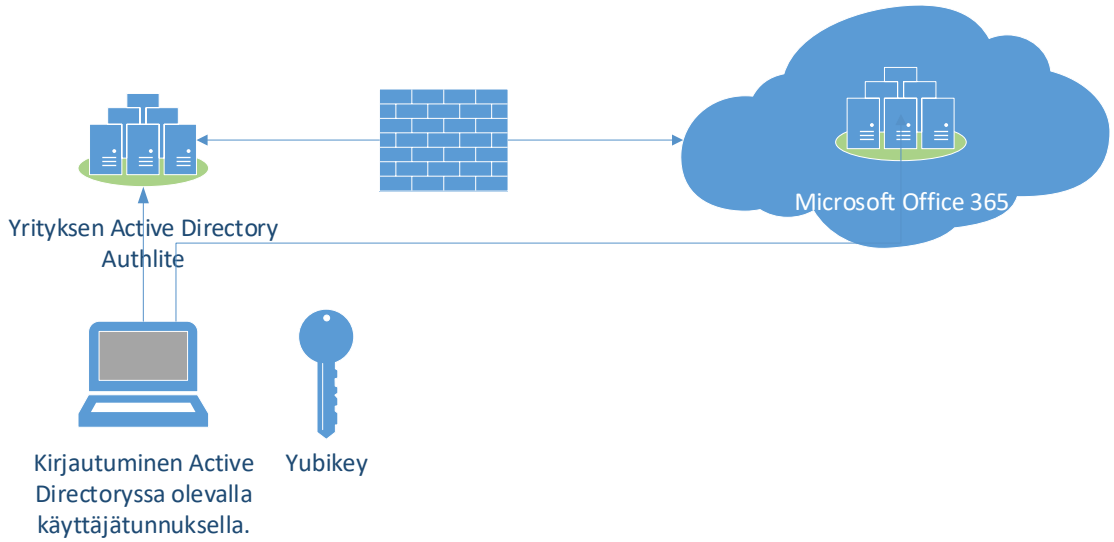
5.4.1 Vaihtoehtoinen valinta

Vertailun lähtökohtana oli yhden käyttäjäkokemuksen ratkaisun valinta. Mikäli tätä vaatimusta muutetaan ja sallitaan erilaiset käyttäjäkokemukset eri palveluille, niin voidaan vaihtoehtoisena ratkaisuna pitää autentikaattori sovelluksen ja Yubico Yubikeyn yhdistelmää. Tässä vaihtoehdossa Office 365 palveluun kirjaudutaan puhelimen autentikaattorisovelluksella ja työasemalle kirjautumiseen käytetään Yubikey avainta. Tällöin kustannukset ovat hankinnan osalta Yubikey avaimet eikä muita kuluja synny käyttöönoton lisäksi.

6 MONIVAIHEISEN TODENNUKSEN KÄYTTÖÖNOTTO

Monivaiheisen todennuksen käyttöönotto vaihtelee valitun ratkaisun mukaan. Tässä työssä ei tarkoituksena ollut Liitteessä on luetteloituna vaiheet Authliten käyttöönottoon. Siinä viitataan valmistajan tarkempaan tekniseen dokumentointiin mihin tulee tutustua seikkaperäisemmin, mikäli ryhtyy käyttöönottamaan Authliten ratkaisua.

Käyttöönotto tehtiin esitellyn vaiheistuksen mukaan erillisessä testiympäristössä mikä asennettiin vain tätä tarkoitusta varten. Testiympäristö käsittää kaksi virtuaalikonetta, palvelimena toimii Windows 2016 ja työasemana Windows 10. Nämä on kytketty toisiinsa lähiverkolla. Lähiverkkoon todentamisen palvelut tuotetaan Windows 2016 palvelimeen asennetulla Active Directorylla. Lisäksi käyttöönotettiin Office 365 palvelu testikäyttöön ja kytkettiin paikallisen testiympäristön Active Directoryyn.



