Jooel Tulisalo

KOHTI PAREMPAA TIETOTURVAA – TUTKIMUS MONIVAIHEISESTA TUNNISTAUTUMISESTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Tulisalo, Jooel
Kohti parempaa tietoturvaa – tutkimus monivaiheisesta tunnistautumisesta
Jyväskylä: Jyväskylän yliopisto, 2020, 52 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Keskustelu tietoturvallisuudesta on lisääntynyt viime aikoina runsaasti. IT-alan ammattilaisten keskuudessa on vahva konsensus siitä, että salasana on riittämätön mekanismi tietoturvalliseen autentikointiin. Tässä pro gradu -tutkimuksessa tutkittiin salasanoja ja vaihtoehtoisia autentikointimenetelmiä sekä etenkin monivaiheiseen tunnistautumiseen liittyviä kokemuksia käyttäjän näkökulmasta. Ihmisten salasanoista ja salasanakäyttäytymisestä johtuen salasanat autentikointimenetelmänä on turvallisuuden kannalta vajavainen. Monivaiheinen tunnistautuminen on tullut paikkaamaan tätä aukkoa. Empiirinen osuus toteutettiin puoliavoimena teemahaastatteluna ja haastateltavia oli yhdeksän. Olennaisimpana tuloksena tässä tutkimuksessa löydettiin, että monivaiheinen tunnistautuminen on varsin toimiva keino turvallisuuden parantamiseen. Sen käyttöön ja käytettävyyteen ei liity juurikaan ongelmia, jolloin se on helppo ottaa käyttöön yksityiselämässä sekä yrityksissä. Toisena tärkeänä asiana havaittiin, että käyttäjät eivät ole juurikaan varautuneet laitteen rikkoontumiseen tai katoamiseen, eli suurin osa ei tiennyt mitä autentikointiin käytettävän laitteen rikkoontumisesta voi seurata. Viimeisenä havainnoitiin, että tietoturvatietoisuuden lisääminen voi parantaa salasanakäyttäytymistä sekä edistää monivaiheisen tunnistautumisen käyttöönottoa.

Asiasanat: Monivaiheinen tunnistautuminen, autentikointi, salasanakäyttäytyminen, tietoturva

ABSTRACT

Tulisalo, Jooel
Towards better security - a study on multi-factor authentication
Jyväskylä: University of Jyväskylä, 2018, 52 pp.
Information Systems, Master's Thesis
Supervisor(s): Siponen, Mikko

There is lot of discussion about cybersecurity nowadays. IT professionals have consensus that passwords are not reliable enough to be the major authentication method anymore. In this master's thesis, the main research point was alternative authentication methods and multi factor authentication and the experiences of usage of those. In the research. The main problem with passwords as authentication method is user's bad password behavior, therefore the multi factor authentication should be implemented broadly to increase the security of authentication. The empirical study was done by using half-open theme interview and there were 9 participants. The main finding of this research was that multi factor authentication is pretty good method to increase the security. The implementation and usage were easy and simple and there were just minor problems with usage, even for not so tech savvy person. The second finding was that users are not well prepared for the loss of the equipment used to verify the multi factor authentication. The third finding was that by giving education and training in cyber security and good password manners the usage of multi factor authentication could also increase.

Keywords: Multifactor authentication, Authentication, Password behavior, Cyber security

SISÄLLYS

1 Johdanto

Jokapäiväisessä elämässämme tunnistaudumme erilaisiin palveluihin useita kertoja päivässä. Töissä kirjaudumme työasemalle, sähköpostiin ja internetin palveluihin. Arkielämässämme tunnistaudumme pankkiautomaatilla ja verkkopankkia käyttäessämme. Tunnistautumiskertoja kertyy kymmenittäin päivän aikana. Yleisin tunnistautumisen menetelmä on käyttäjätunnus ja salasana. Salasanoihin kuitenkin liittyy lukuisa määrä erilaisia riskejä. Erään tutkimuksen mukaan aktiivinen internetin käyttäjä käyttää jopa 15 eri palvelua yhden päivän aikana ja salasanoja on tyypillisesti noin 4–5 erilaista (Ives, Walsh & Schneider, 2004). Tietotekniikan lisääntyessä työvälineenä jatkuvasti myös salasanojen määrä kasvaa, jolloin houkutus uusiokäyttää jo olemassa olevia salasanoja kasvaa sen mukana. Lisäksi erilaiset salasanapolitiikat, kuten salasanan vaihtoväli, voi aiheuttaa ihmisissä reaktion, että salasanan monimutkaisuudesta ei välitetä niinkään, kunhan se on helposti muistettava. Salasanapolitiikkoja miettiessä onkin hyvä löytää kultainen keskitie turvallisuuden ja helppokäyttöisyyden välillä.

Miksi sitten tunnistautumismenetelmistä ja niiden turvallisuudesta puhuminen on olennaista? Kyberturvallisuuden alalla on vahva konsensus siitä, että suurin tietoturvariski on tavallinen käyttäjä (Yampolskiy, 2006). Yleisesti ottaen salasanan joutuminen vääriin käsiin on vain yksittäisen henkilön murhe, mutta otettaessa huomioon, että käyttäjä voi uusiokäyttää salasanaa henkilökohtaisissa- ja yritysjärjestelmissä niin riski ei enää ole pelkästään henkilökohtainen vaan se voi vaikuttaa myös muihin henkilöihin (Furnell, Esmael, Yang & Li, 2018; Weirich & Sasse, 2001b). Kuitenkin tulee huomioida, että käyttäjä tekee virheitä myös tahtomattaan ja vahingossa (Furnell ym., 2018). Tämän vuoksi tarvitsemme tehokkaampia ja turvallisempia tunnistautumismenetelmiä.

Salasanakäyttäytyminen voidaan karkeasti jakaa kahteen näkökulmaan, tekniseen ja sosiaaliseen. Teknisessä näkökulmassa kiinnostavinta on salasanapolitiikat, merkkimäärät ja niissä käytettävät merkit. Sosiaalisessa näkökulmassa voidaan katsoa käyttäjän olettamuksia, kuinka olennainen kohde hän on salasanahyökkäyksille ja kuinka henkilö käyttäytyy esimerkiksi organisaation sisällä; jaetaanko salasanaa ja kuinka tähän suhtaudutaan tiimin sisällä (Weirich

& Sasse, 2001b). Suurin osa tutkimuksista päätyy samaan lopputulokseen, että tavallisen käyttäjän salasanaturvallisuus ja osittain myös tietoisuus riskeistä on vähäinen, joten koulutusta salasanoihin liittyvästä turvallisuudesta tulisi olla enemmän (Weirich & Sasse, 2001b). Molemmat näkökulmat auttavat tunnistamaan henkilön salasanakäyttäytymisessä ilmeneviä riskejä ja toivottavasti auttavat ohjaamaan henkilöitä parempaan salasanakäyttäytymiseen.

Salasanakäyttäytymiseen liittyy vahvasti ymmärrys siitä, kuinka turvallisia salasana ovat. Salasanoihin liittyviä turvallisuusongelmia on paljon, niistä yleisimmät ovat salasanan riittämätön monimutkaisuus, salasanan uusikäyttö sekä salasanan kirjoittaminen ylös tai jakaminen muille.

Esimerkkejä salasanojen riittämättömästä monimutkaisuudesta on useita. Tutkimukset ovat pääsääntöisesti tehty tietylle osajoukolle, mutta tutkimusten tulokset ovat hyvin samantyyppisiä, joten tutkimustulokset voidaan yleistää myös laajemmalle joukolle. Eräässä tutkimuksessa (Komanduri ym., 2011) tutkittiin 5000 henkilön tutkimuksen avulla erilaisia salasanapolitiikkoja. Näistä kiinnostavin on basic8, missä vaatimuksena on vain 8-merkin pituus. Katsoessa mediaanituloksia, voidaan havaita, että suurin osa käyttää salasanassa vain pieniä kirjaimia ja numeroita, pituuden ollessa noin 10 merkkiä. Samansuuntaiseen tulokseen on päädytty myös toisessa tutkimuksessa (Yampolskiy, 2006), joskin tässä on havaittu huomattavasti enemmän vaihtelua suurten ja pienten kirjaimien määrässä. Kun taas vaatimuksiin lisätään vaatimus erikoismerkeistä, tutkimukset osoittavat suosituimpien merkkien olevan ’!’, ’@’ ja ’#’ (Komanduri ym., 2011; Shay ym., 2010; Yampolskiy, 2006).

Useissa tutkimuksissa on myös todettu, että usea tutkittava on jakanut oman salasanansa yhdelle tai useammalle henkilölle, yleisimmin organisaation sisällä, mutta myös sen ulkopuolella (Shay ym., 2010; Stanton, Stam, Mastrangelo & Jolton, 2005; Weirich & Sasse, 2001b). Tämä on luonnollisesti suuri turvallisuusriski organisaatiolle. Syitä jakamiseen on muun muassa tärkeän tiedon saaminen työasemalta henkilön ollessa poissa työaseman ääreltä, korkeammassa asemassa olevien henkilöiden totteleminen, epävirallinen tuki sekä organisoitu jakaminen (Weirich & Sasse, 2001b).

Kuten aiemmin mainittu, myös salasanojen uusiokäyttö on merkittävä riski turvallisuudelle. Henkilö ei välttämättä ymmärrä, että hänen käyttäessä samaa salasanaa useassa paikassa, on salasanaturvallisuus yhtä kuin heikoimman palvelun salasanaturvallisuus (Weirich & Sasse, 2001b). Aiemmin myös totesimme, että salasanojen uusiokäyttö johtuu usein siitä, että salasanoja vaativia palveluita on niin paljon, että henkilö ei pysty käsittelemään kaikkia salasanoja. Eräs tutkimus osoittaa, että aktiivisesti käytössä olevia salasanoja olisi 4–5 (Ives ym., 2004), mutta toisaalta web-palveluihin erikoistuneessa tutkimuksessa näitä havaittiin olevan jopa seisemän (Stanton ym., 2005).

Huonon salasanakäyttäytymisen takia pelkkä salasana on tietoturvan kannalta usein riittämätön vaihtoehto. Tässä tutkimuksessa perehdytään salasanan ohella muihin tunnistautumismenetelmien sekä etenkin monivaiheisen tunnistautumisen käyttöönoton syihin ja käyttökokemuksiin. Ensimmäisessä kappaleessa käymme läpi monivaiheisen tunnistautumisen menetelmiä ja taus-

toja, sen jälkeen perehdymme paremmin yleisimpään autentikointimenetelmään, salasanaan, jonka jälkeen käymme läpi empiirisen osuuden tulokset sekä analyysin ja lopuksi on vielä yhteenveto.

2 Monivaiheinen tunnistautuminen

Monivaiheinen tunnistautuminen (engl. multi-factor authentication, tästä eteenpäin käytetään lyhennettä MFA) on tunnistautumisen menetelmä, missä yhdistetään kaksi tai useampi tunnistautumismenetelmää päästäksemme kirjautumaan sisään palveluun (Aloul, Zahidi & El-Hajj, 2009; Kim & Hong, 2011). Yleensä ensimmäinen tunnistautumisen muoto on salasana ja sen lisäksi käytetään esimerkiksi puhelimeen tulevaa viestiä tai autentikointisovellusta (Ometov ym., 2018; Sabzevar & Stavrou, 2008). Monivaiheisessa tunnistautumisessa yleisimmin käytetäänkin kaksivaiheista tunnistautumista (2FA), mutta mahdollisuus on myös useampiin. Selkeyden vuoksi kuitenkin tässä tutkimuksessa käytetään vain MFA käsitettä.

Salasana on yleisin MFA:n kanssa käytetty tunnistautumismenetelmä, mutta lisäksi on myös muita tunnistautumis- eli autentikointimenetelmiä. Tässä luvussa esitellään tunnistautumisen lähtökohtia, eri tunnistautumismenetelmiä, sekä niiden hyötyjä ja riskejä. Koska salasana yhdistettynä yksilöivään tunnukseen kuten käyttäjätunnukseen on edelleen käytetyin tunnistautumisen muoto, on sille varattu oma lukunsa (3) tässä tutkielmassa.

