Noora Ryhänen

YKSIVAIHEISEN TUNNISTAUTUMISEN PUUTTEET JA MONIVAIHEISEN TUNNISTAUTUMISEN VAIHTOEHDOT YRITYSJÄRJESTELMISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Ryhänen, Noora
Yksivaiheisen tunnistautumisen puutteet ja monivaiheisen tunnistautumisen vaihtoehdot yritysjärjestelmissä
Jyväskylä: Jyväskylän yliopisto, 2023, 26 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Kokko, Tuomas

Informaatioteknologian kehittyminen on lisännyt liiketoimintamahdollisuuksia, mutta samanaikaisesti kasvattanut tietoturvariskien määrää. Tietoturvavahingot voivat aiheuttaa yrityksille erilaisia vahinkoja ja jopa tuhota koko tietojärjestelmän. Ensimmäinen keino tietoturvauhkia vastaan on käyttäjien todentaminen ennen kuin he pääsevät sisään tietojärjestelmiin. Yleisimmin yritysjärjestelmiin kirjaudutaan sisään yksivaiheisella tunnistautumisella käyttämällä salasanaa ja käyttäjätunnusta. Yksivaiheisen tunnistautumisen on kuitenkin havaittu olevan turvallisuudeltaan riittämätön nykypäivän uhkia vastaan. Suositeltavaa olisi ottaa käyttöön monivaiheinen tunnistautuminen, joka lisää turvallisuutta. Tässä tutkielmassa selvitettiin, miksi yksivaiheinen tunnistautuminen on puutteellinen, ja mitä riskejä etenkin käyttäjätunnuksella ja salasanalla kirjautumiseen liittyy. Lisäksi tutkittiin, mitkä monivaiheisen tunnistautumisen keinot voisivat olla yrityksille potentiaalisimmat huomioiden turvallisuus- ja käytettävyysnäkökulman. Salasanojen ja käyttäjätunnusten huomattiin aiheuttavan riskejä etenkin kognitiivisen kuormituksen ja käyttäjien heikon salasanahallinnan vuoksi. Potentiaalisimmiksi monivaiheisen tunnistautumisen keinoiksi tunnistettiin älykortin tai biometriikan yhdistäminen salasanan kanssa. Näistä älykorttipohjainen todennusjärjestelmä saattaa olla vielä parempi, koska se ei ole niin herkkä olosuhteille. Tutkielma toteutettiin systemaattisena kirjallisuuskatsauksena. Aineistona käytettiin pääosin vertaisarvioituja tieteellisiä artikkeleita, joita on etsitty JYKDOK-tietokannasta sekä Google Scholar -hakupalvelusta.

Asiasanat: monivaiheinen tunnistautuminen, yksivaiheinen tunnistautuminen, tunnistautumismenetelmä, tietoturva

ABSTRACT

Ryhänen, Noora
Shortcomings of single-factor authentication and options for multi-factor authentication in enterprise systems
Jyväskylä: University of Jyväskylä, 2023, 26 pp.
Information Systems, Bachelor's Thesis
Supervisor: Kokko, Tuomas

The development of information technology has increased business opportunities, but at the same time it has increased the number of security risks. Security breaches can cause various types of damage to companies and even destroy an entire information system. The first way to deal with security threats is to authenticate users before they have access to information systems. The most common way of logging into enterprise systems is through a single-factor authentication using a password and a username. However, single-factor authentication has been found to be insufficiently secure against current threats. The use of multi-factor authentication is recommended to increase security. This thesis explained why single-factor authentication is inadequate and what the risks are, especially when logging in with a username and password. It also analysed which multi-factor authentication methods could be the most potential for enterprises, considering security and usability aspects. Passwords and usernames were found to cause risks due to cognitive load and poor password management by users. Smart card-password and biometrics-password combinations were identified as the most potential multi-factor authentication methods. Of these, a smart card-based authentication system may be even better, as it is less sensitive to circumstances. The research was conducted as a systematic literature review. The sources used were mainly peer-reviewed scientific articles searched in the JYKDOK database and Google Scholar.

Keywords: multifactor-authentication, single-factor authentication, authentication method, information systems security

KUVIOT

SISÄLLYS

1 JOHDANTO

Tietoturvasta huolehtiminen on nykyään yhä tärkeämpää yrityksille. Hyvin rakennettu kyberturvallisuus suojaa organisaation toimintakykyä sekä mahdollistaa digitaalisten palveluiden ja järjestelmien hyödyntämisen liiketoiminnassa (Kyberturvallisuuskeskus, 2022a). Tärkeys käy konkreettisesti ilmi Ylen artikkelista, jossa Mäentausta (2022) kirjoittaa Muuramen kunnan tehneen rikosilmoituksen mahdollisesta tietomurrosta. Tietomurtoa oli alettu epäillä, kun työntekijät eivät olleet päässeet kirjautumaan sisäisiin järjestelmiin ja esimerkiksi kulunhallinnassa oli ollut häiriöitä. Tilanteen korjaamisen arvioitiin kestävän useita päiviä. (Mäentausta, 2022).

Tässä tutkielmassa selvitetään, millaisia turvallisuushaasteita yrityksille aiheutuu, kun järjestelmiin kirjaudutaan yksivaiheisella tunnistautumisella. Tunnistautuminen tai todennus on prosessi, jolla varmistetaan käyttäjän henkilöllisyys ennen kuin hän pääsee käyttämään järjestelmän resursseja (Velásquez, Caro & Rodríguez, 2018a). Tunnistautumisella varmistetaan, että järjestelmään pääsevät käsiksi vain sellaiset henkilöt, joilla on siihen oikeus. Yksivaiheinen tunnistautuminen tarkoittaa sitä, että järjestelmään kirjaudutaan sisään käyttämällä vain yhtä todennusmenetelmää, esimerkiksi salasanaa ja käyttäjätunnusta. Tässä tutkielmassa yksivaiheisella tunnistautumisella viitataan nimenomaan vain perinteiseen salasanakirjautumiseen, koska se on yleisimmin käytössä oleva tunnistautumiskeino (Zimmermann & Gerber, 2020). Yksivaiheinen tunnistautuminen voi tapahtua myös esimerkiksi sormenjäljen tai kasvojen tunnistuksen avulla, mutta niiden turvallisuuteen ei oteta kantaa tässä tutkielmassa.

Tutkielmassa vertaillaan lisäksi monivaiheisen tunnistautumisen keinoja ja ehdotetaan turvallisuudeltaan ja käytettävyydeltään potentiaalisimpia vaihtoehtoja. Monivaiheisessa tunnistautumisessa käyttäjä kirjautuu järjestelmään sisään käyttäen kahta tai useampaa todennuskeinoa, esimerkiksi älykorttia ja salasanaa. Joissain yhteyksissä todentamisesta voidaan käyttää myös englannin kielestä johdettua termiä autentikointi (engl. authentication). Tässä tutkielmassa käytetään selvyyden vuoksi termejä tunnistautuminen ja todennus.

Tutkielman tavoitteena on löytää yritysten näkökulmasta parhaat monivaiheisen tunnistautumisen keinot huomioiden sekä turvallisuuden, että käytettävyyden. Tutkielman tutkimuskysymykset ovat seuraavat:

- Miksi salasanat luovat tietoturvahaasteita yrityksille?
- Mitkä monivaiheisen tunnistautumisen keinot voisivat olla yrityksille potentiaalisimmat?

Tutkielma on toteutettu ensisijaisesti turvallisuus- ja käytettävyysnäkökulmasta eikä siinä oteta kantaa ratkaisujen tekniseen toteutukseen. Myöskään ratkaisujen kustannuksiin ei oteta tässä vertailussa kantaa.

Velásquezin ym. (2018a) mukaan tutkituimpia todennuskeinoja ovat tekstipohjaiset salasanat, älykortti sekä biometriset perintötekijöihin liittyvät keinot. Tämän tiedon tuella tässä tutkielmassa valitaan tarkempaan tarkasteluun salasanat, älykortti, sormenjälki ja kasvojen tunnistus. Monivaiheisen tunnistautumisen vaihtoehdoista tarkastellaan enimmäkseen salasanan ja älykortin sekä salasanan ja biometrian yhdistelmiä, koska ne näyttäisivät tutkimusaineiston perusteella olevan eniten tutkitut kombinaatiot.