KUVIO 9. Testiympäristön periaatekuva

Vaihtoehtoisen ratkaisun käyttöönoton yleiskuvaukset kirjattiin liitteille perustuen valmistajien ohjeistuksiin.

7 POHDINTA

Opinnäytetyöni loppuvaiheessa maailma koki ennen näkemättömän poikkeustilan COVID-19 pandemian takia. Monet asiat muuttuivat juuri raportin kirjoittamisen viime hetkillä ja kirjoitin tämän pohdinnan kotimaassamme vallitsevan poikkeustilan aikana. Useat valtiot pyrkivät hillitsemään pandemiaa monin keinoin ja kymmenet ellei jopa sadat miljoonat toimihenkilöt siirtyivät parin viikon aikana toimistoilta etätöihin, eikä järjestelyn ajallisesta kestosta ole kenelläkään tarkempaa tietoa. Samaan aikaan alkoivat verkossa leviämään pandemiaa uutisointiin liittyvät huijaukset ja haittaohjelmat, joiden avulla opportunistiset rikolliset pyrkivät hyötymään kaikkiin kohdistuvasta uhasta. Muuttuneessa maailmantilassa johdannossa esitelty monivaiheisen todennuksen tarpeellisuus tietoturvauhkien torjunnassa nousi uuteen tasoon, sillä yhteiskunnan ja yritysten toimihenkilöiden työ siirtyi käytännössä kahdessa viikossa etätyövälineiden kuten Office 365 ja G Suite varaan.

Työn tuloksiksi voidaan lukea kaksi asiaa, yleisen tason vaatimukset monivaiheisen todentamisen toteutukselle ja sitä vastaava toteutus markkinoiden tarjonnasta, joiden myötä saavutettiin työlle asetettu tavoite. Tuloksia hyödyntämällä voi pk-yrityksen tietoturvallisuudesta vastaava ryhtyä toimenpiteisiin oman organisaationsa todentamisen kehittämisessä.

Yleisen tason vaatimusten määrittely oli työni vaikein osuus. Lähtökohtaisesti tietoturvakontrollit, joihin myös monivaiheinen todentaminen lukeutuu, pitäisi aina ottaa käyttöön riskiperusteisesti. Tässä työssä jouduttiin kuitenkin tekemään vaatimusmäärittely perustuen yleiseen uhkakuvaan, tietoturvan yleisesti tunnettuihin parhaisiin käytäntöihin ja kaikkia koskeviin lain säädännön vaatimuksiin perustuen. Tämä seikka tulisikin huomioida työn tuloksia hyödynnettäessä.

Toinen haastetta aiheuttanut seikka oli vertailuun otettavien ratkaisujen valinta. Markkinoilla on merkittävä määrä erilaisia ratkaisuja mutta pk-yritysten vaihtelevan tarpeen vuoksi halusin saada mukaan erilaisia toteutuksia antamaan paremman kuvan mahdollisuuksista kuin niinkään tehdä täydellistä vertailua markkinoilla olevista ratkaisuista, Perustin päätökseni siihen, että määriteltyjen yleisten vaatimusten ja vertailussa kuvattujen ratkaisujen kautta voivat pk-yritysten tietoturvasta vastaavat tehdä tarvittaessa omaa vertailua markkinoiden tarjonnasta ja siinä yhteydessä myös tarkentaa omaa vaatimismäärittelyään tässä työssä tehdystä yleisestä tasosta.

Työtä voisi jatkaa kahdella tavalla. Yleisen vaatimusmäärittelyn lisäksi voisi luoda kysymyspatteriston kartoittamaan tarkemmin pk-yrityksen todentamisen tarvetta ja siitä johtaa vertailtavat asiat sekä pisteytyksen painotus. Toinen jatkoksi tehtävä asia olisi laatia markkinoiden tarjonnan suppeasta kartoituksesta laajamittaisempi vertailu. Parhaimman hyödyn jatkotyössä saataisiin yhdistämällä molemmat, jolloin lopputuloksena olisi tätä työtä laajemmin hyödynnettävä työkalu.