2.1 Yleistä

Tarvitsemme tunnistautumista erilaisiin palveluihin ja ympäristöihin joka päivä työssä ja arjessa. Tarvitsemme pääsyä työasemille, sähköposteihin, internetin palveluihin sekä yrityksen ympäristöihin. Yleisimmin tunnistautumiseen käytetty keino käyttäjätunnus ja salasana (Sabzevar & Stavrou, 2008), mutta se ei ole ainoa käytössä oleva tunnistautumisen menetelmä. Todellisuudessa käyttäjätunnus ja salasana ovat nykyisen laskentatehon takia melko huono vaihtoehto tunnistautumiseen, etenkin ilman lisäsuojausta. Käyttäjien salasanakäyttäytyminen on huonoa, mikä aiheuttaa suuria riskejä yrityksille, sekä käyttäjille itselleen. Salasanakäyttäytymiseen paneudumme enemmän vielä luvussa 3.

MFA onkin tullut paikkaamaan aukkoa yksivaiheisen tunnistautumisen ongelmiin. MFA:ta suositaankin etenkin paikoissa ja palveluissa, jossa turvallisuussuositukset ovat korkeammat, kuten valtioiden organisaatioissa (Kim & Hong, 2011) tai pankkiautomaatilla asioidessa (Aloul ym., 2009).

Pääsääntöisesti tunnistautumisen menetelmät voidaan jakaa kolmeen eri kategoriaan (Aloul ym., 2009; Kim & Hong, 2011; Sabzevar & Stavrou, 2008):

1. Mitä tiedät
2. Mitä omistat
3. Mitä olet

Ensimmäiseen kategoriaan perustuu asioihin mitä vain sinä tiedät. Tähän kategoriaan menevät käyttäjätunnukset ja salasanat sekä erilaiset muistamismenetelmät, kuten graafiset salasanat. Toiseen kategoriaan kuuluu asiat mitä sinä omistat tai mitä sinä pidät hallussasi. Tähän kuuluu erilaiset älykortit, apuvälineet (tokenit) sekä mobiiliautentikointi. Kolmannessa kategoriassa on menetelmät, joissa käytetään jotain henkilölle kuuluvaa ominaisuutta hyväkseen. Tähän kuuluu biometriset tunnisteet kuten iirisskannerit, sormenjälkilukija ja puheentunnistus tai ihmisen käyttäytyminen. (Ometov ym., 2018). Näiden lisäksi puhutaan myös neljännestä, ei vielä niin yleisestä kategoriasta, joka on: ”missä olet”. Tämä perustuu esimerkiksi GPS-paikannukseen tai tiettyyn sijaintiin (Gnanaraj, Ezra & Rajsingh, 2013). Sijainti voidaan määritellä esimerkiksi katsomalla laitteen MAC-numeroa, joka on yksilöllinen ja muuttumaton kaikilla verkkoon kytketyillä laitteilla.

Vaikkakin tässä tutkimuksessa keskitytään etenkin monivaiheiseen tunnistautumiseen arkielämässä ja työpaikalla, on MFA:lla muitakin sovellutuksia. Tutkimuksessaan (Ometov ym., 2018) esittävätkin tutkimuksessaan kolme sovellutusta, missä MFA:ta voidaan käyttää:

- Käyttäjän tunnistautuminen elektronisen laitteen kanssa.
- Infrastruktuurin kanssa tunnistautuminen (kulkulupa)
- Internet of Things -laitteiden tunnistautuminen.

2.2 Erilaiset tunnistautumismenetelmät

Tässä esitellään eri tunnistautumismenetelmiä, jotka ovat vähemmän käytettyjä kuin salasanat, mutta silti käytössä olevia tai potentiaalisia vaihtoehtoja. Täytyy ottaa huomioon, että seuraavaksi mainittujen lisäksi on myös useita muita tunnistautumismenetelmiä, mutta niiden käyttö on vähäistä tai vähän tunnettua.

2.2.1 Vuorovaikutukseton autentikointi

Vuorovaikutukseton autentikointi (engl. zero-interaction authentication) on menetelmä, jossa koneen tiedostot suojataan salausavaimella, jonka avaamiseen käytetään erillistä apuvälinettä (engl. token), joka on tunnistavaan laitteeseen yhteydessä langattomasti ja täysin ilman käyttäjän vuorovaikusta (Truong ym., 2014). Apuväline on jatkuvassa langattomassa yhteydessä työaseman kanssa, jolloin kantajan poistuessa työaseman äärestä, myös muistissa olevat tiedostot salataan. Käyttäjän palatessa autentikointi lähtee taas päälle, jolloin tiedostot ovat taas käytettävissä (Corner & Noble, 2002; Truong ym., 2014).

Tämä tunnistusmenetelmä on turvallinen siinä mielessä, että kyseinen apuväline on yleensä aina käyttäjän mukana. Tämän kadotessa kuitenkin tiedostojen suojausta on vaikeaa poistaa, joka on toisaalta hyödyllinen, jos työasema varastetaan. Murtamiseen voidaan käyttää myös niin kutsuttua ”Relay attack” metodia, jossa murtajat huijaavat salaustiedon vahvistavaa laitetta lähettämällä oikean henkilön salausavainta murtajien tietoon (Truong ym., 2014). Menetelmiä tämän turvallisuuden parantamiseksi on kehitelty ja myös uudet puettavat IoT laitteet voivat edesauttaa tämän tunnistautumismenetelmän käyttöönottoa (Miettinen, Asokan, Nguyen, Sadeghi & Sobhani, 2014).

2.2.2 Biometrinen tunnistus

Biometrinen tunniste on tunnistusmenetelmä, jossa ihminen yksilöidään biometrisen tunnisteen avulla. Tunnisteet voidaan jakaa fyysisiin tunnisteisiin, kuten sormenjälki, silmäkuva tai kasvot, sekä käyttäytymiseen liittyviin tunnisteisiin, kuten puheääni tai allekirjoitus (O'Gorman, 2003). Lopullisen tunnistamisen tekee lähes poikkeuksetta tietokone.

Biometrisiä tunnisteita pidetään potentiaalisena vaihtoehtona MFA:n yhtenä osa-alueena (Braz & Robert, 2006), sillä biometrinen tunniste on lähes poikkeuksetta yksilöllinen, kuten sormenjälki tai silmän iiris. Tunnistautumisen kannalta ongelmia voi aiheuttaa se, että biometrisellä tunnisteella saatu data ei luultavasti ole koskaan täysin samanlaista (Bhargav-Spantzel ym., 2007), vaan siihen vaikuttaa muun muassa vallitsevat sääolosuhteet, valoisuus, ilmanlaatu tai käyttäjän äänen muuttuminen (O'Gorman, 2003). Tällaiset ongelmat vaikuttavat myös käyttäjän halukkuuteen käyttää uusia menetelmiä, jos ne eivät toimi kuten käyttäjä haluaisi.

Sormenjälkitunnistusta pidetään varteenotettavimpana vaihtoehtona biometrisenä tunnisteena, mutta sen käyttö vaatii monivaiheista tunnistautumista ollessaan yksistään liian heikko tunnistautumisen keino. Edullisissa sormenjälkitunnistimissa on riskinä, että ne eivät ole tarpeeksi luotettavia. Eräässä tutkimuksessa verrataan sormenjälkitunnistusta jopa pin-koodiin (Bhargav-Spantzel ym., 2007). Lisäksi sormenjälkitunnistimien hankinta- ja ylläpitokustannukset voivat olla korkeita, esimerkiksi pankkiautomaatti käytössä (Aloul ym., 2009).

2.2.3 Tokenit

Englannin kielen sana ’token’ tarkoittaa tässä tapauksessa tunnistautumiseen käytettävää apuvälinettä, joka voi olla tunnusluvun sisältävä esine, kuten pankkikortti tai sirukortti. Tai vaihtoehtoisesti se voi olla esine, joka luo kertakäyttöisensalasanan (engl. one-time password), aikaan sidotun salasanan (engl. time-synchronous) tai haastepohjaisen tunnisteen (engl. challenge response). Tästä edespäin tällaisesta esineestä käytetään token sanaa. Token-pohjaisen tunnistautumisen etuna on se, että siihen voidaan tallettaa useita salasanoja. Token myös yleensä salaa tiedon paremmin kuin pelkkä salasana. Turvallisuuden kannalta token on näkyvä esine, joten sen puuttuminen on helppo havaita. Lisäksi se voi lisätä turvallisuutta salasanaan verrattuna, sillä mahdollisen hyökkääjän tulee saada ensin token haltuunsa ja sitten vasta voidaan yrittää murtaa siihen liittyvä salasana. (O'Gorman, 2003).

2.2.4 Mobiiliautentikaattori

Mobiiliautentikaattori on varmasti useimmille tuttu tunnistautumisen keino. Useat palveluntarjoajat jo tarjoavat mahdollisuuden käyttää mobiilitunnistinta eli autentikaattoria lisäsuojana mahdollisen muun tunnistekeinon, kuten pinkoodin tai salasanan lisäksi. Tällaista palvelua tarjoaa esimerkiksi Google Authenticator, joka pyytää hyväksymään kirjautumisen liitetystä laitteesta aina, kun se havaitsee tuntemattoman kirjautumisen tuntemattomasta laitteesta. Mobiiliautentikaattori voi olla yrityksille kannattavampi vaihtoehto, kuin erillinen token, sillä sen käyttöönottokustannukset ovat vähäisempiä, koska suurimmalla osalla työntekijöistä on mobiililaite käytössä, jos muutenkin (Aloul ym., 2009).

2.2.5 Single-Sign On (SSO)

Single-Sign On ei ole varsinainen autentikointimenetelmä vaan autentikointia helpottava teknologia. Siinä yhdellä hyvin varmistetulla autentikoinnilla voidaan kirjautua useisiin saman palveluntarjoajan palveluihin samanaikaisesti, ilman että tarvitsee autentikointia tehdä joka kerta uudelleen. Tämä nopeuttaa käyttöä etenkin yritysympäristössä, missä koneelle kirjautuessa voidaan tunnistautua ja sen jälkeen päästään käyttämään yrityksen järjestelmiä Single-Sign On -teknologian avulla kirjoittamatta salasanaa uudelleen ja uudelleen.

2.3 MFA haasteet

Vaikkakin MFA on jo lähes välttämätön turvallisuustekijä, liittyy siihen useita haasteita. Ometov ja kumppanit havaitsivat tutkimuksessaan (Ometov ym., 2018) neljä eri haastetta. Ensimmäisenä haasteena voidaan pitää käyttöönottoa

(engl. user accepctance), joka liittyy etenkin MFA:n käytettävyyteen. Käytettävyyteen liittyvät ongelmat voidaan jakaa kolmeen tekijään:

- Toiminnon nopeus (engl. task efficiency) – Rekisteröitymiseen ja autentikointiin kuluva aika
- Toiminnon helppous (engl. task effectiveness) – Montako kirjautumiskertaa vaaditaan
- Käyttäjän tottumus (engl. user preference) – Suosiiko käyttäjä yhtä menetelmää enemmän kuin toista

Näiden lisäksi vaikuttavana tekijänä voidaan nähdä käyttäjän ikä, vanhemman henkilön ollessa hitaampi kuin nuori. Sukupuolella kuitenkaan ei olla havaittu olevan merkitystä.

Toisena haasteena voidaan pitää integraatiota. Vaikkakin IT-turvallisuuden ja fyysisen turvallisuuden yhdistelmä voi olla hyvinkin tehokas mutta pelkästään niiden saattaminen yhteen voi olla ongelmallista. Tämän lisäksi biometriset tunnisteet pitäisi tehdä niin, että ne ovat yleiskäyttöisiä erilaisten viitekehysten kanssa. Tämän lisäksi moni-biometriset järjestelmätkin tulisi ottaa huomioon. Myös yritysriippuvaisuus voidaan laskea integraation ongelmaksi, sillä yritysten luomat järjestelmät ovat yleisesti hyvin joustamattomia. Erilaisten rajapintojen ja viitekehysten mielekkyyttä ja luotettavuutta ei voida myöskään usein arvioida, koska lähdekoodi ei ole avointa vaan toimittajariippuvaista. Täten MFA ei ole myöskään millään tavalla standardisoitua (Sabzevar & Stavrou, 2008).