Tutkielma on toteutettu systemaattisena kirjallisuuskatsauksena. Lähteinä on käytetty pääasiassa vertaisarvioituja tieteellisiä Julkaisufoorumin (JUFO) arvioimia artikkeleita. Käytetyt artikkelit ovat saaneet JUFO-luokituksen 1–3. Lähteinä on pyritty käyttämään enimmäkseen ajantasaisia artikkeleita, jotka on julkaistu vuonna 2015 tai sen jälkeen. Mukana on kuitenkin myös joitain vanhempia artikkeleita, jotka ovat sisällöltään relevantteja. Tiedonkeruussa on hyödynnetty Jyväskylän yliopiston kirjaston ylläpitämää JYKDOK-tietokantaa sekä Google Scholar -hakupalvelua. Aineistoa on arvoitu kriittisesti muun muassa julkaisuvuosien, vertaisarvioinnin ja JUFO-arviointien perusteella.

Tutkielma etenee siten, että ensimmäisessä sisältöluvussa käsitellään yksivaiheista tunnistautumista ja siinä vastataan ensimmäiseen tutkimuskysymykseen salasanojen aiheuttamista tietoturvahaasteista. Sen alaluvuissa avataan ensin yleisesti tunnistautumista ja tietoturvaa sekä niihin liittyviä käsitteitä, kunnes siirrytään käsittelemään salasanatunnistautumisen puutteita ja keinoja, joilla salasanoja voitaisi vahvistaa. Toinen sisältöluku käsittelee monivaiheista tunnistautumista ja sen alaluvuissa keskitytään omistuspohjaisiin ja biometrisiin todennuskeinoihin sekä niiden puutteisiin. Viimeinen sisältöluku on varattu aineiston analysoinnille ja vertailulle, ja siinä vastataan myös toiseen tutkimuskysymykseen. Tutkielman lopussa tehdään vielä yhteenveto käsitellyistä aiheista ja tuloksista. Tutkielman lukijalla tulisi tämän jälkeen olla hyvä kokonaiskuva aiheen termistöstä sekä ymmärrys siitä, miksi yksivaiheiseen salasanakirjautumiseen liittyy riskejä ja miksi monivaiheinen tunnistautuminen on yrityksille suotavaa. Tutkielma ei tarjoa absoluuttista ratkaisua, koska se on toteutettu turvallisuus- ja käytettävyysnäkökulmasta eikä siinä oteta kantaa muun muassa kustannuksiin, tekniseen toteutustapaan tai kontekstiin. Paras tunnistautumiskeino kullekin yritykselle riippuu aina viimekädessä yrityskohtaisista tarpeista ja tilanteesta.

2 YKSIVAIHEINEN TUNNISTAUTUMINEN

Tässä luvussa käsitellään yksivaiheista tunnistautumista eli SFA:ta (engl. Single-Factor Authentication), joka on yksinkertaisin tunnistautumisen taso. Siinä todentamiseen käytetään todentamistekijää tai -tekijöitä vain yhdestä todentamisryhmästä, esimerkiksi tietopohjaista salasanaa ja käyttäjätunnusta (Ometov ym., 2018, s. 2). Todentamisryhmät avataan tarkemmin alaluvussa 2.1. Yksivaiheinen tunnistautuminen on yksinkertainen ja käyttäjäystävällinen, mutta samalla se on myös turvallisuudeltaan heikoin todentamismenetelmä (Ometov ym., 2018, s. 2).

Tässä luvussa avataan ensin yleisesti tunnistautumista ja tietoturvaa sekä niihin liittyviä käsitteitä. Seuraavissa alaluvuissa käsitellään salasanatunnistautumisen puutteita sekä keinoja, joilla salasanoista saataisiin vahvempia. Luvun tarkoituksena on avata lukijalle yleistä taustaa ja käsitteistöä tunnistautumisesta, tietoturvasta ja salasanoista sekä perustella, miksi yksivaiheinen salasanatunnistautuminen on puutteellista erilaisia uhkia vastaan.

2.1 Yleistä tunnistautumisesta ja tietoturvasta

Velásquezin ym. (2018a) mukaan yksi suurimmista riskeistä mille tahansa järjestelmälle tai tietokonelaitteelle on se, että joku esiintyy valtuutettuna käyttäjänä, vaikka ei oikeasti ole sellainen. Käyttäjän todentaminen on ensimmäinen suojautumiskeino tätä uhkaa vastaan. (Velásquez ym., 2018a). Käyttäjän todentaminen on tärkeää, jotta voidaan varmistua siitä, että palvelimen resursseja käyttävät vain lailliset osapuolet (Wang, Zhang, Zhang & Wang, 2020). Todentaminen tapahtuu siten, että järjestelmä vertaa tunnistautuvan käyttäjän antamia tunnistetietoja järjestelmän tietokantaan tallennettuihin tunnistetietoihin (Limbasiya, Soni & Mishra, 2018). Jos käyttäjän antamat tiedot täsmäävät järjestelmän tietokannan tietoihin, hän pääsee kirjautumaan sisään järjestelmään.

Tietoa, jota käytetään käyttäjän henkilöllisyyden todentamiseen, kutsutaan todentamistekijäksi tai -keinoksi (Velásquez ym., 2018a). Todentamiskeinot jaetaan useimmiten kolmeen eri ryhmään: tietopohjaisiin, omistuspohjaisiin ja

biometrisiin keinoihin. Ometovin, Bezzateevin, Mäkitalon, Andreevin, Mikkosen ja Koucheryavyn (2018) mukaan tietopohjaiset menetelmät ovat jotain sellaista, mitä käyttäjä tietää. Tällaisia ovat esimerkiksi tavallisimmin käytetty käyttäjätunnus-salasana yhdistelmä. Omistuspohjaisissa menetelmissä todentamiseen käytetään jotain käyttäjän fyysisesti omistamaa apuvälinettä, kuten älypuhelinta tai älykorttia. (Ometov ym., 2018, s. 2). Joissain lähteissä omistuspohjaisista todennuskeinoista käytetään käsitettä token-pohjaiset todennuskeinot, koska siinä tarvitaan todentamiseen jotain välillistä objektia eli ”tokenia”. Biometriset todennusmenetelmät hyödyntävät käyttäjän ominaisuuksia tai kykyjä. Ne voivat liittyä henkilön käyttäytymiseen tai fysiologiseen piirteeseen (Ometov ym., 2018, s. 2). Tulisalo (2020) tarkentaa pro gradu -tutkielmassaan, että biometrisessä tunnisteessa henkilö yksilöidään esimerkiksi sormenjäljen, puheäänen, silmäkuvan, kasvojen tai allekirjoituksen avulla. Nämä biometriset tunnisteet ovat lähes aina yksilöllisiä, mikä tekee niistä hyvän keinon tai osakeinon tunnistautumiseen. (Tulisalo, 2020, s. 11). Lisäksi on olemassa esimerkiksi sijaintiin tai sosiaalisiin verkostoihin liittyviä todentamiskeinoja, mutta kolme yllä mainittua ryhmää ovat tunnetuimmat ja käytetyimmät (Velásquez ym., 2018a), joten tässä tutkielmassa keskitytään niihin.

Tunnistautumistietojen joutuminen vääriin käsiin voi vahingoittaa paitsi yksittäisiä henkilöitä, myös yrityksiä. Kyberturvallisuuskeskuksen (2022b) yrityksille suunnatusta toimintaohjeesta käy ilmi, että tunnusten joutuminen vääriin käsiin johtuu yleisimmin kolmannen osapuolen tietovuodosta, salasanojen uudelleenkäytöstä tai tietojenkalastelusta (Kyberturvallisuuskeskus, 2022b, s. 2). Tietojenkalastelu on Huangin, Man ja Chenin (2011) mukaan vakava uhka käyttäjien luottamuksellisten tietojen turvallisuudelle. Usein tietojenkalasteluhyökkäyksissä ihmisiä huijataan paljastamaan arkaluonteisia tietoja lähettämällä valeviestejä suurelle määrälle käyttäjiä. Jos käyttäjä noudattaa viestin ohjeita, hänet ohjataan yleensä hyvin rakennetuille väärennetyille verkkosivuille ja pyydetään antamaan arkaluonteisia tietoja. Suurin osa tietojenkalasteluhyökkäyksistä pyrkii varastamaan käyttäjien salasanoja ja käyttäjätunnuksia. Kun hyökkääjä saa tunnukset tietoonsa, hän pyrkii niiden avulla saamaan arvokkaampia tietoja vaarantuneilta tileiltä. (Huang ym., 2011). Tietoturvavahingot voivat vaihdella pienistä tappioista koko tietojärjestelmän tuhoutumiseen (Jouini, Rabai & Aissa, 2014).