LÄHTEET

Alexander, E. 27.11.2018. Usability is security. Duo. Viitattu 18.2.2020. https://duo.com/blog/part-1-usability-is-security

Authlite. Viitattu 7.3.2020. https://www.authlite.com

Azure Active Directory Pricing. Microsoft. Viitattu 20.3.2020. https://azure.microsoft.com/en-us/pricing/details/active-directory/

Child, M. 21.10.2019. Balancing Security with User Experience: How Everyone Wins! Lastpass. Viitattu 18.2.2020. https://blog.lastpass.com/2019/10/balancing-security-with-user-experience-how-everyone-wins.html/

Cimpanu, C. 27.8.2019. Microsoft: Using multi-factor authentication blocks 99.9% of account hacks. ZDNet. Viitattu 17.2.2020. https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/

Duo. Viitattu 7.3.2020. https://www.duo.com

Duo. 2020. Two-Factor Authentication (2FA) from Duo. Viitattu 28.2.2020. https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa

EU yleinen tietosuoja-asetus. Viitattu 17.2.2020. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI#d1e40-1-1

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

iSynergy 27.1.2020. Why you should reconsider using SMS for your MFA needs. Viitattu 10.3.2020. https://www.icsynergy.com/2020/01/reconsider-using-sms-mfa-needs/

Kyberturvallisuuskeskus 4.10.2019. Näin pidät huolta tietoturvasta kotona ja työpaikalla. Viitattu 11.2.2020, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvaohjeet/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla

Kyberturvallisuuskeskus 2018. Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota! Varoitus 3/2018. Viitattu 31.1.2020, https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Logging Into Microsoft Windows with Duo. Viitattu 21.3.2020. Duo. https://guide.duo.com/rdp#win-logon-auth

Mattila, A-L. 2014. Tietoa sähköpostiviestien tietoturvasta. Oulun Ammattikorkeakoulu. Viitattu 3.2.2020, https://it.oamk.fi/3300.

Millman, R. 20.1.2020. Sim swap attacks making two-factor authentication via smartphones obsolete. SC Media. Viitattu 10.3.2020. https://www.scmagazineuk.com/sim-swap-attacks-making-two-factor-authentication-via-smartphones-obsolete/article/1671302

Opsec Oy. Yubikey. Viitattu 7.3.2020. https://www.opsec.fi/fi/ratkaisut/yubikey/

Opsec Oy, Yubikey ohje. Viitattu 20.3.2020. Ei julkaistu.

OWASP Foundation Inc. 2020. Password Storage Cheat Sheet. Viitattu 4.2.2020. https://owasp.org/www-project-cheat-sheets/cheatsheets/Password_Storage_Cheat_Sheet.html

Pervilä,M. 31.7.2019. Kysely: 66 prosenttia pk-yritysten johtajista ei usko, että juuri heidän johtamansa yritys voisi joutua kyberiskun kohteeksi. Tekniikka ja talous. Viitattu 17.2.2020 https://www.tekniikkatalous.fi/uutiset/kysely-66-prosenttia-pk-yritysten-johtajista-ei-usko-etta-juuri-heidan-johtamansa-yritys-voisi-joutua-kyberiskun-kohteeksi/06dbca2c-f213-4492-8a30-225b9be0f362

Rikama, S. 2019. Yritysten digitaalinen liiketoiminta mittareiden valossa. Työ- ja elinkeinoministeriö. Yrityskatsaus 1/2019. Viitattu 3.2.2020, https://yrityskatsaus.fi/yritysten-digitaalinen-liiketoiminta-mittareiden-valossa/

Serpa,J. 30.5.2018. Cloud Security Trailing Cloud App Adoption in 2018. Bitglass. Viitattu 17.2.2020. https://www.bitglass.com/blog/cloud-security-trailing-cloud-apps

Sihvola, I. 26.9.2017. Painoarvojen ja erilaisten laskukaavojen käyttäminen tarjousten vertailussa. Hansel, Viitattu 20.3.2020. https://www.kinno.fi/sites/default/files/sihvola_hansel_painoarvojen_ja_laskukaavojen_kayttaminen.pdf

Stewart, J., Chapple, M. & Gibson, D. 2015. Certified Information Systems Security Professional Study Guide. 7.painos. Indianapolis: Sybex.

Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä [verkkojulkaisu]. ISSN=1797-2957. 2019, 3. Pilvipalvelut. Helsinki: Tilastokeskus [viitattu: 12.2.2020]. Saantitapa: http://www.stat.fi/til/icte/2019/icte_2019_2019-12-03_kat_003_fi.html

Tilastokeskus viitattu 13.2.2020. Käsitteet: PK-Yritys. https://www.stat.fi/meta/kas/pk_yritys.html

Using YubiKeys with Azure MFA. 1.7.2019. Yubico, Viitattu 20.3.2020. https://support.yubico.com/support/solutions/articles/15000024567-using-yubikeys-with-azure-mfa#Logging_into_O365_with_YubiKeys_as_a_Second_Factor%C2%A0f2ze0j

Vesterinen, P. 27.9.2019. Yrityksiin kohdistuvat kyberuhat 2019. Helsingin seudun kauppakamari. Viitattu 18.2.2020. https://view.24mags.com/helsinki.chamber/yrityksiin-kohdistuvat-kyberuhat-2019#/page=1

Yubico. Viitattu 7.3.2020. https://www.yubico.com

AUTHLITE JÄRJESTELMÄN KÄYTTÖÖNOTON VAIHEET **LIITE 1**

Tässä on eriteltynä ne vaiheet, miten AuthLite otetaan käyttöön Active Directory ja Office 365 todentamiseen. Vaiheistus on tarkoitettu suuntaa antavaksi tehtävälistaksi eikä varsinaiseksi asennusoppaaksi. Ennen käyttöönoton aloittamista tuleekin tutustua valmistajan dokumentaatioon osoitteessa https://www.authlite.com/docs/2_3/id_1126579819/.

1. Asennuksen suunnittelu ja vähimmäisvaatimusten tarkastus.
    a. Tuetut käyttöjärjestelmät ja vähimmäisvaatimukset https://www.authlite.com/docs/2_3/id_1805207740/ ja https://www.authlite.com/docs/2_3/id_1866910622/
2. Asennus palvelimelle
    a. Asennuksen ohjeistus eri alustoille ja palvelin rooleilla https://www.authlite.com/docs/2_3/id_779534525/
3. Lisenssin asennus
    a. Lisenssin asennuksen ohjeistus https://www.authlite.com/docs/2_3/id_1370961686/
    b. Lisenssiavaimen hankinta https://tix.authlite.com/tickets/new/2-Authlite-Activation
4. Käyttäjien määrittely
    a. Ryhmien luonti https://www.authlite.com/docs/2_3/id_589094306/
    b. Authliten asettaminen käyttämään ryhmiä https://www.authlite.com/docs/2_3/id_1288347853/
    c. Perusryhmä Auhtlite käyttäjille https://www.authlite.com/docs/2_3/id_1161038366/
5. Yubikey avainten määrittely käyttäjille
    a. Avainten määrittely työasemalla https://www.authlite.com/docs/2_3/id_1142456219/
    b. Avainten tuonti Authlite järjestelmään https://www.authlite.com/docs/2_3/id_268561548/
    c. Avainten asettaminen käyttäjlle https://www.authlite.com/docs/2_3/id_1432569501/
6. Sovelluksen asennus tietokoneille
    a. https://www.authlite.com/docs/2_3/id_1255664859/
7. Monivaiheisen todennuksen käyttöönotto