Kolmantena haasteena nähdään turvallisuus ja yksityisyys. Tunnistautumiseen käytettävät laitteet, kuten biometriset tunnisteet sisältävät useita komponentteja ja sensoreita, jotka ovat vaarassa hyökkäyksille. Krakkerit voivat päästä käsiksi esimerkiksi sensorin tallentamaan tietoon tai jopa itse sensoriin. Myös sijaintiin perustuvissa teknologioissa on omat ongelmansa, sillä sijainti dataa voidaan syöttää vastaanottavaan päähän, jolloin järjestelmä ei toimi enää oikein.

Neljäs haaste on ympäristöön liittyvät tekijät. Etenkin biometrisissä tunnisteissa, kuten sormenjäljissä tai kasvontunnistuksessa voidaan vaatia tietynlaisia olosuhteita, että tunnistaminen onnistuu. Tämä johtuu sensoreista, jotka voivat saada erilaista dataa riippuen asennosta, valoisuudesta, kosteudesta ja muista tekijöistä (Ometov ym., 2018).

MFA:n haasteet ovat sekä teknisiä, että käyttäjälähtöisiä. Ongelmana on edelleen sensorien tarkkuus, niiden kohtalaisen helppo murrettavuus sekä käytettävyys. Tässä tutkimuksessa tulemme keskittymään ennen kaikkea käyttäjälähtöisiin ongelmiin eli käytettävyyteen. Tunnistautumiseen käytettävien laitteiden teknologiaan ja teknisiin piirteisiin ei tässä tutkimuksessa oteta kantaa.

Tässä osiossa kävimme lyhyesti läpi autentikointia ja monivaiheisesta tunnistautumista. Tutustuimme erilaisiin tunnistautumismenetelmiin, joita voidaan käyttää yksinään (1FA) tai yhdessä toisen autentikointimenetelmän kanssa (MFA). Vaikka MFA parantaa turvallisuutta laitteisiin tai infrastruktuu-

riin kirjautuessa, sisältää se myös riskejä ja haasteita, mitkä tulee ottaa huomioon käyttöönotossa.

3 Salasanat

Tässä osuudessa käymää läpi salasanoihin liittyvää teoriaa. Salasanan ollessa edelleen käytetyin tunnistautumisen muoto, sekä yleensä myös MFA:n yksi tunnistautumisvaihe, tulee meidän olla tietoisia salasanoista ja niihin liittyvästä tieteellisestä keskustelusta. Ensimmäisenä käymme läpi salasanatyypit, jonka jälkeen tarkastellaan organisaatio näkökulmaa. Tämän jälkeen katsomme vielä riskejä, sekä salasanakäyttäytymistä.

3.1 Alkuperä

Salasana on keino salata asioita muilta henkilöiltä, päästäkseen käsiksi salattuihin asioihin tulee siis tietää salasana. Salasanaa käytetään yleisesti yhdessä käyttäjätunnuksen kanssa. Englannin sana ”password” kääntyy huonosti suomen kielelle, sillä meillä salasanalla voidaan tarkoittaa laajemmin laitteen tai tietojärjestelmän lukitukseen tarkoitettua keinoa.

Alun perin salasanoja käytettiin unix-pohjaisissa järjestelmissä, joissa järjestelmän rajoitusten takia suurin sallittu merkkimäärä oli 8-merkkiä. Tähän perustuen edelleen suositaan 8-merkkisiä salasanoja (Keith, Shao & Steinbart, 2007). Salasana on yksi kolmesta autentikoinnin kategoriasta. Kaksi muuta kategoriaa ovat tokenit (eli merkit) ja biometriset tunnisteet. Autentikointikategoriat ovat jaettu kysymyksiin ”Mitä sinä tiedät”, ”Mitä sinä omistat” ja ”Kuka sinä olet” (O'Gorman, 2003).

3.2 Salasanatyypit

Usein salasanoista puhuttaessa tarkoitetaan alfanumeerisia salasanoja, joka on edelleen yleisin salasanatyyppi. Älylaitteiden ja sitä myötä salasanojen lisääntyminen kuitenkin aiheuttaa painetta uusien salasanatyyppien kehittämiselle, sillä alfanumeeriset salasanat eivät ole tietoturvallisia, ellei niistä tehdä tarpeek-

si monimutkaisia. Salasanatyyppejä on kuitenkin muitakin, joita esittelen tässä kappaleessa.

3.2.1 Tekstipohjaiset salasanat

Tekstipohjaiset salasanat ovat ensimmäinen salasanatyyppi, sekä edelleen suosituin tietojärjestelmiin kirjautumisen muoto (Biddle, Chiasson & Van Oorschot, 2012; Campbell, Ma & Kleeman, 2011; Komanduri ym., 2011; Sabzevar & Stavrou, 2008). Tekstipohjainen salasana on salasanatyyppi, joka koostuu alfanumeerisista merkeistä eli aakkoset A-Z sekä numerot 0-9. Nykyisin salasanavaatimuksissa kuitenkin vaaditaan yleisesti myös symboleita, joten puhutaan tekstipohjaisista, eikä alfanumeerisista salasanoista. Tekstipohjaisten salasanojen etuna voidaan pitää, että ne voidaan kirjoittaa helposti esimerkiksi näppäimistöllä ilman muita apuvälineitä (Komanduri ym., 2011). Lisäksi ne ovat helppoja ja halpoja ottaa käyttöön, sekä ne ovat tuttuja kaikille käyttäjille (Biddle ym., 2012; Campbell ym., 2011; Keith ym., 2007). Kääntöpuolena tekstipohjaiset salasanat ovat usein ei-tietoturvallisia, sillä helpomman muistettavuuden vuoksi niistä tehdään lyhyitä ja helposti arvattavia (Dagvatur, Z., Mohaisen, A., Lee, K., Nyang,D., 2019; Wiedenbeck, Waters, Birget, Brodskiy & Memon, 2005). Myös vähäinen tietämys salasanan murtamistekniikoista voi olla osasyy huonolaatuisiin salasanoihin. (Dagvatur, Z., Mohaisen, A., Lee, K., Nyang,D., 2019)

Toisaalta nykyisin on herätty siihen tosiasiaan, että kompleksiset ja lyhyet alle 10-merkkiset salasanat eivät ole niin tietoturvallisia kuin pitkät salasanat (Keith ym., 2007). Pitkistä salasanoista puhuttaessa voitaisiin puhua salasanan sijaan salasanalauseesta (engl. passphrase), joskin pitkä salasana voi olla myös muu kuin salasanalause. Pitkät salasanalauseet ovat turvallisempia kuin lyhyet salasanat, koska ne on yleisesti helpompia muistaa, mikä vähentää esimerkiksi paperille kirjoittamisen tarvetta (Keith ym., 2007). Toisissa tutkimuksissa kuitenkin on havaittu, että satunnaisen salasanan ja salasanalauseen muistamisen välillä ei havaittu merkittäviä eroja (Yan, Blackwell, Anderson & Grant, 2004). Muistamisen lisäksi salasanalauseet ovat turvallisempia, sillä erilaiset salasanan murtamistekniikat, kuten brute force toimii paremmin lyhyillä kuin pitkillä salasanoilla (Keith ym., 2007; Yan ym., 2004).

3.2.2 Graafiset salasanat

Graafiset salasanat tulivat vaihtoehdoksi tekstipohjaisille salasanoille ja aikaisimmat tiedot ovat 1999-luvulta. (Biddle ym., 2012) Graafiset salasanat sisältävät grafiikkaa, kuten piirroksia, kuvia tai pisteitä. Tällainen kirjautumismuoto on helpompi muistettava ja turvallisempi, kuin alfanumeeriset salasanat, jotka muistettavuuden vuoksi tehdään usein liian yksinkertaisiksi (Dagvatur, Z., Mohaisen, A., Lee, K., Nyang,D., 2019; Wiedenbeck ym., 2005). Graafisia salasanoja on erityyppisiä, joten niitä avataan hieman enemmän seuraavaksi.

Ensimmäinen graafinen salasanatyyppi on muistamiseen perustuvat salasanat (engl. recall-based systems), jossa tyhjälle sivulle tai ristikolle piirretään

salainen piirros. Tällainen salasana on kohtuullisen helppo muistaa, mutta voi myös aiheuttaa ongelmia, sillä muistamisen apuna voidaan käyttää jotain näkyvää muotoa. Tällöin myös muilla on mahdollista hyödyntää kyseistä muotoa, jolloin piirroksen arvattavuus on helpohko. (Biddle ym., 2012).

Toisena salasanatyyppinä on tunnistamiseen perustuvat salasanat (engl. recognition-based systems). Tällaiset salasanat perustuvat yleisesti kuvasarjoihin, joista tunnistetaan aiemmin valitut kuvat vääristä kuvista. Turvallisuuden kannalta tällainen tyyppi ei ole sen parempi kuin 4–5 merkkinen pin-koodi. Toisaalta näiden etuna on se, että ihminen yleisesti muistaa näkemänsä kuvat melko tarkasti, joten kirjautuminen sujuu vaivattomasti. (Biddle ym., 2012).

Kolmas tyyppi on vihje-muistamistyyppi (engl. cued-recall system). Tässä tyypissä käyttäjän tulee muistaa tiettyjä pisteitä tai asioita kuvista, jopa tietyssä järjestyksessä. Tämä tapa on helpompi kuin täysin muistiin perustuvat tyypit. Tämä tyyppi on turvallinen siinä mielessä, että kuva ei välttämättä anna mitään vihjeitä muille, kuin sen alkuperäiselle tekijälle. Erilaiset klikkauksen seurantasoftat, sekä selän takaa katsomiselle tämä on toki haavoittuvainen. (Biddle ym., 2012).

Kokonaisuudessaan graafiset salasanoja pidetään hyvänä vaihtoehtona tekstipohjaiselle salasanalle sen käyttäjäystävällisyyden vuoksi. Graafiset salasanat tarjoavat lukemattomia mahdollisia yhdistelmiä, jotka on helpompia muistaa kuin tavallinen 8-merkkinen salasana (Sabzevar & Stavrou, 2008).

3.3 Salasanat organisaatiossa

Salasanaturvallisuuteen vaikuttaa useat tekijät. Lähtökohtaisesti kuitenkin voidaan ajatella, että salasanaturvallisuus on aina kiinni loppukäyttäjästä ja hänen toiminnastaan. Organisaatioiden ja palveluntarjoajien turvallisuutta ohjaa usein standardit ja salasanapolitiikat. Nämä ei kuitenkaan välttämättä riitä, jos käyttäjä ei saada toimimaan tietoturvallisella tavalla.

3.3.1 Standardit

Standardit ovat hyväksi todettuja käytäntöjä, joita olisi hyvä noudattaa. Salasanaturvallisuudesta puhuttaessa voidaan puhua kyberturvallisuusstandardeista tai laajemmin informaatioteknologian standardeista. Tunnetuin standardien myöntäjä on International Organization for Standardization (ISO). Suomessa standardeja myöntävä taho on SFS (Suomen standardisoimisliitto). Salasanastandardeista puhuttaessa voidaan myös katsoa muita isoja tietotekniikka auktoriteetteja, kuten NIST (National Institute of Standards and Technology). NIST on määritellyt salasanalle seuraavanlaiset standardit:

- Salasanan tulee olla vähintään kahdeksan merkkiä pitkä
- ASCII, välilyönti ja Unicode merkit tulisi olla hyväksyttyjä
- Salasanaa luotaessa ei tulisi olla vihjeitä tai kysymyksiä

- Salasana ei tulisi olla sama kuin jo aiemmin vuodettu salasana
- Salasanan ei tulisi sisältää sanakirja sanoja
- Salasanassa ei tulisi olla useita peräkkäisiä tai toistuvia merkkejä kuten ’aaaa’ tai ’1234’
- Salasanan ei tulisi sisältää viittauksia esimerkiksi yrityksen nimeen tai muuhun näkyvillä olevaan asiaan.

Edellä mainitut ovat yhdistetty NIST:in ohjeista salasanan autentikoijaa (engl. authenticator) sekä salasanan varmistajaa (engl. verifier) koskevista ehdoista ((Grassi, Fenton & Burr, 2017) kohdat 5.1.1.1 ja 5.1.1.2)).