2.2 Salasanatunnistautumisen puutteet

Aakkosnumeerinen salasana pysyttelee edelleen yleisimpänä todentamiskeinona, vaikka sillä tiedetään olevan useita puutteita (Zimmermann & Gerber, 2020). Meng, Wong, Furnell ja Zhou (2015) ovat jakaneet tietopohjaisten tunnistautumiskeinojen riskit ulkoisiin ja sisäisiin tekijöihin. Ulkoisia tekijöitä ovat esimerkiksi hakkerit ja haittaohjelmat. Ulkoinen riski saattaa toteutua esimerkiksi niin, että hakkeri saa selville käyttäjän salasanan ja pääsee käsiksi arkaluontoisiin tietoihin. Sisäisiin tekijöihin luetaan mukaan muun muassa käyttäjien

tottumukset ja salasanakäyttäytyminen. Tässä tapauksessa heikot salasanat tai salasanojen huono hallinta saattaa vaarantaa tilin ja sen tiedot. (Meng ym., 2015). Huonoa salasanakäyttäytymistä ja salasanojen hallintaa on esimerkiksi se, että salasanoja kirjoitetaan muistilapuille, niitä jaetaan toisille henkilöille tai niitä säilytetään muuten huolimattomasti niin, että salasanat voivat päätyä vääriin käsiin.

Salasanat aiheuttavat kognitiivista kuormitusta etenkin yhden palvelimen ympäristöissä. Ali ja Pal (2017) nostavat artikkelissaan esille, että yhden palvelimen ympäristöissä käyttäjän on tunnistauduttava erikseen kuhunkin palvelimeen, kun taas monipalvelintodennuksessa käyttäjälle riittää yksi kirjautuminen, jonka kautta hän pääsee useisiin palvelimiin. Ongelmana yhden palvelimen ympäristössä on se, että tunnistautuessaan eri palvelimille käyttäjän on myös muistettava useita salasanoja ja käyttäjätunnuksia. Tämä taas saattaa johtaa siihen, että kätevyyden vuoksi käytetään samoja salasana-käyttäjätunnus yhdistelmiä useille eri tileille. (Ali & Pal, 2017). Käyttäjät käyttävät samoja salasanoja uudelleen, jotta he säästäisivät uusien salasanojen luomiseen ja muistamiseen liittyvää vaivaa (Stobert & Biddle, 2018, s. 15). Sen lisäksi kognitiivista kuormitusta pyritään vähentämään luomalla helposti muistettavia salasanoja (Zimmermann, Marky & Renaud, 2022). Helposti muistettavat salasanat ovat kuitenkin yleensä vahvuudeltaan heikkoja ja helposti arvattavia. Tämä helpottaa hakkereiden työtä esimerkiksi salasanojen arvaushyökkäyksissä.

Heikkojen salasanojen luominen ja salasanojen uudelleenkäyttäminen ei Tamin, Glassmanin ja Vandenwauverin (2010) tutkimuksen perusteella kuitenkaan selity pelkästään salasanojen unohtamisen pelolla. Heidän tutkimuksessaan ilmeni, että heikkoon salasanahallintaan vaikutti enemmän mukavuudenhalu kuin huoli salasanojen unohtamisesta. (Tam ym., 2010). Useat henkilöt myös saattavat jakaa salasanansa organisaation sisällä tai jopa sen ulkopuolella olevien kanssa (Tulisalo, 2020, s. 7). Syynä saattaa olla muun muassa se, että työntekijän tietoja tarvitaan tämän ollessa lomalla tai muuten poissa työpaikalta. Työntekijä saattaa tällöin lähettää salasanansa sähköpostin välityksellä tai kirjoittaa tunnukset muistilapulle talteen jollekin työkaverilleen. Tässäkin tapauksessa huonon salasanakäyttäytymisen syynä vaikuttaisi olevan enemmän käytännön syyt ja mukavuuden halu kuin unohtamisen pelko.

Salasanan puutteisiin vaikuttaa myös mahdollinen ristiriitaisuus todellisen turvallisuuden ja käyttäjän kokeman turvallisuuden välillä (Zimmermann ym., 2022). Turvallisuudella tarkoitetaan tässä yhteydessä sellaisten tietojen suojaamista, jotka loukkaavat yksityisyyttä tai joita voitaisiin käyttää petolliseen tarkoitukseen (Tam ym., 2010). Zimmermann ja Gerber (2020) toteavat tutkimuksessaan, että tunnistusjärjestelmien todellinen turvallisuus voi olla käyttäjille vaikea arvioida, koska se on ikään kuin näkymätön osa-alue verrattuna esimerkiksi käytettävyyden arviointiin. Toisaalta Tamin ym. (2010) tutkimuksesta käy ilmi, että käyttäjät tietävät hyvien ja huonojen salasanojen välisen eron sekä huonon salasanakäyttäytymisen seuraukset. Tätä tukee myös Stobertin ja Biddlen (2018, s. 30) havainto siitä, että tavallisten käyttäjien lisäksi useat tietoturva-asiantuntijat käyttävät salasanoja uudelleen tai turvautuvat muihin vähemmän turvallisiin käytäntöihin. Osalla käyttäjistä huono salasanakäyttäytyminen voi johtua

tiedonpuutteesta, mutta isolla osalla se vaikuttaisi liittyvän enemmän mukavuudenhaluun ja käytännöllisyyteen, kuten aiemmin mainittiin Tamin ym. (2010) tutkimukseen liittyen.

Tamin ym. (2010) tutkimuksessa kävi ilmi, että tutkimukseen osallistuneet henkilöt olivat enemmän huolissaan yksityisyydensuojaan liittyvistä asioista kuin tietoturva-ammattilaisten nimeämistä riskeistä. Haastatellut olivat eniten huolissaan yksityisten tietojen paljastumisesta tuttaville tai työtovereille. Sen sijaan muun muassa petoksista ja identiteettivarkauksista haastatellut eivät olleet niin huolissaan, vaikka he ymmärsivätkin niihin liittyvät riskit. (Tam ym., 2010). Tutkimukseen osallistuneet henkilöt olivat enemmän huolissaan yksityisyyden suojaan kuin turvallisuuteen liittyvistä asioista, mikä voi johtua esimerkiksi siitä, että he kokevat yksityisyyteen liittyvät asiat konkreettisempina omalta kannaltaan.

Edellä mainittujen haasteiden lisäksi Limbasiya ym. (2018) mainitsevat, että perustodennusjärjestelmässä palvelimella ylläpidetään salasanataulukkoa, josta palvelin tarkastaa tunnistautumistietojen oikeellisuuden, kun käyttäjä pyrkii kirjautumaan palvelimelle. Tämä muodostaa riskin silloin, jos tunnistautumistiedot on tallennettu palvelimelle selväkielisenä tekstinä. Tällöin hyökkääjän voi olla helpompi varastaa tunnistautumistiedot salasanataulukosta. (Limbasiya ym., 2018).

2.3 Keinot salasanan vahvistamiseksi

Koska salasanat pysyttelevät edelleen suosituimpana tunnistautumiskeinona, on syytä miettiä, miten käyttäjiä voidaan kannustaa parempaan salasanakäyttäytymiseen ja vahvempien salasanojen luomiseen. Aihe on tärkeä myös, jos salasanaa käytetään yhtenä monivaiheisen tunnistautumisen keinona.