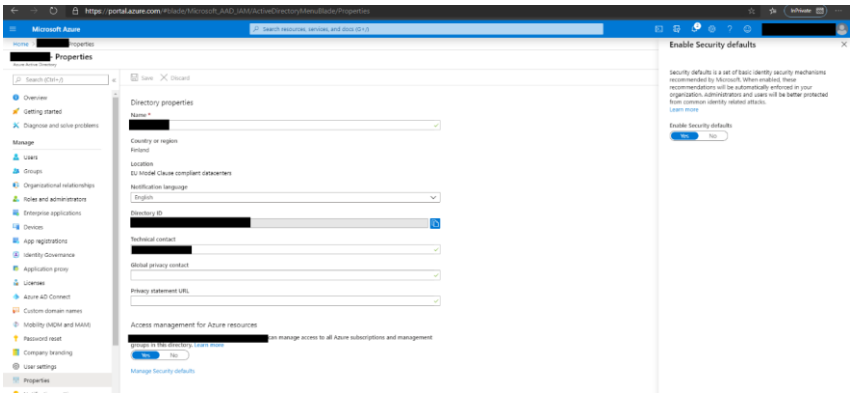
a. Tietokoneille kirjautumisen asetukset https://www.auth-lite.com/docs/2_3/id_1587484890/
b. Tietokoneille kirjautumisen pakottaminen https://www.auth-lite.com/docs/2_3/id_217022693/
c. Office 365 kirjautumisen käyttöönotto Authlite https://www.auth-lite.com/docs/2_3/id_1655819967/
d. Office 365 kirjautumisen käyttöönotto Microsoft https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

Monivaiheisen todentamisen käyttöönotto Office 365 ympäristössä vaatii aluksi järjestelmän hallinnoijan koko organisaatiota koskevien toimenpiteiden suorittamista. Niiden jälkeen monivaiheinen todennus voidaan ottaa käyttöön varsinaisille käyttäjille. Office 365 palvelun ja Active Directoryn integraatio voidaan toteuttaa Azure AD Connect työkalulla. Sen avulla käyttäjät ja salasanat voidaan synkronoida Active Directoryn ja Office 365 palvelun välillä mikä helpottaa käyttäjän toimia, kun kirjautumisen tiedot ovat samat. Lisätietoja saatavilla Microsoftin dokumentaatiossa osoitteessa https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis ja https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express.

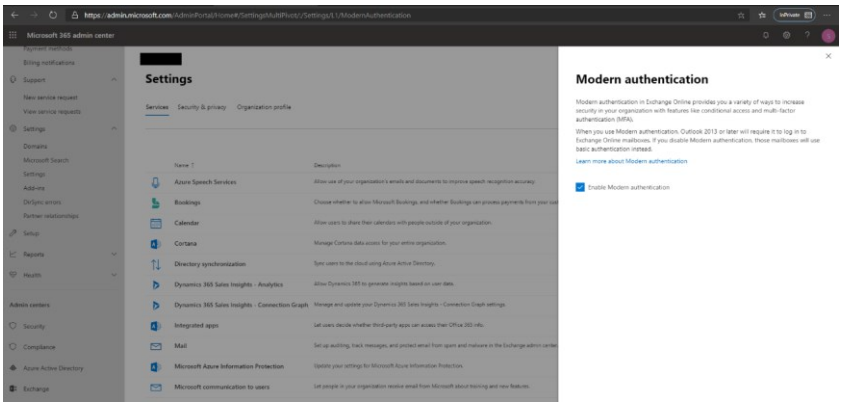
Järjestelmän valmistelevat toimet

Järjestelmän käyttöönotto vaatii muutamien asetusten tekemistä. Nämä asetukset on esitelty ohessa toimenpidettä selkeyttävien kuvakaappausten kanssa.

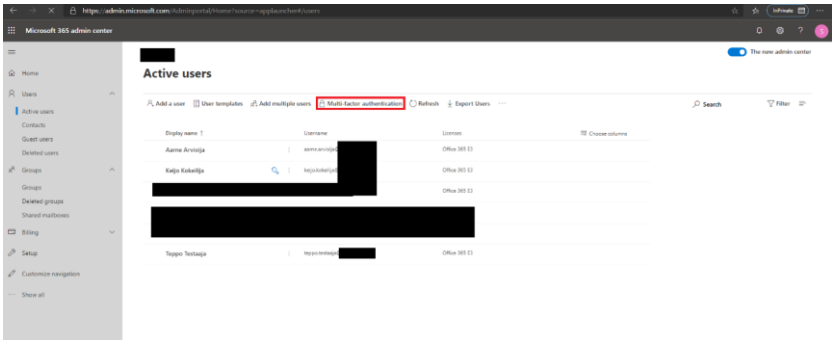
1. Aseta käyttöön Security Defaults asetus.