3.3.2 Salasanakäytännöt

Siinä missä standardit määrittelevät mitä tulisi tehdä, salasanakäytännöt/salasanapolitiikat (engl. password policy) ovat niitä käytännön toimia, joita tehdään. Salasanakäytännöt ovat niitä, jotka näkyvät päivittäisessä elämässä esimerkiksi työpaikoilla tai esimerkiksi web-sovelluksissa. Salasanakäytännöt on usein johdettu joko yrityksen omista, tai yleisemmistä, kuten NIST:n standardeista. Yritykset saavat itse määritellä omat salasanakäytäntönsä, eikä niitä ole rajattu millään tavalla. Salasanakäytännöt kuitenkin pitkälti määrittävät millaisen salasanan käyttäjät tekevät. Kohtalaisen turvallisesta salasanakäytännöstä voitaisiin esimerkkinä pitää Microsoftin Windows 10 asetettua salasanakäytäntöä (Microsoft, 2017), joka sisältää seuraavat vaatimukset, huomioitavaa on, että nämä ei täytä kaikkia NIST:n suosittelemia vaatimuksia:

- Iso kirjain
- Pieni kirjain
- Vähintään 10 merkkiä
- Ei-alfanumeerinen merkki, € ja £ merkkejä ei lasketa mukaan
- Unicode -merkki, joka ei ole aakkonen, tähän sisältyy muun muassa aasialaiset unicode merkit

Tämän kaltainen salasana on tänä päivänä erittäin yleinen, joskin merkkimäärä voi olla lyhempi, kuten 8-merkkiä. Salasanakäytäntöjen puolesta puhuu esimerkiksi tutkimus missä havaittiin, että vain 5 merkin salasana, jossa oli muitakin rajoituksia, oli murrettavissa 33 % tapauksista. Kun taas 8-merkin salasana rajoitusten kanssa oli murrettavissa vain 12.5 % tapauksista. (Proctor, Lien, Vu, Schultz & Salvendy, 2002) Tässä tulee kuitenkin huomioida, että kehittyneempien murtamisohjelmien ja valmiiden salasanalistojen takia alle 8 merkkiset salasanat ovat lähes varmasti murrettavissa säädyllisessä ajassa.

3.4 Riskit

Tietoturva on tänä päivänä pahempi uhka kuin koskaan ennen ja salasanat ovat avain organisaation tietojärjestelmiin ja yksityisessä käytössä luottokortti- sekä muihin henkilökohtaisiin tietoihin, joten myös kyberrikolliset ovat kiinnostuneita niistä. Kuten edellä mainittiin erilaiset standardit ja käytännöt voivat vaikuttaa salasanojen luomiseen, mutta se ei vielä poista käyttäjien riskialtista käyttäytymistä. Itse käyttäytymiseen menemme syvemmin myöhemmin tässä tutkielmassa, mutta tässä kappaleessa on tarkoitus esitellä erilaisia riskejä, joita salasanoihin liittyy.

3.4.1 Hakkerointi/krakkerointi

Ensimmäisenä varmasti kaikille mieleen tuleva turvallisuuspoikkeama salasanoista puhuttaessa on hakkerointi. Tämä voi olla kuitenkin harhaanjohtava termi, sillä hakkerointia voidaan tehdä myös hyvässä tarkoituksessa, niin sanottua 'valkohattu-hakkerointia'. Useat yritykset palkkaavatkin valkohattuhakkereita testaamaan heidän järjestelmiään. Tällainen toiminta on aina etukäteen sovittua, joten sitä ei tule yhdistää krakkerointiin.

Henkilökohtaiseen hyötymiseen tai puhtaaseen vahingontekoon liittyvissä tapauksissa puhutaan krakkeroinnista ja krakkereista (eng. cracker) (Adams, Sasse & Lunt, 1997). Krakkerit ovat niitä, jotka tunkeutuvat tietojärjestelmiin ja saavuttavat näin haluamansa hyödyn. He voivat esimerkiksi salata tärkeän tiedoston ja antaa oikeudet takaisin vain lunnaita vastaan. Kun krakkeri on saanut käyttöönsä salasanan, on todennäköistä, että hän pääsee käsiksi myös muihin käyttäjän käyttämiin järjestelmiin, sillä salasanojen uusiokäyttö on erittäin tavallista käyttäjien keskuudessa.

Krakkerointimenetelmiä on useita eikä nämä menetelmät vaadi useinkaan juuri minkäänlaisia tietoteknisiä taitoja, kuten usein krakkereista ajatellaan. Tunnetuimpia näistä menetelmistä lienee kalasteluviestit (engl. phishing), brute force -hyökkäykset), keyloggerit, ja olan yli kurkkiminen (engl. shoulder surfing).

Phishing eli kalasteluviesti on keino, missä käyttäjälle lähetetään sähköpostissa linkki sivustolle, jonka takana pyydetään esimerkiksi henkilötietoja tai luottokorttitietoja. Viestissä voidaan myös suoraan kalastaa käyttäjän tietoja.

Brute force -tekniikka on kohtalaisen varma tekniikka, mutta muut keinot ovat huomattavasti vähemmän aikaa kuluttavia ja helpompia. Brute force -tekniikassa käytetään tietokoneen laskentatehoa hyväksi. Tietokone laitetaan syöttämään satunnaisia merkkijonoja, tai jonkin vuodetun salasanalistan mukaisia salasanoja ja näin yritetään arvata käyttäjän salasana.

Keyloggerit ovat sovelluksia tai jopa fyysinen laite, joka seuraa käyttäjän tekemää näppäimistö syötettä. Käyttäjän kirjautuessa palveluun saadaan siten hänen käyttäjätunnuksensa ja salasana selville.

Olan yli kurkkiminen on kirjaimellisesti henkilön selän takaa kurkkimista. Tämä on varmasti yleisin keino saada esimerkiksi pankkikortin pin-koodi selville, mutta yhtä hyvin tätä voidaan käyttää, vaikka julkisissa paikoissa saadakseen käyttäjän salasana selville.

3.4.2 Salasanojen uusiokäyttö

Salasanojen uusiokäyttö on yleistä, sillä se keventää salasanan muistamisesta aiheuttamaa kuormaa (Zhang, Luo, Akkaladevi & Ziegelmayer, 2009). Se on myös nopeampi keino päästä kirjautumaan järjestelmään, koska yksittäinen salasana on helppo kirjoittaa ulkomuistista. Haittapuolena uusiokäytössä taas on se, että krakkereiden saatua selville tämän salasanan, pääsevät he kirjautumaan myös muihin palveluihin, missä käytetään samaa salasanaa. Organisaatiossa tämä voi tarkoittaa sitä, että päästään ensin käsiksi mitättömän tuntuiseen järjestelmään, mutta sen jälkeen voidaan kirjautua myös kriittisiin järjestelmiin (Ives ym., 2004; Stobert & Biddle, 2014).

3.4.3 Salasanan jakaminen

On yllättävän yleistä, että salasanaa jaetaan esimerkiksi työkavereiden tai opiskelutovereiden kesken. Syynä voi olla esimerkiksi työn kannalta relevantin tiedon saaminen toisen ollessa poissa (Shay ym., 2010), tai jopa pelkkä luottamus toiseen työntekijään tai omaan puolisoon (Singh, Cabraal, Demosthenous, Astbrink & Furlong, 2007; Weirich & Sasse, 2001a). On sanomattakin selvää, että jaettu salasana voi tarjota pääsyn myös muihin käyttäjän käyttämiin palveluihin, sillä salasanojen uusiokäyttö on yleistä.

3.5 Salasanakäyttäytyminen

Käyttäjän käyttäytymisen on havaittu olevan yksi merkittävin tekijä puhuttaessa tietojärjestelmien tietoturvasta (Campbell ym., 2011; Leach, 2003). Yhtenä osa-alueena käyttäjien turvattomasta käyttäytymisestä on salasanoihin liittyvä käyttäytyminen, joka jakautuu sosiaalisiin ja teknisiin, sekä muistiin liittyviin tekijöihin.

Käyttäytyminen itsessään on laaja käsite eikä sen tarkka määritelmä ole helppoa esittää. Tieteen näkökulmasta käyttäytyminen kuitenkin tarkoittaa tapaa, jolla ihminen tai eläin käyttäytyy tietyssä tilanteessa tiettyjen olosuhteiden vallitessa. (https://dictionary.cambridge.org/dictionary/english/behaviour) Koska käyttäytymiseen vaikuttaa olosuhteet, on tiettyihin asioihin olemassa omat käyttäytymistutkimuksensa. Esimerkiksi voidaan puhua kuluttajakäyttäytymisestä ja organisaatiokäyttäytymisestä. Myös tietoturvaan ja salasanoihin liittyen on paljon omanlaistansa käyttäytymistä, jota tässäkin tutkimuksessa halutaan tutkia.

Salasanakäyttäytymisestä on tehty jonkin verran aiempaa tutkimusta ja käyttäytymisen taustalla olevat vaikuttimet voidaan yleisesti jakaa kahteen osioon, sosiaalisiin ja teknisiin. Näiden lisäksi kuitenkin havaittiin vielä muistiin liittyvät vaikuttimet. Seuraavaksi paneudumme näihin kolmeen osa-alueeseen syvemmin. Sosiaalisessa näkökulmassa voidaan katsoa käyttäjän olettamuksia, kuinka olennainen kohde hän on salasanahyökkäyksille ja kuinka henkilö käyttäytyy esimerkiksi organisaation sisällä; jaetaanko salasanaa, kuinka tähän suhtaudutaan esimerkiksi tiimin sisällä ja niin edelleen (Weirich & Sasse, 2001b). Teknisessä näkökulmassa kiinnostavinta on salasanapolitiikat, merkkimäärät ja niissä käytettävät merkit. Salasanakäyttäytymiseen pureutumalla voidaan saada lisää tietoa, että miksi ihmiset käyttävät heikkoja salasanoja ja käyttäytyvät ei-turvallisella tavalla huolimatta siitä, että tiedämme, mikä on hyvän ja huonon salasanan ero (Tam, Glassman & Vandenwauver, 2010).

3.5.1 Sosiaaliset tekijät

Weirichin ja Sassen tutkimuksessa (Weirich & Sasse, 2001a), jossa haastateltiin teknologia-alan työntekijöitä sekä opiskelijoita, löydettiin kuusi asiaa, jotka vaikuttavat salasanakäyttäytymiseen. Identiteettiongelmat, sosiaaliset ongelmat, itsesuojelu, vähättely, vastuuvelvottomuus ja hyvä käytös ilman erillistä syytä.

Identiteettiongelman taustalla oli ajatus siitä, että hyvän salasanakäytännön omaavaa henkilöä voidaan pitää paranoidina, toisaalta osa henkilöistä oli myös ylpeitä siitä, että he eivät ymmärrä tietoturvallisuudesta.

Sosiaalisena ongelmana nähtiin se, että salasanaa jaetaan työkavereille luottamuksen näyttäjänä. Jos salasanaa ei jaeta työkavereille, nähdään se automaattisesti epäluottamuksena toista henkilöä kohtaan. Yhtä lailla voidaan nähdä, että epäluottamus kohdistuu myös esimerkiksi puolisoon tai perheenjäseneen.

Itsesuojelulla tarkoitetaan, että työntekijä kokee olevansa niin vähäarvoinen, että hän ei voi olla hakkerien kohteena vaan hakkerit keskittyvät rikkaisiin ja kuuluisiin henkilöihin. Vähättely taas liittyy siihen, että jos hakkerit pääsisivätkin työasemalle ei siellä ole mitään olennaista tietoa. Samankaltaisen havainnon tekivät myös Adams ja Sasse tutkimuksessaan (Adams & Sasse, 1999).

Vastuuvelvottomuudella kirjoittajat tarkoittavat sitä, että vastaajat ovat tietoisia, että heidän toimintansa ei ole täysin ohjeiden mukaisia, mutta syynä on epärealistiset odotukset ja yleiset käytännöt. Osa kuitenkin koki olevansa vastuussa siitä, jos tietojärjestelmiin päästään käsiksi, koska ovat kirjoittaneet salasanoja ylös paperille.

Viimeisenä asiana löydettiin hyvä käyttäytyminen ilman erityistä syytä. Nämä henkilöt toteuttavat hyvää salasanakäytäntöä huolimatta siitä, että se ei ole tiukasti säädeltyä. Heidän mielestään se ylläpitää ammatillista pätevyyttä sekä pysyvyyttä alalla.