Limbasiyan ja Doshin (2017) mukaan käyttäjien valitsemat helpot ja yleiset salasanat altistavat erilaisille arvaushyökkäyksille, minkä vuoksi käyttäjien tulisi sisällyttää salasanoihin erikoismerkkejä, numeroita sekä pieniä ja isoja kirjaimia. Yleisten sanojen tai henkilötietojen käyttöä salasanana tulisi välttää, koska ne on helppo saada selville. (Limbasiya & Doshi, 2017). Zimmermannin ym. (2022) mukaan yksi keino edellä kuvaillun kaltaisiin vahvempiin salasanoihin on salasanamittarit, jotka antavat salasanaa luodessa palautetta sen vahvuudesta. Heidän tutkimuksessaan selvitettiin salasanamittareiden tuloksena syntyneiden salasanojen eroja. Salasanamittarit saattavat antaa vahvuuden lisäksi myös ohjeita, miten salasanasta saisi vahvemman. Tutkimuksessa kävi ilmi, että sellaiset salasanamittarit, jotka antavat sekä palautetta vahvuudesta että lisäohjeita, olivat melko tehokkaita parantamaan salasanojen vahvuutta. Salasanamittareiden avulla käyttäjät voidaan ohjata luomaan turvallisempia salasanoja. (Zimmermann ym., 2022).

Salasanamittareiden lisäksi Zimmermann ym. (2022) toteavat, että salasanojen turvallisuutta voi parantaa järjestelmän valmiiksi luomat salasanat tai salasanojen säännöllinen uusiminen. He lisäävät kuitenkin, että näihin keinoihin

liittyy inhimillisiä tekijöitä, jotka heikentävät tehokkuutta. Järjestelmien luomat salasanat ovat usein hankalia muistaa, jolloin käyttäjät kirjoittavat ne ylös ainakin aluksi. Salasanojen säännöllinen uusiminen taas voi turhauttaa käyttäjiä, jolloin samasta salasanasta luodaan erilaisia variaatioita, jotka on helppo muistaa ja toisaalta myös arvata. (Zimmermann ym., 2022).

Tam ym. (2010) ehdottavat turvallisuuden parantamiseksi myös kertakirjautumisratkaisua kertakäyttöisen salasanan avulla. Kertakäyttöinen salasana toimii siten, että käyttäjän syöttäessä käyttäjätunnuksensa luodaan kirjautumista varten jokin satunnainen koodi, jonka voi käyttää vain kerran (Velasquez ym. 2018b). Koodi lähetetään käyttäjälle sähköpostiin tai tekstiviestillä ja se on käytössä rajatun ajan, jonka sisällä kirjautuminen tulee tehdä tai muuten pitää pyytää uusi koodi.

Sisäiset työntekijät vaikuttaisivat muodostavan suurimman uhkan yrityksen tietoturvalle, mikä johtaa tarpeeseen lisätä tietoturvakoulutusta ja tietoisuutta työntekijöiden keskuudessa (Keller ym., 2005). Myös Tulisalo (2020) ja Kyberturvallisuuskeskus (2022b) kannustavat organisaatioita kouluttamaan henkilöstöään ja pitämään salasanakäytännöt ajan tasalla riskien minimoimiseksi. Tam ym. (2010) eivät kuitenkaan tue ajatusta, että pelkkä käyttäjien valistaminen salasananhallinnan tärkeydestä kannustaisi heitä toimimaan paremmin, koska lopulta mukavuudenhalu ja helppous ohjaavat käyttäjien toimintaa enemmän kuin järkisyyt. Tamin ym. (2010) sekä Stobertin ja Biddlen (2018) tutkimuksien mukaan käyttäjät ovat valmiita tinkimään mukavuudesta ja panostamaan enemmän salasananhallintaan, jos he kokevat käytettävän tilin tai järjestelmän tärkeäksi. Esimerkiksi pankkitiliin liittyviä kirjautumistietoja hallitaan huolellisemmin kuin sähköpostin tunnuksia, koska pankkitilin vaarantumisesta saattaa aiheutua käyttäjälle suuria henkilökohtaisia tappioita. Tamin ym. (2010) mukaan yritysten tulisi tehdä käyttäjät tietoisiksi huonon salasanakäyttäytymisen seurauksista ja tuoda esille, mitä järjestelmän vaarantumisesta voi aiheutua. Lisäksi käyttäjät tulisi pitää ajan tasalla tietoturvaongelmista ja esimerkiksi hakkerointiyrityksistä. (Tam ym., 2010). Pitämällä käyttäjät tietoisina todellisista tietoturvaongelmista tietoturvallisuus pysyy myös konkreettisena. Tietoturvakoulutusta voidaan tarjota etenkin sellaisille henkilöille, joille aihe ei ole niin tuttu. Myös uusille työntekijöille olisi hyvä käydä läpi yrityksen tietoturvakäytänteet perehdytyksen yhteydessä.

3 MONIVAIHEINEN TUNNISTAUTUMINEN

Yksivaiheista tunnistautumista kohtaan ilmenneiden tietoturvahyökkäysten vuoksi on alettu enenevissä määrin tutkia monivaiheista tunnistautumista turvallisuuden lisäämiseksi (Khan, Ali Akbar, Shahzad, Farooq & Khan, 2015). Limbasiya ja Doshi (2017) nostavat esille, että informaatioteknologian ja tietotekniikan käyttö on laajentunut paljon viime vuosikymmenien aikana ja säilytämme paljon tärkeää tietoa erilaisissa sähköisissä järjestelmissä. Tallennetuille tiedoille olisi tärkeää tarjota riittävä tietoturva, minkä vuoksi olisi suositeltavaa ottaa käyttöön vahva todennusjärjestelmä. (Limbasiya & Doshi, 2017). Suojaamattomien tunnistetietojen paljastuminen on suuri riski verkossa oleville yrityksille (Khan ym., 2015).

Ometovin ym. (2018) mukaan kaksivaiheinen tunnistautuminen eli 2FA (engl. Two-Factor Authentication) on yksivaiheista tunnistautumista asteen turvallisempi. Siinä tunnistautumiseen tarvitaan kaksi tekijää eri todennusryhmistä. Kaksivaiheisessa tunnistautumisessa voidaan esimerkiksi yhdistää perinteinen tietopohjainen käyttäjätunnus-salasana yhdistelmä jonkin omistuspohjaisen, kuten älykortin, kanssa. Monivaiheinen tunnistautuminen eli MFA (engl. Multi-Factor Authentication) tarjoaa kaikista korkeimman suojan. Siinä henkilöllisyyden tunnistaminen perustuu vähintään kahteen tai useampaan eri tekijään eri ryhmistä. (Ometov ym., 2018, s. 2) Tässä tutkielmassa käytetään yleisesti termiä monivaiheinen tunnistautuminen, kun todentamiskeinoja on kaksi tai enemmän. Selvyyden vuoksi ei käytetä termiä kaksivaiheinen tunnistautuminen, koska monivaiheinen tunnistautuminen pitää myös sen sisällään.

Kahden tai useamman tunnistautumiskeinon käyttäminen lisää turvallisuutta (Ometov ym., 2018, s. 19) ja kiinnostus monivaiheista tunnistautumista kohtaan onkin kasvanut (Velásquez ym., 2018a). Tekstisalasanojen ja älykorttien käyttö on selvästi yleistynyt monivaiheisen tunnistautumisen keinona (Velásquez ym., 2018a). Toisaalta biometriset tunnistautumiskeinot ovat olleet suosittuja käyttäjien keskuudessa (Zimmermann & Gerber, 2020). Salasana näyttäisi olevan yleisin monivaiheisen tunnistautumisen osakeino (Tulisalo, 2020, s. 7), joten näiden tietojen perusteella tässä tutkielmassa tarkastellaan

monivaiheisen tunnistautumisen vaihtoehtoja, joissa salasana on yhdistetty älykorttiin tai biometriseen tunnistautumiskeinoon.

Turvallisuuden ja käytettävyyden välinen kompromissi on kriittinen tekijä tunnistusjärjestelmän toimivuuden kannalta (Ometov ym., 2018, s. 4), mutta näiden tasapaino on ollut yleensä hankala saavuttaa (Zimmermann & Gerber, 2020). Turvallisuuden asiantuntijat vaikuttavat keskittyvän enemmän turvallisuuteen kuin käytettävyyteen ja käytettävyyden asiantuntijat taas suhtautuvat liian optimistisesti turvallisuuteen (Bonneau, Herley, van Oorschor & Stajano, 2012, s. 553). Mengin ym. (2015) mukaan tunnistusjärjestelmän huono käytettävyys voi heikentää turvallisuustasoa, kun taas heikko turvallisuus voi suoraan vahingoittaa käyttäjiä ja yrityksiä. Huono käytettävyys johtaa ennen pitkää aiemmissa luvuissa käsiteltyihin ongelmiin salasanojen ja muiden todennuskeinojen huonosta hallinnasta. Käyttäjät tavoittelevat vaivattomampaa ja helpompaa käytettävyyttä, mikä saatetaan tehdä turvallisuuden kustannuksella.