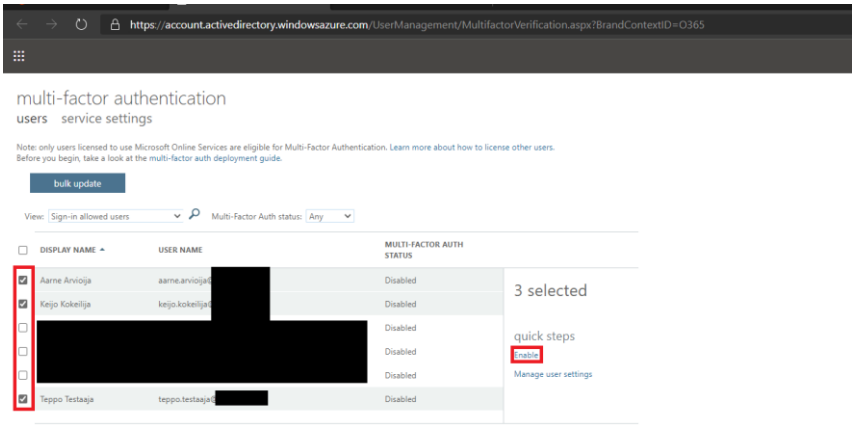


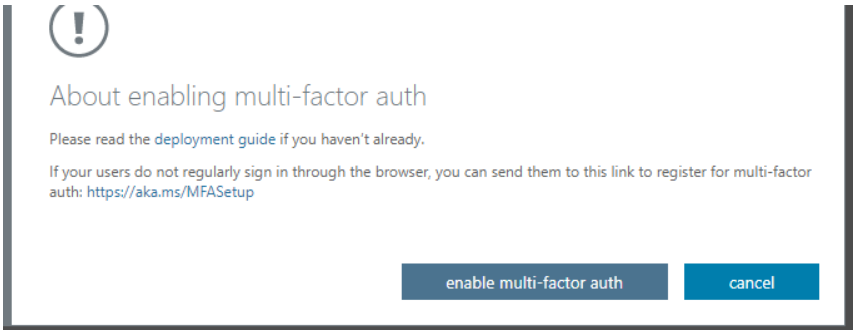
2. Ota käyttöön Modern authentication ominaisuus.

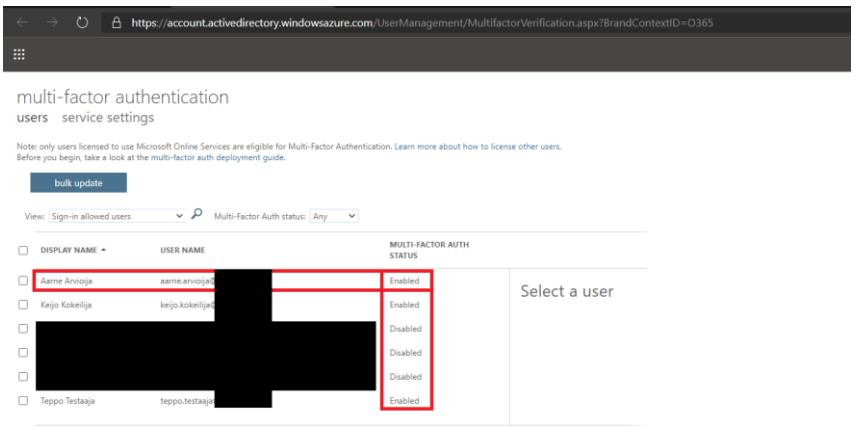


3. Aktivoi monivaiheinen todentaminen yhdelle tai useammalla käyttäjälle.









Tarkempi ohjeistus on saatavilla Microsoftin dokumentaatiossa osoitteessa https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