3.5.2 Tekniset tekijät

Organisaatiotasolla suurin käyttäjien salasanakäyttäytymiseen vaikuttava tekijä on jo aiemmin mainitut salasanapolitiikat, sillä ne määrittävät raamit luotavalle salasanalle (Komanduri ym., 2011). Tietohallinnon on hyvä huomioida, millaiset salasanakäytännöt yrityksessä otetaan käyttöön, sillä liian tiukat salasanavaatimukset voivat aiheuttaa turhautumista (Komanduri ym., 2011) ja muita lieveilmiöitä, kuten salasanan kirjoittamista paperille (Adams ym., 1997; Campbell ym., 2011) tai jakamista muille (Campbell ym., 2011). Usein salasanapolitiikat ovatkin jonkinlainen välimuoto turvallisen ja muistettavan salasanan väliltä (Campbell ym., 2011).

Salasanapolitiikkojen merkityksestä kertoo tutkimukset, mistä käy ilmi, että ilman minkäänlaisia salasanavaatimuksia salasanojen merkkipituus on yleisesti alle 8-merkkiä. Tämän lisäksi, johtuen käyttäjien vähäisestä salasanojen murtamiseen liittyvistä tekniikoista, salasanat usein sisältävät sanakirjasanoja tai läheisten nimiä (Adams & Sasse, 1999), sekä vain vähän numeroita tai erikoismerkkejä (Zviran & Haga, 1999). Ilman pakotettua tarvetta on myös harvinaista, että käyttäjä oma-aloitteisesti vaihtaisi salasanansa. Tähän on osasyynä myös palvelujen ja sitä myötä salasanojen ja käyttäjätunnusten suuri määrä. On kuitenkin viitteitä siitä, että palveluihin lisätyt salasanamittarit, etenkin avaavan selityksen kera voi saada käyttäjän parantamaan salasanojensa laatua (Furnell ym., 2018). Eräässä tutkimuksessa myös havaittiin, että edes datan sensitiivisyys, käyttäjän määrittelemänä, ei vaikuttanut salasanojen monimutkaisuuteen tai niiden vaihtoväliin (Zviran & Haga, 1999).

Toisena syynä käyttäjät usein sanovat, että pidemmän ja monimutkaisemman salasanan luominen ja sen käyttäminen vievät työaikaa tärkeämmiltä asioilta. Tämä voi joiltain osin pitää paikkaansa. Eräässä tutkimuksessa havaittiin, että 8-merkkisen rajoitetun salasanan keksimiseen meni jopa kolme kertaa enemmän aikaa, kuin 8-merkkisen rajoittamattoman salasanan. Samaisessa tutkimuksessa ei kuitenkaan havaittu kuin alle kahden sekunnin ero näiden käyttämisessä kirjautumiseen (Proctor ym., 2002). Tutkimuksessa kuitenkin salasanan luomisen ja sen käyttämisen välissä oli vain lyhyt aika, joten pidemmällä aikavälillä tarkasteltuna kompleksinen salasana saattaa olla vaikeampi palauttaa mieleen, kuten tulemme puhumaan seuraavassa osiossa.

3.5.3 Muisti

Sosiaalisten ja teknisten tekijöiden lisäksi ihmisen muisti on merkittävä tekijä puhuttaessa salasanakäyttäytymisestä (Sasse, Brostoff & Weirich, 2001). Juuri muistamiseen liittyvät tekijät määrittelevät osittain käytettäviä salasanapolitiikkoja ja muistaminen vaikuttaa myös arkiseen salasanakäyttäytymiseen. Kun ihminen kokee, että hän ei pysty muistamaan salasanaansa johtaa tämä huonoon salasanakäyttäytymiseen, kuten muistettavamman, mutta ei niin turvallisen salasanan luomiseen (Woods & Siponen, 2019). Mahdollisesti salasana voidaan myös kirjoittaa paperille tai muuhun näkyvälle paikalle ylös. Tämä paperi

taas on usein käyttäjän lähettyvillä kuten näytössä, lompakossa tai muistivihossa, mistä se on helppo löytää tarvittaessa. Tämä lisää luonnollisesti riskiä salasanan joutumisesta vääriin käsiin jo pelkästään olan yli kurkistamalla. Muistamista vaikeuttaa edelleen se, että salasanan lisäksi käyttäjän tulee muistaa myös käyttäjätunnuksensa (Adams & Sasse, 1999).

Muistin ja salasanan yhteydestä on löydetty paljon tutkimustuloksia ja nämä asiat helpottavat myös ihmisen salasanakäyttäytymisen ymmärtämistä. Woods ja Siponen esittävät omassa tutkimuksessaan salasanan muistamiseen liittyvän prosessin. Käyttäjän täytyy ensin opetella uusi salasana, sitten säilyttää se ja lopulta vielä palauttaa se muistista (Woods & Siponen, 2018). Prosessi sinänsä on hyvin yksinkertainen, mutta salasanan muistamiseen liittyen on tiettyjä ihmisen muistiin liittyviä lainalaisuuksia, joita Sasse, Brostoff ja Weirich (2001) esittelevät artikkelissaan

- Työmuistin kapasiteetti on rajoitettu
- Muisti heikkenee ajan myötä, joka johtaa siihen, että ihminen ei pysty muistamaan täydellisesti asioita
- Tutun asian tunnistaminen on helpompaa kuin muistaminen ilman avustavaa tekijää
- Usein käytettyjen asioiden muistaminen on helpompaa kuin harvoin käytettyjen. Paljon käytettyjen asioiden muistaminen tulee myös automaattiseksi.
- Ihminen ei pysty unohtamaan asioita tarpeen mukaan vaan ne pysyvät muistissa, vaikka niitä ei tarvitsisi muistaa
- Merkitykselliset asiat on helpompia muistaa (kuten sanat), kuin merkityksettömät asiat (kuten satunnaiset merkki- ja numerojonot).
- Erillään olevia asioita voidaan käyttää muistamisen tukena. Kuitenkin samantyyppiset asiat voivat sekoittua keskenään.

Edellä olevan listauksen perusteella olisi helposti ajateltavissa, että huonomuistisen henkilön on vaikeampi palauttaa mieleen salasanansa, mutta Woods ja Siponen havaitsivat omassa tutkimuksessaan, että huonomuistisuuden ja salasanan mieleen palauttamisen välillä ei ole välttämättä merkittävää yhteyttä (Woods & Siponen, 2018). Tämän lisäksi salasanojen muistettavuutta on mahdollista kasvattaa ilman että se vaikuttaa salasanan käytettävyyteen (Woods & Siponen, 2019).

Tässä osuudessa kävimme läpi salasanoihin ja salasanakäyttäytymiseen liittyviä tekijöitä. Aineiston perusteella löydettiinkin monenlaisia havaintoja. Käyttäjän käyttäytymiseen vaikuttaa olennaisesti sosiaaliset tekijät, kuten työilmapiiri, henkilöt käsitys itsestään ja motivaatio. Tämän lisäksi siihen vaikuttaa myös tekniset tekijät, kuten salasanan merkkien määrä ja kompleksisuus sekä muistiin liittyvät tekijät, kuten usean salasanan muistaminen ja mieleen palauttaminen. Näihin asioihin on pyritty löytämään ratkaisuja esimerkiksi tiukemmilla salasanapolitiikoilla, joka aiheuttaa kuormitusta ja vastarintaa käyttäjien keskuudessa. Salasanakäyttäytymisen parantamiseen kuitenkin parempi keino

on koulutuksen ja tietoturvatietoisuuden lisääminen (Adams & Sasse, 1999). Toisaalta tällä hetkellä salasanakäyttäytymisen parantamisen sijaan koulutusta tulisi keskittää enemmän MFA:n käyttöönottoon, sillä salasanoista on vaikea saada tarpeeksi turvallisia ja käytännöllisiä yksistään.

4 Empiirinen osuus

Tässä osuudessa käydään läpi tämän tutkimuksen empiirisen tutkimukseen liittyvät tehtävät. Ensimmäisenä käydään läpi laadullisen tutkimuksen taustaa ja miksi se on valittu tämän tutkimuksen menetelmäksi. Tämän jälkeen käydään läpi haastattelumenetelmä ja aineiston keruu. Lopuksi käydään läpi tulokset ja analyysin.

4.1 Laadullinen tutkimus

Tämän tutkimuksen empiirinen osuus tehtiin laadullisena tutkimuksena. Keskeistä laadullisessa tutkimuksessa on tutkittavien kokemukset ja tutkimuksen tarkoituksena on luoda tulkinta kohteena olevasta ilmiöstä. Tällainen tutkimus on aina subjektiivista, sillä tutkija tekee oletuksia oman ymmärryksensä varassa. Laadulliselle tutkimukselle tyypillistä on, että siinä ei välttämättä testata ennalta-asetettua hypoteesia, sen sijaan annetaan enemmän tilaa aineistolle. Kuitenkin tutkijan teoriataustan ja hermeneuttisten periaatteiden vuoksi saattaa alkuperäiset tutkimuskysymykset vaihdella aineistosta löydettyjen havaintojen myötä. (Puusa & Juuti, 2020).

Laadullisessa tutkimuksessa teoria on myös keskeisessä osassa. Kirjallisuusvaiheessa pyritään löytämään tutkimukselle teoreettinen perustelu, mitä ilmiöstä jo tiedetään ja millaiset näkökulmat ovat jääneet vaille huomioita aiemmassa tutkimuksessa. Teoriakatsauksen avulla saadaan käsitys laajasta alueesta käsitteitä, samalla se auttaa tekemään perusteltuja rajauksia ja auttaa päättämään tutkimuksen näkökulmaa, lähestymistapaa ja laajuutta.

Laadullisen tutkimuksen menetelmiä on useita, usein aineistoina kuitenkin käytetään tekstimateriaalia, joka on kirjoitettu luonnollisella kielellä. Tässä tutkimuksessa on aineiston hankintaan käytetty haastatteluita. Tämän lisäksi aiemmasta tutkimuksesta on luotu teoriatausta pohjustamaan tutkimuksen aihetta. Haastattelut sopivat hyvin abstraktien asioiden tutkintaan, sillä se antaa haastattelijalle kohtalaisen paljon vapauksia toteutuksen muodossa. ”Haastatte-

lussa on keskeistä pyrkiä saamaan mahdollisimman paljon tietoa halutusta asiasta ja monipuolinen kuva kiinnostuksen kohteena olevasta ilmiöstä" (Puusa & Juuti, 2020).

Haastattelumenetelmään sisältyy useita rajoitteita. Rajoitteet voivat liittyä esimerkiksi haastattelutilanteen tuomaan paineeseen haastattelijassa/haastateltavassa. Haastateltava voi myös antaa vaikeisiin kysymyksiin sosiaalisesti hyväksyttäviä vastauksia rehellisen vastauksen sijaan. Haastattelija voi myös omalla puheellaan ja sanamuodoillaan vaikuttaa saataviin vastauksiin, tätä kutsutaan reaktiivisuudeksi. Voi myös olla, haastateltava ei ymmärrä haastattelijan kysymystä tai tulkitsee sen väärin. Syynä voi olla esimerkiksi huonosti muotoiltu kysymys tai käytetyt käsitteet ovat liian haastavia haasteltavalle. (Puusa & Juuti, 2020).

4.2 Haastattelut

Haastattelutyyppejä on useita ja tässä haastattelussa sovellettiin puolistrukturoitua ja teemahaastattelua. Kysymykset oli jaettu teemoittain eri lohkoihin, mutta välillä haastateltavat vastailivat jo toisessa osiossa oleviin kysymyksiin. Haastateltavia johdateltiin kertomaan kokemuksiaan monivaiheisesta tunnistautumisesta kysymysten avulla, tavoitteena oli kuitenkin saada haastateltavat keskustelevaan kanssakäymiseen. Ensimmäinen haastateltava (H1) (haastateltavista käytetään tästä eteenpäin merkintää H1-H9) kuvasikin haastattelun jälkeen tilannetta seuraavin sanoin « ...hoiti haastattelun niin et oli lähinnä mukavaa ja ennen kaikkea mielenkiintoista keskustelua asian ympärillä! » Tällä tavalla haastattelijat mahdollisesti avaavat kokemuksiaan enemmän, kuin vastaamalla vain selkeisiin kysymyksiin. Haastateltavien vastauksien perusteella saatettiin tehdä myös lisäkysymyksiä, jotta ilmiötä voidaan tutkia tarkemmin. Osa haastateltavista antoi myös niin hyviä näkökulmia, että ne lisättiin kysymyslistaan seuraavia haastateltavia varten. Jotkin kysymykset myös tuntuivat haastateltavista turhauttavilta, joten ne otettiin lopulta pois tai muutettiin toiseen muotoon. Kaiken kaikkiaan haastatteluihin tuli ensimmäisestä viimeiseen useita pieniä muutoksia, jotta haastatteluista saataisiin mahdollisimman ilmiötä kuvaavia.