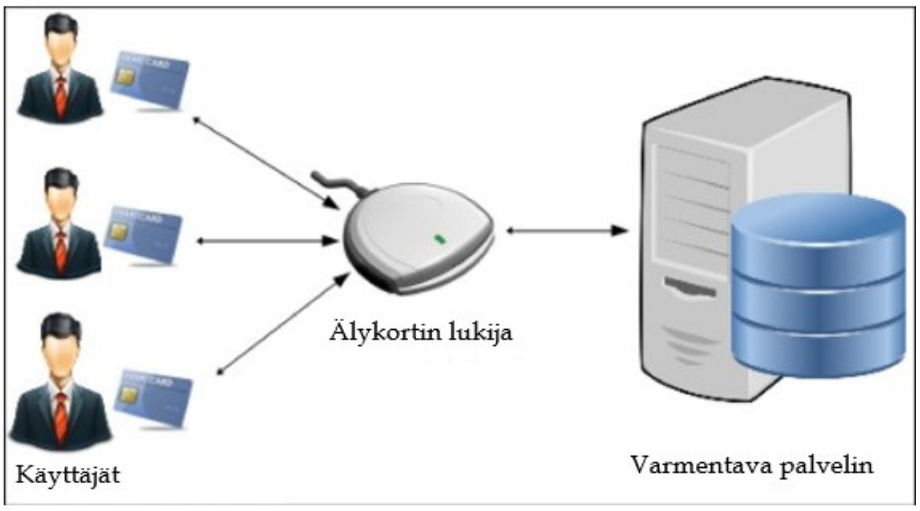
Tässä luvussa lukijalle avataan omistuspohjaisten ja biometristen todennusmenetelmien teoriaa ja käyttöä monivaiheisen tunnistautumisen osakeinona. Lisäksi pohditaan näiden menetelmien puutteita, sillä niiden huomioiminen on avainasemassa, kun halutaan parantaa turvallisuutta (Wang ym., 2020).

3.1 Omistuspohjaiset menetelmät

Omistuspohjaisissa todennusmenetelmissä tunnistautumiseen käytetään jotain fyysistä apuvälinettä kuten älykorttia tai älypuhelinta. Esimerkiksi älypuhelimessa toimiva mobiiliautentikaattori toimii siten, että salasanan kirjoittamisen lisäksi käyttäjän tulee vahvistaa tunnistautuminen älypuhelimeen tulevan vahvisteen avulla (Tulisalo, 2020, s. 12). Vahvistepyyntö voi tulla esimerkiksi puhelimeen asennetun erillisen sovelluksen kautta (Velásquez ym., 2018b). Tällaisia tunnettuja sovelluksia ovat esimerkiksi Microsoft Authenticator ja Google Authenticator. Tässä tutkielmassa keskitytään kuitenkin enimmäkseen älykorttipohjaiseen todentamiseen, koska se on kerätyn aineiston pohjalta tutkituin omistuspohjainen todennusmenetelmä.

Älykortti on yleensä pankkikortin kokoinen muovinen kortti, johon on upotettu todennustietoja sisältävä siru (Velásquez ym., 2018b). Älykortista voidaan käyttää myös termiä toimikortti tai sirukortti. Käytännössä monivaiheinen älykorttipohjainen tunnistautuminen toimii siten, että käyttäjän on asetettava älykortti lukulaitteeseen ja näppäiltävä sen jälkeen salasana (Jiang, Ma, Li & Li, 2015). Älykorttipohjaiseen todennusjärjestelmään kuuluu rekisteröintivaihe, kirjautumisvaihe ja varmennusvaihe (Wang, Wang, Xu & Guo, 2017). Rekisteröintivaiheessa kullekin käyttäjälle annetaan yksilöidyllä tunnisteella ja salasanalla varustettu älykortti (Yang, Wong, Wang & Deng, 2008). Kun rekisteröitynyt käyttäjä haluaa päästä järjestelmään, kirjautumisvaiheessa lähetetään palvelimelle käyttöoikeuspyyntö. Tämän jälkeen varmennusvaiheessa palvelin tarkistaa, että todentamistiedot täsmäävät tietokantaan tallennettuihin tietoihin. Jos tiedot vastaavat toisiaan, todennusprosessi on onnistunut ja käyttäjä pääsee kirjautumaan

sisään järjestelmään. (Wang ym., 2017). Kuviossa 1 on havainnollistettu älykortin toiminta. Monivaiheisessa tunnistautumisessa järjestelmä vaatii käyttäjältä vielä oikean salasanan, jonka jälkeen hän pääsee käyttämään järjestelmän resursseja. Älykortin tulee olla koko istunnon ajan lukijassa ja käyttäjä kirjataan automaattisesti ulos, jos kortti otetaan lukijasta pois.



KUVIO 1 Älykortin toiminta (Limbasiya ym., 2018 mukaan)

Älykortit ovat vahva todentamiskeino, koska ne on suojattu sekä fyysisesti että loogisesti (Bouchaala, Ghazel & Saidane, 2022). Käyttäjällä on oltava hallussaan fyysinen kortti sekä tiedossaan oleva salasana, jotta hän voi päästä palvelimelle (Yang ym., 2008, s. 1160). Todentamiseen käytettävän apuvälineen katoaminen tai varastaminen vaikuttaisi olevan todennäköisin riski, mikä liittyy omistuspohjaisiin menetelmiin. Käytännössä hyökkääjä voi varastaa älykortin ja poimia siihen tallennetut tiedot (Yang ym., 2008, s. 1161). Älykortin saamisen jälkeen hyökkääjä voi suorittaa salasanan arvaushyökkäyksen, jolla pyritään saamaan kortin salasana selville (Limbasiya & Doshi, 2017). Kortin puuttuminen on kuitenkin helpompi huomata verrattuna esimerkiksi salasanojen ja käyttäjätunnusten vuotamiseen, mikä mahdollistaa nopeamman reagoinnin. Hyökkääjän tulisi saada ensin haltuunsa älykortti ja sen jälkeen murtaa vielä siihen liitetty salasana (Tulisalo, 2020, s. 12). Siihen mennessä käyttäjä on saattanut jo huomata kortin katoamisen ja tehnyt tarvittavat ilmoitukset ja toimenpiteet yrityksen käytäntöjen mukaisesti. Kortin katoaminen tai rikkoutuminen saattaa olla piinallinen prosessi, jos siihen ei ole varauduttu yrityksessä millään tavalla (Tulisalo, 2020, s. 38). Yrityksillä tulisikin olla etukäteen sovittuna selkeät toimintatavat ja menetelmät tällaisten tilanteiden varalle.

Wangin ym. (2020) mukaan älykorttipohjainen todennusmenetelmä on suositeltavaa etenkin monipalvelinympäristöissä, joissa käyttäjä voisi kirjautua mihin tahansa palvelimelle käyttämällä älykorttia ja salasanaa. Tällaisessa ympäristössä palvelimen ei tarvitse välttämättä ylläpitää taulukkoa, jossa on salasanaan liittyviä tarkistustietoja, jolloin palvelimelle ei myöskään aiheudu uhkaa

salasanatietokannan vuotamisesta tai suuren salasanatietokannan ylläpitämisestä. (Wang ym., 2020).

3.2 Biometriset menetelmät

Biometrisessa tunnistusjärjestelmässä käyttäjä tunnistetaan jonkin käyttäjän henkilökohtaisen ominaisuuden perusteella. Mengin ym. (2015) mukaan biometriset tunnistusmenetelmät voidaan yleisesti jakaa fysiologisiin ja käyttäytymiseen perustuviin keinoihin. Fysiologisissa keinoissa hyödynnetään käyttäjän fyysisiä ominaisuuksia kuten sormenjälkeä, kasvojen tunnistusta tai iiristunnistusta. Fysiologisen biometriikan etuna on se, että piirteet ovat yleensä ainutlaatuisia ja yksilöllisiä. Käyttäytymiseen perustuvassa biometriassa taas käytetään tunnistautumiseen käyttäjän toimintaa kuten äänen- tai allekirjoituksen tunnistusta. (Meng ym., 2015). Tässä tutkielmassa keskitytään tarkastelemaan fysiologisia keinoja ja erityisesti sormenjälki- ja kasvojentunnistusta, koska fysiologinen biometria tarjoaa yleisesti suuremman todennustarkkuuden kuin käyttäytymiseen perustuvat keinot (Meng ym., 2015).