Käyttäjän valmistelevat toimet ja todentamisen käyttö

Käyttäjän valmistelevat toimet ovat sovelluksen asennus ja sen määrittely Office 365 palvelun todentamisen menetelmäksi. Sovellus on saatavilla Androidlle https://play.google.com/store/apps/details?id=com.azure.authenticator ja iOSille https://apps.apple.com/app/azure-authenticator/id983156458

Ohje käyttöönotosta ja käytöstä on osoitteessa https://support.office.com/en-us/article/use-microsoft-authenticator-with-office-365-1412611f-ad8d-43ab-807c-7965e5155411

Teknisesti Yubikey avaimet toimivat Active Directoryn näkökulmasta älykortteina ja niissä käytetään sertifikaatteja todentamiseen. Sertifikaattipalveluiden ja sen taustalla olevan julkisen avaimen infrastruktuurin laajempi esittely on tämän opinnäytetyön laajuuden ulkopuolella. Lisätietoja asiasta on saatavissa useista lähteistä ja Microsoftin toteutuksesta voi lukea osoitteessa https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v%3Dws.11)

Yubikeyn käyttöönoton päävaiheet ovat

1. Asennuksen suunnittelu ja vähimmäisvaatimusten tarkastus.
2. Sertifikaattien varmentajan (certificate authority) asennus.
3. Sertifikaatti mallipohjan (certificate template) valmistelu.
4. Ryhmäkäytäntöjen (group policy) määrittely.
5. Käyttäjien Yubikey avainten käyttöönotto.

Kaikkien vaiheiden tarkempi ohjeistus on Yubicon dokumentaatiossa osoitteessa https://support.yubico.com/support/solutions/articles/15000006456-yubikey-smart-card-deployment-guide

Asennuksen suunnittelu ja vähimmäisvaatimusten tarkastus

Ennen asennusta tulee se suunnitella ja varmistaa vähimmäisvaatimusten täyttyminen. Yubikeyn käyttöönoton suunnittelussa tulee päättää miten Yubikey avaimet asennetaan ja jaellaan käyttäjille, mahdollisessa lukkiutumistilanteessa PUK-koodin käyttö, vaatiiko Yubikey kosketusvahvistuksen kirjautumiseen sekä miten tietokone käyttäytyy, kun avain irrotetaan. Vähimmäisvaatimukset ovat lähinnä käyttöjärjestelmän ja Active Directoryn versioiden tarkistukset.

Sertifikaattien varmentajan (certificate authority) asennus

Sertifikaattien varmentaja tehdään palvelimella, että avaimille voidaan jakaa sertifikaatit todentamista varten. Sertifikaatin varmentaja palvelu on osa Windows käyttöjärjestelmän palveluita ja sen vuoksi sen käyttöönottoa ennen tulee tutustua myös Microsoftin ohjeistukseen aiheesta osoitteessa https://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx

Sertifikaatti mallipohjan (certificate template) valmistelu

Sertifikaatin mallipohja toimii kaikkien avaimiin myönnettävien sertifikaattien mallina. Mallipohja valmistellaan Yubicon dokumentaation mukaan avaimen asentamiseksi.

Ryhmäkäytäntöjen (group policy) määrittely

Ryhmäkäytännöt ovat Active Directoryn työkalu jakaa keskitetysti asetuksia tietokoneille ja käyttäjille. Niitä käytetään Yubikeyn yhteydessä määrittelemään asetukset, miten avaimet jaetaan käyttäjille ja miten niitä käytetään. Ryhmäkäytäntöjen toiminnan laajempi esittely on tämän opinnäytetyön laajuuden ulkopuolella. Lisätietoja asiasta on saatavissa osoitteessa https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v%3Dws.11)

Käyttäjien Yubikey avainten käyttöönotto

Yubikey avaimet otetaan käyttöön suunnitteluvaiheessa päätetyillä menettelyillä.