4.2.1 Tekninen toteutus

Haastattelut hoidettiin vallitsevan Covid-19 pandemian vuoksi täysin tietokoneen välityksellä. Haastateltavat etsittiin käyttämällä LinkedIn sekä Facebook-verkostoja ja myös suoraan tuttavapiiriä. Varsinaista aikarajaa ei asetettu, mutta haastattelut pyrittiin tekemään kahden viikon sisällä. Sen takia haastateltavia löytyi yhteensä yhdeksän. Muutama henkilö lupautui myös olemaan varahenkilönä, jos tarpeeksi haastateltavia ei löydy. Yhdeksän

haastattelun jälkeen kuitenkin näytti, että uusia merkittäviä näkökulmia ei ole enää tulossa, joten haastattelut päätettiin lopettaa siihen.

Haastatteluiden äänitykseen käytössä oli pääasiassa Skypen kuluttajaversio, yksi haastattelu tehtiin kuitenkin myös käyttäen Discord palvelua. Kaikki äänitettiin sekä ohjelman omalla nauhoituksella, että OBS-studio kaappausohjelmalla, näin saatiin varmistettua, että tallenne tulee varmasti talteen. Skypen etuna voidaan pitää sitä, että se säilyttää videot pilvessä 30 vuorokauden ajan. Tämän lisäksi tallenteet myös siirrettiin toiselle levylle mahdollisen rikkoontumisen vuoksi. Päätoimisena laitteena toimi oma kotikäytössä oleva työpöytä PC, tämän lisäksi varalaitteena oli HP kannettava tietokone. Kahden haastattelun aikana PC jumittuikin, joten varalaite oli otettava käyttöön. Myös varalaitteella oli Skype-ohjelmisto ja OBS-studio. Haastateltavat otti tämän rennosti ja huumorilla ja haastatteluita päästiin jatkamaan vain minuuttien sisällä ongelmien alkamisesta. PC:n lisäksi käytössä oli myös Logitech web-kamera ja HyperX Cloud -headset. Web-kameraa käytettiin, kun se oli mahdollista ja haastateltavalle annetiin mahdollisuus valita haluaako hän käyttää web-kameraa vaiko ei.

4.2.2 Litterointi

Litteroinnissa käytettiin avuksi VLC media player -sovellusta, jolla äänitteet säädettiin 0.4-05x nopeudelle, jolloin se helpotti kirjottamista. Tekstit litteroitiin peruslitterointi tasolla, jolloin ylimääräinen puhe ja äännähdykset sekä täytesanat jätettiin pois. Myös täysin aiheen vierestä mennyt keskustelu jätettiin pois. Kaikkea ei litteroitu sanatarkasti vaan enemmän asiapitoisesti, jos sillä ei ole kysymyksen vastaamisen kannalta merkittävästi vaikutusta. Litteroitu teksti ryhmiteltiin kysymyksittäin omaksi Excel -taulukoksi, jolloin eri vastauksia on helppo tarkastella samanaikaisesti. Kysymysten ollessa valmiiksi teemoittain, helpottaa tämä haastattelujen analysointia ja tulkitsemista.

4.2.3 Haastateltavat

Kuten aiemmin sanottu haastateltavat hankittiin käyttäen LinkedIn ja Facebook -kontakteja sekä tuttavapiiriä, taulukossa 1 näkyy henkilöiden taustatiedot sekä tietoteknisen osaamisen taso sekä laitteiden käyttö päivän aikana. Mahdollisesti omien verkostoitteni takia, tietoteknisen osaamisen taso oli keskimääräistä parempaa ja IT-alalla työskentelevien osuus on kohtalaisen suuri. Tämä voi biasoida, eli vääristää tutkimustulosta. Toisaalta verkostoissani on paljon myös muiden alojen edustajia, joten mahdollisuus on myös siihen, että muut kuin IT-alan henkilöt eivät ole ottaneet käyttöön monivaiheista tunnistautumista. On myös mahdollista, että osa tuttavapiiristäni ei edes tiedä mikä monivaiheinen tunnistautuminen on ja tämän takia jätti vastaamatta kutsuuni, vaikka he käyttäisivätkin monivaiheista tunnistautumista esimerkiksi työpaikalla. Jälkikäteen tarkasteltuna olisi ilmoitusta voinut hieman tarkentaa, sillä esimerkiksi suurin

osa verkkopankeista tarjoaa nykyään jo mahdollisuuden monivaiheiseen tunnistautumiseen.

TAULUKKO 1 Haastateltavien taustatiedot

Sukupuoli	Ikä	Ammatti	Tietotekninen osaaminen	Laitteiden käyttö
H1. Mies	32	Tietoturva-asiantuntija	Kaukana peruskäyttäjästä, mutta ei mestaritason velho	10-14h
H2. Mies	34	Järjestelmäasiantuntija	Peruskäyttäjään verrattuna kohtuullisen hyvä	8-10h
H3. Mies	25	Service Desk employee	Kiitettävä	10h
H4. Mies	25	Insinööriopiskelija	Peruskäyttö helppoa, mutta syväosaaminen puuttuu	6h ja yli
H5. Mies	27	Sovelluskehittäjä	Erittäin hyvä	Jatkuvasti
H6. Mies	24	B2B-myyjä	Normaalia edistyneempi käyttäjä	12–15 h « Silloin kun ei nukuta »
H7. Mies	27	Huoltoinsinööri	Ihan ok, nopea omaksumaan, mutta ei mikään mestari.	Suurin osa valveillaoloajasta
H8. Mies	32	Tietojärjestelmätiede -Opiskelija	Hyvä	12h
H9. Nainen	31	Viestintä- ja markkinointipäällikkö	Hyvä substanssisovellusten osaaminen, mutta yleiset taidot ei niin hyvät.	10h

4.3 Tulokset

Tässä kappaleessa käymme läpi haastattelujen tuloksia niiden teemojen mukaisesti mitä haastattelussa käytettiin. Haastattelun teemat olivat **taustatiedot**, jossa demografisten tekijöiden lisäksi kyseltiin teknologiaosaamista ja innostusta

uusia teknologioita kohtaan. **Autentikointimenetelmät**, jossa kyseltiin salasanojen käyttöä sekä muiden menetelmien käyttöä. **Käyttöönoton tekijät**, missä käytiin läpi käyttöönoton helppoutta sekä itse käyttämistä. **Ongelmat ja riskit** osiossa kysyttiin mahdollisista teknisistä ongelmista mihin on törmätty ja mahdollisten ongelmien varautumiseen. **Turvallisuus** osiossa kyseltiin kokemuksia menetelmän käyttöönoton jälkeisestä turvallisuudentunteesta ja joistain turvallisuustekijöistä. **Muut** kohdassa kysyttiin yleisiä asioita liittyen monivaiheiseen tunnistautumiseen.

4.3.1 Taustatiedot

Taustatiedot on suurimmalta osin esitelty taulukossa 1, henkilöiltä kuitenkin kysyttiin näiden lisäksi myös suhtautumisesta uusiin teknologioihin. Suhtautumista löytyy varauksellisuudesta erittäin myönteiseen. Suurin osa haastateltavista kertoi olevansa ensimmäisten omaksujien joukossa tai ainakin testaavansa uusia teknologioita alkupäässä. Mukaan mahtuu kuitenkin myös henkilöitä, jotka suhtautuvat varauksellisesti uusiin teknologioihin. Kuten taulukosta voidaan todeta, suurin osa haastatelluista pitää omaa tietoteknistä osaamistaan keskimääräistä parempana. Vertailukohtana haastatteluissa käytettiin « tavallista käyttäjää », joka ainakin IT-alalla on yleinen vertailukohta. Ainoastaan henkilö H9 piti omaa osaamistaan « taustajärjestelmien » osalta heikkona, mutta taas työssä käytössä olevien substanssisovellusten osaamista hyvänä. Taulukosta voimme myös nähdä, että laitteiden käyttö on tässä ryhmässä suurta, johtuen osittain tietokoneella tehtävästä työstä, mutta lähes kaikki, henkilöä H9 lukuun ottamatta kertoivat myös käyttävänsä tietoteknisiä laitteita reilusti myös vapaa-ajalla. Täytyy kuitenkin huomioida, että taustatiedot ovat haastateltujen omia arvioita, eikä todellisia lukuja voida näiden perusteella mitata, näillä kysymyksillä haettiin ymmärrystä haastateltavien kiinnostuksesta ja innostuksesta teknologiaa kohtaan.

4.3.2 Autentikointimenetelmät

Tässä osiossa ensimmäisenä kysyttiin haastateltavien salasanoihin liittyvistä tuntemuksista ja niiden turvallisuudesta. Lähtökohtaisesti salasanat herättivät melko negatiivisia tunteita, esimerkiksi H3 ilmaisi asian: « *öö.. Pakollinen paha, yleensä ne aiheuttaa enemmän vaikeuksia kuin hyötyä* ». Toisaalta H7 ilmaisee asian « *Tietyllä tavalla välttämätön paha, mutta hyvä siihen on satsata. Se on semmnonen erusvarma tietoturvan ylläpitotapa. Tai keino pitää omat jutut turvassa*". Salasanojen turvallisuudesta oltiin pitkälti yhtä mieltä, että se on « peruskäyttäjän » näkökulmasta heikkoa. Ongelmiksi mainittiin muun muassa kirjallisuudessakin mainitut salasanojen kierrättäminen, niiden suuri määrä ja muistamisongelmat. Toisaalta 5/9 haastateltavista mainitsi tässä tilanteessa käyttävänsä salasanamanageria salasanojen hallintaan. Haastatellut, jotka ovat ottaneet käyttöön salasanamanagerin olivat salasanojen turvallisuuteen liittyen omalta kohdal-

taan luottavaisempia, kuin henkilöt, jotka eivät maininneet salasanamanagerista.

Seuraava kysymys oli salasanakäyttäytymisestä. Salasanamanagereita käyttävät haastateltavat luonnollisesti pitivät omaa salasanakäyttäytymistään hyvänä ja salasanamanageria onkin käytetty salasanojen säilytyksen lisäksi salasanageneraattorina, jolloin salasanat ovat pitkiä ja monimutkaisia. Muitakin ominaisuuksia pidettiin hyvinä, kuten H9 ilmaisi "*Ja tuo lastpassihan on sellanen, et se herjaa, jos on huonoja tai päällekkäisiä salasanoja. Se tavallaan niinkun tsemppaa parempaan suuntaan*". Noin puolet haastatelluista kuitenkin kertoi, että käyttävät vakiosalasanaa tai samankaltaista salasanaa useassa paikassa. Erikoispiirteenä H1 piti omaa salasanakäyttäytymistään tärkeänä ammatillisen velvoitteen takia;

> …Et jos mä käyn saarnaamassa eteenpäin, et pitäis varmaan itekki tehä samalla lailla, kun sanoo

Muista autentikointimenetelmistä käytössä oli yleisimmin biometriset tunnisteet ja erilaiset tunnistautumissovellukset. Biometrisistä tunnisteista käytössä on sormenjälkitunnistus sekä FaceID-kasvontunnistus, jota käytetään etenkin puhelimen kanssa. Yksi henkilö myös mainitsi aiemmin käyttäneensä token-avaimenperää, mutta vaihtaneensa sen myöhemmin puhelinsovellukseen. Töissä käyvistä kaikki kertoivat käyttävänsä MFA:ta ainakin joissain työhön liittyvissä palveluissa. Kellään ei ollut kuitenkaan Windowsiin kirjautuessa kaksivaiheista tunnistautumista käytössä. Useissa työpaikoissa oli käytössä myös SSO, joten autentikaattorin tarve on vähäinen, jos kirjaudutaan aina samalta laitteelta tuttuihin palveluihin. Suuri osa oli ottanut MFA:n käyttöön omasta valinnastaan myös vapaa-ajalla ja osa kertoi, että töistä saatu oppi oli siirtynyt käyttöön myös vapaa-ajalla, etenkin salasanamanagerien osalta. Vain H9 kertoi, että ei käytä MFA:ta ollenkaan vapaa-ajalla, lukuun ottamatta verkkopankin mobiilitunnistautumista.