Biometriikan eduiksi on todettu muun muassa sen turvallisuus ja pysyvyys sekä vaikeus kadottaa, unohtaa ja murtaa (Limbasiya & Doshi, 2017). Sormenjälkitunnistus on laajimmin käytetty biometrinen tunnistuskeino ja sitä käytetäänkin paljon esimerkiksi älypuhelimissa (Ometov ym., 2018, s. 4) Sormenjälkitunnistus tarjoaa melko korkean todennustarkkuuden ja se on useimmiten helppokäyttöinen (Meng ym., 2015), mutta siihen liittyy myös erilaisia puutteita.

Olosuhteet näyttäisivät vaikuttavan sormenjälkitunnistautumiseen onnistumiseen. Esimerkiksi viillot, lika ja kuluminen sormenpäissä saattavat vaikuttaa sormenjäljen kuvioon ja siten vaikeuttaa tunnistamista (Meng ym., 2015). Myös esimerkiksi sormien kylmyys saattaa haitata tunnistamista. Zimmermannin ja Gerberin (2020) tutkimuksessa käyttäjät arvioivat sormenjälkitunnistuksen turvallisimmaksi todennuskeinoksi ja käytettävyydeltään toiseksi parhaimmaksi keinoksi heti salasanatunnistautumisen jälkeen. Useat tutkimukseen osallistuneet myös pitivät sormenjälkeä mahdottomana varastaa tai väärentää, vaikka niin ei todellisuudessa ole. (Zimmermann & Gerber, 2020). Sormenjälki on melko helppo väärentää, minkä vuoksi sitä ei suositella käytettäväksi ainoana todentamiskeinona (Ometov ym., 2018, s. 4–10).

Toinen tutkielmassa tarkasteltava biometriikan keino on kasvojen tunnistus. Kasvojen tunnistuksessa henkilö tunnistetaan ja todennetaan digitaalisesta kuvasta tai videokuvasta kasvonpiirteiden avulla (Meng ym., 2015). Sormenjäljen tavoin olosuhteet vaikuttavat myös kasvojen tunnistuksen onnistumiseen. Mengin ym. (2015) havaintojen mukaan kasvojen tunnistus ei välttämättä toimi huonossa valaistuksessa tai aurinkolasien, hiusten tai muiden kasvot osittain peittävien objektien kanssa. Sormenjäljen tavoin kasvojentunnistus on herkkä väärennöshyökkäyksille. Väärennettyjä kasvoja voidaan melko tehokkaasti ja helposti hankkia esimerkiksi valokuvista ja hyödyntää niitä huijaamaan kasvojentunnistusjärjestelmää. (Meng ym., 2015).

Ometov ym. (2018, s. 9) mainitsevat, että edellä mainittujen puutteiden lisäksi biometristen todennuskeinojen käyttö saattaa olla hankalaa erityisesti vammautuneille tai ikääntyneille henkilöille. Uudemmassa tutkimuksessa Furnell, Helkala ja Woods (2022) kuitenkin toisaalta pitävät fysiologista biometriikkaa melko hyvin soveltuvana myös vammautuneille henkilöille. Heidän mukaansa etenkin fysiologinen biometriikka on yleisesti hyvä keino parantamaan todennusjärjestelmän helppokäyttöisyyttä. Lisäksi he huomauttavat, että kaikkien todennusvaihtoehtojen kohdalla voidaan kritisoida ja väitellä siitä, soveltuvatko ne jollekin tietylle käyttäjäryhmälle. Käyttäjille tulisi tarjota yksilöllisiä vaihtoehtoja heille parhaiten soveltuvista todennuskeinoista. (Furnell, Helkala & Woods, 2022). Yritysmaailmassa voi kuitenkin olla haastavaa ja kallista lähteä tarjoamaan jokaiselle työntekijälle yksilöityjä todennuskeinoja. Koska biometristen todennuskeinojen esteettömyys vaikuttaa olevan kiistelty aihe, siitä tarvittaisi lisätutkimuksia.

Biometristen todennuskeinojen turvallisuus on jossain määrin edelleen avoin tutkimusongelma (Khan ym., 2015), mutta biometriikka on kuitenkin tärkeä osa monivaiheisen tunnistautumisen tulevaisuutta (Ometov ym., 2018, s. 19). Todennustarkkuuden ja turvallisuuden lisäämiseksi suositellaan, että biometriikkaa käytettäisi yhdessä jonkin muun todennuskeinon kanssa (Meng ym., 2015). Koska biometriset keinot on todettu helpoiksi väärentää, mutta ne ovat kuitenkin käytettävyydeltään yleisesti melko helppoja, niitä tulisi harkita monivaiheisen tunnistautumisen osakeinona. Biometriikan yhdistäminen salasanan kanssa lisäisi turvallisuutta ja vähentäisi riskiä sille, että järjestelmiin pääsisi käsiksi joku ulkopuolinen pelkällä väärennöshyökkäyksellä. Hyökkääjän tulisi sekä onnistua väärentämään biometriikkaa, että murtaa siihen liitetty salasana.

4 ANALYSOINTI JA VERTAILU

Tässä luvussa tehdään analysointia ja vertailua aiemmin käsitellyistä monivaiheisen tunnistautumisen vaihtoehdoista. Lisäksi käsitellään lyhyesti, mitä muita asioita yritysten tulisi ottaa huomioon tietoturvan osalta.

Aiemman perusteella voidaan todeta, että kaikissa todennusmenetelmissä on hyviä ja huonoja puolia. Jotta käyttöön saataisiin mahdollisimman toimiva todennusmenetelmä, on valinnassa otettava huomioon sekä turvallisuus- että käytettävyysnäkökulma. Yhdistelemällä tunnistuskeinoja ja luomalla monivaiheisen tunnistautumisen menetelmiä meillä on hyvät mahdollisuudet kehittää turvallisia ja käyttäjäystävällisiä vaihtoehtoja (Furnell, Helkala & Woods, 2022).

Älykorttipohjainen todennusjärjestelmä vaikuttaisi olevan yksi yleisimmistä ja kätevimmistä menetelmistä (Wang ym., 2017). Suurimmaksi riskiksi tunnistettiin älykortin katoaminen tai varastaminen, minkä vuoksi olisi erityisen tärkeää varmistaa järjestelmien turvallisuus myös tällaisissa uhkatilanteissa (Jiang ym., 2015). Älykorttipohjaisen todennusmenetelmän turvallisuus edellyttää, että käyttäjät pitävät huolta älykortista ja toimivat lisäksi tietoturvakäytäntöjen mukaisesti (Limbasiya & Doshi, 2017). Tähän liittyy esimerkiksi salasanan turvallinen hallinta. Älykortin kadotessa huomio kiinnittyy siihen liitettyyn salasanaan ja sen turvallisuuteen. Salasanan tulisi olla vahva ja hyvin suojattu, jotta se pysyy turvassa myös silloin, kun älykortti katoaa (Yang ym., 2008, s. 1161). Erityisen riskin järjestelmälle voisi aiheuttaa esimerkiksi se, jos käyttäjä on kirjoittanut älykorttiin liitetyn salasanan talteen muistilapulle ja kiinnittänyt muistilapun älykorttiin. Tällöin älykortin haltuunsa saava henkilö, joko organisaation sisältä tai sen ulkoa, pääsisi helposti kirjautumaan järjestelmiin ja voisi päästä käsiksi tietoihin, jotka eivät hänelle kuulu.

Toisena potentiaalisena monivaiheisen tunnistautumisen menetelmänä tarkasteltiin biometrian ja salasanan yhdistelmää. Biometrinen todennus vaikuttaa lupaavalta, mutta sen suurimpia puutteita ovat edelleen tarkkuus ja nopeus (Meng ym., 2015). Älykorttiin verrattuna olosuhteilla on paljon suurempi vaikutus biometrisen todennuksen onnistumiseen. Älykortti saattaisi olla jossain määrin vakaampi todennuskeino, koska siihen ei vaikuta esimerkiksi lämpötila tai valaistus. Toisaalta älykortin sirun kuluminen tai siihen tulleet naarmut saattavat

heikentää todennuksen onnistumista samalla tavalla kuin sormen viillot vaikeuttavat sormenjälkitodennusta. Älykortti on todennäköisesti kuitenkin biometriaa helpompi vaihtaa uuteen tietyin aikavälein tai tarvittaessa, kun kulumista havaitaan. Biometriikan etu älykorttiin verrattuna on se, ettei sitä voi varastaa tai kadottaa. Huonona puolena todetaan, että se on kuitenkin kohtalaisen helppo väärentää.