Viimeisenä kohtana tässä osiossa vielä kysyttiin, onko haastateltavat saanut suosituksia lähipiiriltään tai onko tapahtunut tietoturvarikkomusta, mitkä olisi vaikuttanut käyttöönottoon. Haastateltavista kukaan ei muistanut saaneensa suosituksia läheiseltään, ainakaan merkittävässä määrin. Yleisemmäksi käyttöönoton syyksi mainittiinkin palvelun ehdotus käyttöönottoon. Haastateltavat oli myös suurimmalta osin sitä mieltä, että jos palvelu ei suosittelisi käyttöönottoa niin käyttöönotto jäisi tekemättä tai ainakin viivästyisi. Myöskään lähipiirille sattuneesta tietoturvarikkomuksesta ei kukaan ollut saanut lisävauhtia käyttöönottoon.

4.3.3 Käyttöönoton ja käytettävyys

Kaksivaiheisen tunnistautumisen käyttöönottoa kaikki piti helppona, mutta ei välttämättä yksinkertaisena. Vain H9 oli saanut koulutuksen käyttöönottoon edustamansa yrityksen puolesta. Hän kokikin, että koulutuksesta oli suuri apu käyttöönotossa. Käyttöönotossa ei myöskään havaittu juurikaan ongelmia, on-

gelmat liittyivät ennemmin autentikointiin käytettävän laitteen vaihtamiseen, johon ei ollut varauduttu etukäteen.

Itse käytettävyydessä nousi esiin joitain pieniä ongelmia, mutta kukaan ei kokenut niitä ylitsepääsemättömiksi vaikeuksiksi, turhautuneisuutta se kuitenkin on herättänyt. H3 antoi esimerkin, missä työn puolesta on MFA:n poistaminen käytöstä voinut ottaa jopa useita kuukausia. H8 taas koki sähköpostin kautta klikattavaa linkkiä vaivalloiseksi ja mainitsikin lopuksi, että saattaisi jättää ottamatta käyttöön MFA:n, joka käyttää tuota menetelmää. Lisäksi hän oli havainnut ongelman, jos autentikointipyyntö tulee useaan laitteeseen niin se ei synkronoidu muiden laitteiden kanssa automaattisesti. Ilmoitus kirjautumisesta siis voi jäädä toiselle laitteelle, vaikka se on jo hyväksytty toisella. H9 mielestä käytettävyys on tehty niin helpoksi kuin se voi olla, mutta kertoi myös, että ongelmatilanteet « ottavat päästä ».

4.3.4 Riskit

Riskiosiossa kysyttiin muita kuin käyttöönotossa ja käytettävyydessä koetut ongelmia ja niihin varautumista. Ensimmäisenä kysyttiin, onko autentikointiin käytettävä laite unohtunut ja mitä seurauksia siitä oli. Unohduksia oli tapahtunut vain vähän, mutta esimerkiksi laitteen rikkoontumisia oli tapahtunut. Haastateltavat, joille tällainen oli tapahtunut, olikin sittemmin paremmin varautunut tulevaa varten esimerkiksi pitämällä varalaitetta, johon on myös asennettu autentikaattorisovellus tai kirjaamalla autentikaattorin palautukseen käytettävän koodin ylös. Kuitenkin suurin osa ei ole varautunut siihen, että autentikointiin käytettävä laite rikkoontuu tai katoaa, eikä kaikki edes välttämättä tiedä kuinka siinä tilanteessa tulisi toimia. Kaikki käyttivät autentikointiin puhelinta, joka kulkee suurimmalta osin aina mukana, joten sen katoamista tai rikkoontumista ei pidetty suurena riskinä.

Haastateltavilta kysyttiin myös, onko kirjautuminen estynyt teknisen vian takia ja näitä ei ole juurikaan havaittu. H6 mainitsikin, että

> kaksivaiheinen tunnistautuminen on toiminut ihan uskomattoman hyvin.

Osa kuitenkin mainitsi, että välillä autentikaattori ole hyväksynyt käytettyä koodia tai se on jouduttu avaamaan uudelleen.

4.3.5 Turvallisuus

Haastateltavilta kysyttiin, kokevatko he nyt olevansa enemmän turvassa kuin ennen. Vastaukset olivat suurimmalta osin myönteisiä, mutta esimerkiksi H1 koki olonsa edelleen turvattomaksi, mutta kuitenkin turvallisemmaksi kuin ennen MFA:n käyttöönottoa. H9 myös mainitsi, että turvallisuuden tunne ei tule vaan itselle vaan myös ympärillä oleville.

Haastattelussa kysyttiin myös, onko haastateltavat saaneet viestejä oudosta kirjautumisesta ja mitä he tekivät. Osalle tällaisia ilmoituksia oli tullut ja sen

seurauksena ainakin osa oli vaihtanut salasana. Silloin nämä viestit on katsottu tarkkaan ja selvitetty onko niiden alkuperä mahdollisesti jossain omassa laitteessa. Osa taas kertoi, että sen jälkeen, kun on ottanut MFA:n käyttöön ei ole enää tullut ilmoituksia.

Seuraavaksi kysyttiin, onko tietoturvatietoisuus lisääntynyt tai onko MFA:n käyttöönotto vaikuttanut muuhun tietoturvakäyttäytymiseen. Haasteltavien vastauksista saa käsityksen, että se ei ole juurikaan vaikuttanut suuntaan eikä toiseen, mutta kynnys ottaa MFA muuallakin käyttöön on madaltunut. H6 vastasi oivallisesti « ...*Mun mielestä tämmösen toimintamallin käyttäminen viestii enemmän siitä tietoisuudesta kuin lisää tietoisuutta* ». Tähän liittyen haastateltavilta myös kysyttiin käyttävätkö he samaa salasanaa palveluissa, jossa on käytössä MFA ja palveluissa, joissa sitä ei ole. Suurin osa kertoi käyttävänsä eri salasanoja, yleensä salasanamanagerin avustavana, mutta H4 ja H7 ilmoittivat käyttävänsä samaa salasanaa useissa paikoissa.

Viimeisenä kysyttiin vielä, ottaisivatko haastateltavat MFA:n käyttöön palveluissa, joissa se ei ole vielä mahdollista. Suurin osa kertoi, että ottaisivat käyttöön, etenkin jos sen käyttö on yksinkertainen, kuten vaikkapa push-notifikaatio puhelimeen. Jos taas käyttöönotto tai käytettävyys on monimutkaisempi niin kynnys on suurempi. H6 ja H9 myös epäilivät MFA:n tarpeellisuutta joissakin palveluissa.

4.3.6 Muut

Muut osiossa oli tarkoitus kysyä suosituksia ja yleistä mielikuvaa MFA:n käytöstä. Koska haastateltavien joukko oli suurimmalta osin IT-alan ammattilaisia niin kysymys jätettiin pois. H9 ollessa eri toimialalta kysymys kuitenkin hänelle esitettiin. Hän oli sitä mieltä, että käyttö voi olla turhauttavaa, jos sille ei anneta kunnollista syytä. Käyttöönotossa hän koki työpaikan tarjoaman koulutuksen hyödylliseksi.

Tässä osiossa kävimme läpi haastattelun tulokset pääpiirteittäin. Tulokset olivat melko lailla odotettuja, mutta myös joitain odottamattomia vastauksia tuli vastaan, joita käsittelemme paremmin analyysiosiossa.

5 Analyysi ja johtopäätökset

Tässä kappaleessa käymme läpi tulokset ja teemme niistä analyysia hyödyntäen aiempaa kirjallisuutta. Koska MFA on edelleen vahvasti sidonnainen salasanoihin, peilataan analyysi vaiheessakin näitä kahta keskenään soveltuvin osin. MFA on vielä kohtalaisen tuore asia, vaikkakin sen on ollut useilla palveluntarjoajilla käytössä jo varmasti yli 10-vuotta. MFA kuitenkin käsitteenä voi olla muille, kuin IT-alalla työskenteleville tai aktiivisesti tietotekniikkaa käyttäville outo, joka tuli esiin myös tutkimuksen haastateltavia etsiessä. Tämän voidaan nähdä vaikuttaneen haastattelun tuloksiin, sillä haastateltaviksi valikoitui pitkälti IT-alalla työskenteleviä henkilöitä tai muuten aktiivisesti laitteiden käyttöä harrastavia henkilöitä. Ainoastaan yksi haastateltavista (H9) ei työn ulkopuolella käytä aktiivisesti tietoteknisiä välineitä.

Analyysissa käytetään hyödyksi teemoittelua, joka oli luonnollinen valinta, kun haastattelut oli jaettu valmiiksi teemoihin. Haastattelun teemat käytiin jo tulos osuudessa lävitse, joten niitä ei tässä enää tarkenneta. Analyysin tarkoituksena on tulkita käyttäjien vastauksia ja löytää vastaukset tutkimuskysymyksiin, jotka olivat seuraavanlaiset

- Mitkä olivat MFA:n käyttöönoton syyt?
- Minkälaisia kokemuksia MFA:n käytöstä on?

MFA on tutkimuksen kohteena vielä suhteellisen tuore, eikä sen käyttöä tai käyttöönottoa olla vielä suurissa määrin tutkittu, kuten esimerkiksi salasanoihin liittyvää käyttäytymistä. Tämän takia tutkimuskysymykset jätettiin melko avoimiksi, sillä itse ilmiöön haluttiin perehtyä useista näkökulmista katsottuna. Koska salasana käyttäytyminen on niin läheinen ilmiö MFA:n käytön kanssa, haluttiin sitäkin sisällyttää tutkimukseen. Seuraavaksi käymme tulokset ja niiden analyysin läpi teemakohtaisesti, kuten tulos osiossakin.

5.1 Taustatiedot

Kuten jo todettu taustatiedoista paljastuu, että haastatellut on pääasiassa IT-alan ammattilaisia tai ainakin harrastelijoita. Kaikki haastateltavat olivat korkeakoulutettuja tai kävivät korkeakoulua parhaimmillaan. Haastateltavat myös piti omaa osaamistaan keskimääräistä parempana yhtä (H9) lukuun ottamatta. Henkilöt myös käyttävät laitteita kohtalaisen runsaasti, osa jopa kaiken aikaa nukkumisen ulkopuolella. Vähiten laitteita käyttää H9, joka kertoi käyttävänsä lähinnä työaikana tietotekniikkaa säännöllisesti. Kaiken kaikkiaan H9 toimii hyvänä verrokkina muille, ammattimaisemmin tietotekniikkaa käyttäville henkilöille. Kokonaisuutena H9 vaikuttaakin niin sanotulta « tavalliselta käyttäjältä ». Tutkimuksen kannalta tällaisia henkilöitä olisi suonut olevan enemmän, jotta tulokset koskettaisivat laajempaa ihmisryhmää. Yksi tutkimuksen tarkoitus kuitenkin oli tutkia, voisiko MFA soveltua laajalle käyttäjäkunnalle, sillä salasanat yksinään ovat riittämätön tunnistautumisen keino. Tähän ongelmaan kuitenkin voidaan osaltaan vastata myös niiden vastausten osalta mitä saatiin ja katsomalla niitä käyttöönottoteoriaan peilaamalla.

Taustatietojen perusteella voimme ainakin todeta, että nuoret aikuiset henkilöt käyttävät aktiivisesti MFA-lisäsuojausta, joskin taustat voivat vaikuttaa käyttöönottoon myös jonkin verran. Haastatellut henkilöt olivat suurimmalta osalta myönteisiä uusia teknologioita kohtaan, mikä on luultavasti edesauttanut myös MFA:n käyttöönottoa.

5.2 Autentikointimenetelmät

Haastateltavilta kysyttiin heidän suhtautumistaan salasanoihin ja heidän salasanakäyttäytymisestään. Salasanoihin kohdistui lähtökohtaisesti negatiivisia tunteita, kuten turhautumista ja muistamisongelmia.