Salasanaa voidaan edelleen tietyin ehdoin pitää pätevänä monivaiheisen tunnistautumisen osakeinona etenkin, kun se on käyttäjien keskuudessa suosittu käytettävyyden ja mieltymysten osalta (Zimmermann & Gerber, 2020). Salasanan turvalliseen hallintaan ja käyttöön liittyviä ehtoja käsiteltiin tarkemmin luvussa 2.3. On todella tärkeää, että salasana on turvallinen ja riittävän vahva myös silloin, kun sitä käytetään monivaiheisen tunnistautumisen osakeinona. Yksi vaihtoehto voisi olla kertakäyttöiset salasanat, joita tarkasteltiin luvussa 2.3. Kertakäyttöisen salasanan yhdistäminen biometriaan tai älykorttiin vähentäisi niin sanottuun pysyvään salasanaan liittyviä riskejä. Aiheesta ei kuitenkaan löydy vielä tutkimuksia ja esimerkiksi sen teknistä toteutusta pitäisi selvittää, jotta voidaan todeta, olisiko ratkaisu käyttökelpoinen.

Yrityksellä on iso rooli monivaiheisen tunnistautumisen käyttöönotossa ja sen edistäjänä (Tulisalo, 2020, s. 43). Turvallisuutta pohtiessa ei voida unohtaa inhimillisiä tekijöitä, sillä teknologian valtavasta kehityksestä huolimatta ihminen on edelleen tietoturvan heikoin lenkki (Tam ym., 2010). Ilman monivaiheista tunnistautumista yrityksen tietoturva on pahimmillaan heikoimman salasanan ja salasanakäyttäytyjän varassa (Tulisalo, 2020, s. 38). Soomro, Shah ja Ahmed (2016) nostavat artikkelissaan esille yrityksen johdon roolia tietoturvan hallinnassa. Heidän mukaansa lukuisilla johdon toimilla, kuten esimerkiksi tietoturvapolitiikan kehittämisellä ja toteuttamisella sekä tietoisuuden lisäämisellä on merkittävä vaikutus tietoturvallisuuden hallinnan laatuun. Aiemmin tietotekniikan ammattilaisten on katsottu olevan vastuussa tietoturvasta, mutta nykyään vastuuta on alettu siirtää enemmän yrityksen johdolle. (Soomro ym., 2016). Käytännössä tietoturvasta huolehtiminen kuuluu jokaisen yksittäisen työntekijän vastuulle ja heidän tulisi omalla toiminnallaan huolehtia esimerkiksi kirjautumistunnusten turvallisesta hallinnasta. Organisaatioita kehotetaan omaksumaan kokonaisvaltaisempi lähestymistapa tietoturvan hallintaan muun muassa yrityksen johdon osallistumisen, tietoturvapolitiikan kehittämisen ja toteuttamisen sekä tietoturvatietoisuuden ja -koulutuksen keinoilla (Soomro ym., 2016). Yrityksen johdolla on merkittävä rooli esimerkiksi monivaiheisen tunnistautumisen käyttöönotossa. Monivaiheisen tunnistautumisen käyttöönotto voikin olla yritykselle helpompi ja tehokkaampi keino parantaa tietoturvaa verrattuna siihen, että keskityttäisi noudattamaan tiukkaa salasanapolitiikkaa (Tulisalo, 2020, s. 47).

Yrityksillä tulisi olla jonkinlainen suunnitelma ja toimintaohje siltä varalta, että työntekijän tunnistautumisväline vuotaa tai katoaa. Kellerin ym. (2005, s. 17) tutkimuksen mukaan 16,7 prosentilla pienyrityksistä ei ollut hätätoimintasuunnitelmaa tietoturvauhkien varalle ja kolmanneksella tutkimukseen osallistuneista yrityksistä oli hätätoimintasuunnitelma, mutta se oli riittämätön. Lisäksi ulkoisten tietoturvaloukkausten riskiä pidettiin yrityksissä suhteellisen pienenä.

(Keller ym., 2005, s. 17). Huomioitavaa kuitenkin on, että kyseinen tutkimus on vuodelta 2005 eikä vertailuarvoja tältä vuosikymmeneltä löytynyt. Todennäköisesti nykyään yrityksissä ymmärretään ja tunnistetaan paremmin myös ulkoisten tietoturvauhkien riskit.

Läpikäydyn aineiston ja sen analysoinnin perusteella älykortin ja salasanan yhdistelmä vaikuttaisi olevan tällä hetkellä yleisesti potentiaalisin monivaiheisen tunnistautumisen keino. Biometriaan liittyy enemmän epävarmuustekijöitä ja sen todennus- ja toimintavarmuus on edelleen heikompi kuin älykortin. Luultavasti biometriset keinot tulevat kuitenkin kehittymään tulevaisuudessa ja esimerkiksi käyttäytymiseen perustuvaa biometriikkaa aletaan käyttää kehityksen myötä laajemmin (Ometov ym., 2018, s. 19). Kullekin yritykselle sopivin todennusmenetelmä riippuu kuitenkin aina esimerkiksi kontekstista ja kustannuksista, joita ei tässä tutkielmassa käsitelty. Todennusmenetelmästä riippumatta yritysten on panostettava myös tietoturvallisuuden hallintaan ja työntekijöiden valistamiseen tietoturvan tärkeydestä. Työntekijöillä tulisi olla tiedossa, kuinka tunnistautumiseen käytettäviä tietoja hallitaan turvallisesti, ja heidän tulisi olla myös tiedostaa, mitä konkreettisia riskejä tietojen vuotamisesta voi seurata.

5 YHTEENVETO

Informaatioteknologian kehittyminen on lisännyt mahdollisuuksia, mutta samaan aikaan siihen liittyvät riskit ovat kasvussa. Yrityksillä on järjestelmissään paljon tärkeää tietoa, joka halutaan pitää suojassa ulkopuolisilta. Tämän vuoksi käyttäjät on tärkeää todentaa ennen kuin he pääsevät käsiksi järjestelmän tietoihin. Yleisimmin todentaminen on tapahtunut yksivaiheisen tunnistautumisen kautta eli salasanan ja käyttäjätunnuksen avulla. Sen on kuitenkin huomattu olevan riittämätön nykypäivän uhkia vastaan. Turvallisuuden lisäämiseksi yrityksille suositellaan monivaiheisen tunnistautumisen käyttöönottoa.

Tutkielman tavoitteena oli löytää yritysten näkökulmasta parhaat monivaiheisen tunnistautumisen keinot huomioiden sekä turvallisuuden, että käytettävyyden. Tutkimuskysymykset olivat seuraavat:

- Miksi salasanat luovat tietoturvahaasteita yrityksille?
- Mitkä monivaiheisen tunnistautumisen keinot voisivat olla yrityksille potentiaalisimmat?

Tutkielma toteutettiin systemaattisena kirjallisuuskatsauksena. Lähteinä käytettiin pääasiassa vertaisarvioituja tieteellisiä artikkeleita, joille Julkaisufoorumi on antanut luokituksen 1–3. Aineistoa on etsitty pääasiassa Jyväskylän yliopiston kirjaston JYKDOK-tietokannasta sekä Google Scholar hakupalvelun kautta. Artikkeleita on arvioitu kriittisesti vertaisarvioinnin ja JUFO-luokituksen lisäksi myös niiden julkaisuvuoden perusteella. Tutkielmassa on pyritty käyttämään enimmäkseen sellaista aineistoa, joka on julkaistu vuonna 2015 tai jälkeen. Mukana on myös joitakin vanhempia artikkeleita, jotka ovat tutkielman kannalta relevantteja.

Tutkielman aihetta on rajattu jonkin verran. Yksivaiheisen tunnistautumisen osalta on keskitytty tietopohjaiseen salasana-käyttäjätunnus yhdistelmään. Omistuspohjaisista todennusmenetelmistä on tarkasteltu älykorttia ja biometriikan puolelta sormenjälkeä ja kasvojen tunnistusta.

Salasanojen suurimmiksi haasteiksi tunnistettiin niiden luoma kognitiivinen kuormitus käyttäjälle sekä heikko salasananhallinta. Vahvat ja turvalliset salasanat saattavat olla hankalia muistaa, minkä vuoksi käyttäjät kirjoittavat niitä ylös muistilapuille tai pyrkivät tekemään salasanoista helpommin muistettavia. Helpot salasanat ovat usein myös turvallisuudeltaan heikompia, koska ne ovat helpompia arvata ja saada selville. Lisäksi työntekijät saattavat jakaa salasanansa työkaverille esimerkiksi loman tai muun poissaolon vuoksi. Mielenkiintoinen havainto oli se, että käyttäjien salasanakäyttäytymistä vaikuttaisi ohjaavan enemmän mukavuudenhalu ja käytännön syyt kuin tietoturvallisuuden ja sen riskien tiedostaminen.

Salasanojen vahvistamiseksi ehdotettiin muun muassa salasanamittareita. Lisäksi työntekijöiden tietoturvakoulutus tulisi pitää ajan tasalla ja kertoa avoimesti esimerkiksi yritykseen kohdistuneista hakkerointiyrityksistä. Turvalliseen todennusmenetelmien hallintaan vaikutti se, jos työntekijät ymmärsivät konkreettiset riskit, joita tietoturvan rikkoutumisesta voi aiheutua.

Tutkielman perusteella potentiaalisimpia monivaiheisen tunnistautumisen keinoja vaikuttaisivat olevan älykortin ja salasanan sekä biometrian ja salasanan yhdistelmät. Älykortti saattaa olla ehkä vielä biometriaa toimivampi keino, koska se ei ole niin herkkä olosuhteille. Esimerkiksi lämpötilan, valaistuksen ja viiltojen havaittiin heikentävän biometristen keinojen todennusvarmuutta. Älykortin todennäköisimmäksi riskiksi tunnistettiin sen katoaminen. Toisaalta todettiin, että älykortin katoaminen huomataan todennäköisesti helpommin kuin biometrian väärennös tai salasanan vuotaminen. Tutkielma ei kuitenkaan tarjoa yrityksille suoraa ratkaisua, koska siinä ei ole otettu huomioon yrityksen tilannetta, todennusmenetelmien kustannuksia tai teknistä toteutusta. Lisäksi tutkielma on melko rajattu eikä sisällä esimerkiksi empiiristä tutkimusta. Sopivien todennusmenetelmien valitseminen on yrityskohtaista, mutta monivaiheisen tunnistautumisen käyttöönotto on kuitenkin suositeltavaa yrityksestä riippumatta.

Jatkotutkimusaiheina voisi olla esimerkiksi empiirisen tutkimuksen toteuttaminen älykortin ja salasanan sekä biometrian ja salasanan toimivuudesta käytännössä. Tässä tutkielmassa oli rajattu pois edellä mainittujen ratkaisujen kustannukset ja tekninen toteutustapa, joten ne voisivat olla hyviä tutkimuskohteita jatkon kannalta. Lisäksi tutkimusaiheena voisi olla älykortin ja biometrian yhdistäminen monivaiheiseksi todennuskeinoksi. Mielenkiintoisia jatkotutkimusaiheita voisivat olla myös mobiiliautentikaattorin käyttö monivaiheisessa tunnistautumisessa sekä turvallinen tunnistautuminen etätyöympäristössä. Yksi tärkeä näkökulma olisi myös saavutettavuus eli vammaisten tai muuten toimintakyvyltään rajoittuneiden ihmisten keinot tunnistautumiseen.

LÄHTEET

Ali, R., & Pal, A. K. (2018). An efficient three factor–based authentication scheme in multiserver environment using ECC. *International Journal of Communication Systems*, *31*(4), 1-22. https://doi.org/10.1002/dac.3484

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

Bouchaala, M., Ghazel, C., & Saidane, L. A. (2022). Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card. *The Journal of Supercomputing*, *78*(1), 497–522. https://doi.org/10.1007/s11227-021-03857-7

Furnell, S., Helkala, K., & Woods, N. (2022). Accessible authentication: Assessing the applicability for users with disabilities. *Computers & security, 113*, 102561. https://doi.org/10.1016/j.cose.2021.102561

Huang, C.-Y., Ma, S.-P., & Chen, K.-T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications*, *34*(4), 1292–1301. https://doi.org/10.1016/j.jnca.2011.02.004

Jiang, Q., Ma, J., Li, G., & Li, X. (2015). Improvement of robust smart-card-based password authentication scheme. *International Journal of Communication Systems*, *28*(2), 383–393. https://doi.org/10.1002/dac.2644

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia computer science, 32*, 489-496. https://doi.org/10.1016/j.procs.2014.05.452

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security Threats and Practices in Small Businesses. *Information Systems Management*, *22*(2), 7–19. https://doi.org/10.1201/1078/45099.22.2.20050301/87273.2

Khan, S. H., Ali Akbar, M., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, *48*(2), 458–472. https://doi.org/10.1016/j.patcog.2014.08.024

Kyberturvallisuuskeskus. (2022a, 17. marraskuuta). *Ohjeet ja oppaat organisaatioille ja yrityksille*. Haettu 17.11.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

Kyberturvallisuuskeskus. (2022b). *Toimintaohje – Vuotaneet tunnukset*. Haettu 17.11.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuotaneet%20tunnuksetToimintaohje.pdf

Limbasiya, T., & Doshi, N. (2017). An analytical study of biometric based remote user authentication schemes using smart cards. *Computers & Electrical Engineering*, *59*, 305–321. https://doi.org/10.1016/j.compeleceng.2017.01.026

Limbasiya, T., Soni, M., & Mishra, S. K. (2018). Advanced formal authentication protocol using smart cards for network applicants. *Computers & Electrical Engineering*, *66*, 50–63. https://doi.org/10.1016/j.compeleceng.2017.12.045

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys & Tutorials*, *17*(3), 1268–1293. https://doi.org/10.1109/COMST.2014.2386915

Mäentausta, R. (2022, 9. marraskuuta). *Kunnan työntekijöitä kohtasi ikävä yllätys maanantaiaamuna – Muuramen kunta epäilee joutuneensa tietomurron kohteeksi*. Yle.

Haettu 16.11.2022 osoitteesta https://yle.fi/a/74-20004117

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), Art. 1. https://doi.org/10.3390/cryptography2010001

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stobert, E., & Biddle, R. (2018). The Password Life Cycle. *ACM Transactions on Privacy and Security*, *21*(3), 1–32. https://doi.org/10.1145/3183341

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233–244. https://doi.org/10.1080/01449290903121386

Tulisalo, J. (2020). *Kohti parempaa tietoturvaa: Tutkimus monivaiheisesta tunnistautumisesta* [pro gradu -tutkielma, Jyväskylän yliopisto]. JYX-julkaisuarkisto. https://jyx.jyu.fi/handle/123456789/72547

Velásquez, I., Caro, A., & Rodríguez, A. (2018a). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

Velásquez, I., Caro, A., & Rodríguez, A. (2018b). Kontun: A Framework for recommendation of authentication schemes and methods. *Information and Software Technology*, *96*, 27–37. https://doi.org/10.1016/j.infsof.2017.11.004

Wang, C., Wang, D., Xu, G., & Guo, Y. (2017). A lightweight password-based authentication protocol using smart card. *International Journal of Communication Systems*, *30*(16), e3336. https://doi.org/10.1002/dac.3336

Wang, D., Zhang, X., Zhang, Z., & Wang, P. (2020). Understanding security failures of

multi-factor authentication schemes for multi-server environments. *Computers & Security*, *88*, 101619. https://doi.org/10.1016/j.cose.2019.101619

Yang, G., Wong, D. S., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*, *74*(7), 1160–1172. https://doi.org/10.1016/j.jcss.2008.04.002

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, *133*, 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006

Zimmermann, V., Marky, K., & Renaud, K. (2022). Hybrid password meters for more secure passwords – a comprehensive study of password meters including nudges and password information. *Behaviour & Information Technology*, *0*(0), 1–44. https://doi.org/10.1080/0144929X.2022.2042384