> Ja miten niinku normaalit, ei tekniset ihmiset. Niin se on niinku yks suurin tietoturvaheikkouksista ja haavoittuvuuksista. Osuu peruskäyttäjään yritystasolla ja käyttäjätasolla. Koko internet on rikki siltä osin, että ihmiset uudelleen käyttää salasanoja. Se on sellainen asia, jonka täytyy jotenkin muuttuu ja miten mä sen nään niin se ei tuu muuttuun. Hyvin epätodennäköisesti kaikki ihmiset ottais käyttöön salasanamanagereita. Suhde salasanoihin on se, että niistä pitäis luopua, ja pitäis siirtää malliin missä voidaan tunnistautua. -*H1*.

> Viha-rakkaussuhde. Just eilen kiroilin taas yhden palvelun kanssa missä olin vaihtamassa salasanaa ja sitten salasanamanagerilla generoin pitkän hyvän salasanan erikoismerkkeineen ja muineen niin sitten palvelu sanoi, että maksimi 20 merkkiä. Et siis niinku. Salasana on turvallinen kuin niitä käyttää oikein. -*H2*.

> Onhan se niiden muistaminen välillä haaste. Mutta mä oon oikeestaan delegoinu sen nykyään salasanamanageriin. -H3no siis se on yks sana, joka sun pitää muistaa, mutta monestihan niitä joutuu vaihtelemaan sitä mä niinku vihaan et mä joudun opette-

> lemaan jonku salasanan uudelleen. Mieluummin käytän niinku maailmantappiin asti sitä vanhaa salasanaa. -*H4*.

Suurin osa kuitenkin tästä huolimatta toteuttaa hyvää salasanakäyttäytymistä, johon salasanamanagerit ovat olleet suuri apu. Salasanamanagerien käyttö oli huomattavan korkea tässä haastatteluryhmässä, sillä yhden aiemman tutkimuksen mukaan vain 6 % kyselyyn vastanneista käytti salasanamanageria (Das, Bonneau, Caesar, Borisov & Wang, 2014). Salasanojen tietoturvaa ei pidetty vakuuttavana, etenkään « Tavallisen käyttäjän » osalta. Osa kuitenkin oli sitä mieltä, että oikein käytettynä, kuten salasanamanagerin ja salasanageneraattorin kanssa ne tuovat kuitenkin riittävää turvaa. Tutkimuksessa olikin löydettävissä yhteys hyvän salasanakäyttäytymisen ja MFA:n aktiivisen käytön kanssa. Esimerkiksi H1, H5 toteuttavat erittäin hyvää salasanakäyttäytymistä ja myös käyttävät MFA:ta aktiivisesti lähes kaikkialla. Henkilöt, jotka eivät toteuta niin hyvää salasanakäyttäytymistä, kuten H4 ja H7 ei myöskään käyttänyt niin aktiivisesti MFA:ta vaan lähinnä satunnaisissa palveluissa. Salasanoihin liittyen myös saatettiin kokea ammatillista velvoitetta hyvää salasanakäyttäytymistä kohtaan. Etenkin H1 koki jonkinlaista painetta hyvää salasanakäyttäytymistä kohtaan, koska käy itse asiakkaille puhumassa näistä asioista.

Muista autentikointimenetelmistä suosittuja olivat biometriset tunnisteet, kuten sormenjälki ja kasvojen tunnistus. Kasvojen tunnistusta käyttivät kolme haastateltavaa. Samaiset henkilöt noudattivat muutoinkin parempaa tietoturvakäyttäytymistä. Kasvojentunnistuksen käyttö tunnistautumisen olikin yllättävä tulos tässä tutkimuksessa. Teknologia on vielä kohtalaisen tuore, joten sen soveltuvuutta muutoinkin kuin mobiililaitteissa olisi varmasti hyvä tutkimuksen aihe.

Haastateltavien joukosta 7/9 oli ottanut MFA:n käyttöön itsenäisesti arkielämässään. H9 taas kertoi käyttävänsä MFA:ta vain työn puolesta. Kysyttäessä miksei hän käytä sitä myös arkielämässään saatiin vastaus:

> Mä en kauheesti oikeen keksi, että missä mä sitä käyttäisin. Jotenki mun sovellusten ja tietotekniikan käyttö menee niin tänne työn puolelle. -*H9*.

Edellä olevan vastauksen perusteella voitaisiin päätellä, että lähinnä töissä tietotekniikkaa käyttävät henkilöt eivät ole niin valveutuneita turvallisuusasioista, kuin IT:tä myös vapaa-ajalla käyttävät henkilöt. Useilla haastatelluilla ensimmäinen MFA:n käyttö liittyikin johonkin pelikirjasto-sovellukseen, kuten Steam, Battle.net tai Uplay. Moni perustelikin näitä valintojaan sillä, että niissä voi olla rahallista omaisuutta tai tuhansia käytettyjä tunteja takana, joten niiden menettäminen olisi erittäin ikävää ja taloudellisesti rasittavaa.

H6 kertoi, että oli alkanut aluksi käyttämään MFA:ta töissä, mutta sitten siirtynyt käyttämään sitä myös arjessa. Hän myös käytti MFA:ta hieman erilailla, kuin muut, sillä hän ei ole ottanut MFA:ta käyttöön itse palveluissa vaan hänellä on se käytössä salasanamanagerissa, joten päästäkseen käsiksi omiin salasanoihinsa hän tarvitsee ensin MFA tunnistautumisen.

Yksi ennakko-oletus tutkimusta tehdessä oli, että henkilöille olisi lähipiirissä tapahtunut jokin tietoturvapoikkeama tai muuten, joku olisi heille suositellut käyttöönottoa, mutta näin ei ollut kenenkään kohdalla. Työn ja lähipiirin ollessa suuri vaikuttaja uuden teknologian käyttöönotossa, oli tämän tutkimuksen tulos yllättävä ja luulenkin että henkilöiden taustat ovat tässä vaikuttaneet asiaan. Suurin osa haastatelluista kertoikin, että olivat ottaneet MFA:n käyttöön luultavasti syystä, että palvelu itse tarjosi käyttöönottoa ja haastateltavat halusi parantaa turvallisuuttaan näissä palveluissa. Haastateltavat olivat myös sitä mieltä, että MFA otetaan helpommin käyttöön, jos palvelu tarjoaa sitä jo rekisteröitymisvaiheessa, muutoin se saattaa jäädä ottamatta käyttöön kokonaan tai ainakin viivästyy. Palveluntarjoajilla voikin olla suuri vaikutus siihen, otetaanko MFA laajasti käyttöön käyttäjien keskuudessa vai ei.

5.3 Käyttöönotto ja käytettävyys sekä ongelmat ja riskit

Tutkimuksessani havaittiin, että käyttöönotto oli suurimmalle osalle helppoa. Haastateltavat kokivat, että palvelut tarjosivat riittävän ohjeistuksen käyttöönottoon tai löysivät ohjeistuksen käyttöönottoon jonkun muun palvelun kautta helposti, joskin toiset palvelut ovat toimineet toista paremmin, kuten oheisista kommenteista voidaan nähdä.

> En muista sinne asti, mutta siis mä oon aika varma, että mä oon kattonu jonku youtubevideon koska se on tosi perust kuinka mä otan uusia asioita käyttöön, et mä katon jonku videon mistä näkee "how does it work". Se on vaan helppoa ottaa sillai käyttöön. -*H1.*

> Nekin on ollu vähän niinku palveluntarjoajakohtaisia. Microsoft tuotteiden kaa on ollu vähän jonkinlaista säätöä, esimerkiksi blizzard ja gmail on mennyt aika nätisti. Niissä ei oo ollu mitään. -*H2.*

> Microsoft ympäristössä tosi kätevä. Käytetään msa-autentikaattoria niin se on helppo. -*H3.*

> Se oli simppeliä. Naputella vaan. Töissä se ei ollu mun tehtävä laittaa, että se vaan aktivoitiin. Mutta mitä ite oon käyttäny niin se on tehny niin helpoksi, kuten kuluttajasovellukselta odottaa. Ja käyttäminen on yksinkertaista. -*H7.*

> Muistaakseni opasti, käyttöönotot ollu aika iisejä, että palvelut on aika step-by-step on opastanut, kuinka se aktivoidaan ja mitä tietoja tarvii lisätä jne. -*H8.*

Kaksi haastateltavista kuitenkin oli sitä mieltä, että käyttöönotto, etenkin vähemmän asioihin perehtyneiden osalta tulisi aloittaa kouluttamisesta, että mihin me tarvitsemme MFA:ta ja kuinka sitä käytetään, tähän antaa tukensa myös tutkimustieto (Furnell ym., 2018):

> Tota, mä koen et se on aika helppo, kun sul on se appi puhelimessa ja tiiät mitä sä oot tekemässä. Eli kun sä otat sen käyttöön niin sä avaat puhelimen skannaat qr-koodin sen jälkeen syötät seuraavan vapaan numeron ja painat ok. niinku mun mielestä se on sillai tosi nopee ja suoraviivainen mut sit jos mun pitäis ensin opiskella et mikä tää juttu on, miten sitä käytetään, mistä mä saan tän puhelimeen, miks näin pitää tehä niin se polku tavallaan on liian pitkä sinne asti, et en mä sitä rekisteröitymisvaiheessa jaksais tehä jos ei se ois mulle tiedossa. Et tavallaan se on niinkun aika moni tekee silla et ne ottaa sen käyttöön kerran ja sit ne ottaa sen käyttöön mones paikas, mut jos sitä ei oteta ekan kerran käyttöön niin ei sitä varmaan oteta juurikaan. -*H1.*

> Se ehkä vaatii ymmärryksen aiheesta, että sillä löytyy halu ottaa se käyttöön. Se semmonen ymmärryttäminen tämmösissä tietoturvajutuissa on tosi tärkeetä. Ja ymmärrän että se saattaa välissä tuntua turhalta, mutta sitten pitää muistuttaa syistä siellä takana. -*H2.*

Haastateltavat myös mielellään käyttäisi MFA:ta myös paikoissa, missä se ei ole vielä mahdollista.

> Kaikkialla missä on mahdollista. -*H1.*

> On semmosia missä käyttäisin mieluusti autentikaattoria, mutta niihin ei saa kuin käyttäjätunnuksen ja salasanan. -*H2.*

> Kyllä sen hyvinkin palveluun ottais käyttöön missä mahdollisuus olis. -*H5.*

> Kyllä ehkä joissain vois. Etenki jos on palvelu, jossa käytetään maksukorttitietoja tai vastaavaa, kun kaikissa ei kuitenkaan oo. Yleensä kuitenkin käytän luottokorttia ja jos jotain tapahtuu, niin se menee yleensä luottoyhtiön tappioksi. Et ei se ny maailmaa kaada, jos niis palveluis ei oo, mutta kyllähän se päänvaivaa aiheuttaa. -*H8.*

Esteenä käyttöönotolle voisi kuitenkin olla sen hyödyllisyys tai jopa minkä tyyppinen MFA on kyseessä:

> Paino tolla sanalla, että jos se on helppoa, et kyllä mä sitä käyttäisin. Jos se voisi olla niinkin yksinkertainen kuin paina puhelimella nappia accept nyt niin sitä käyttäisin niin monessa paikkaa kuin on mahdollista. Kokisinko mä sen tarpeelliseksi kovin moneen paikkaan, niin en välttämättä. Mutta jos se on helppoa niin miksi ei. -*H6.*

> Kyllä sillee jos sen sais nopeasti ja helposti. Ei muutaku raksi ruutuun ja tulee viesti. Mutta jos ei tarvis mitään erillistä sellasta, ehkä se helppous et kuinka helposti sen sais. Et esimerkiks sellanen missä tulee vaan viesti, niin se tuntuu vaivattomalta ottaa käyttöön. Ja mikä gmailissa on semmonen ilmotus mikä tulee näytön yläreunaan. -*H7.*

> Kyllä mä voisin käyttää. Mutta jos mä esim. kerran vuodessa käyttäisin niin en tiiä jaksaisinko. Et varmaan vähän semmonen palvelun käytön useus on semmonen määrittävä tekijä siinä. -*H9.*

Kuten edellä mainituista voimme huomata, ei käyttöönotto ole ollut varsinaisesti hankalaa, eikä siihen ole sisältynyt juurikaan ongelmia. Jonkin tyyppisiä MFA-järjestelmiä, kuten sähköpostitunnistautumista, kuitenkin pidettiin turhauttavana, jolloin sen käytön aloittamista voidaan miettiä kahdesti. Myös harvoin käytetyissä, tai niin sanotusti « turhissa » palveluissa, kuten satunnaisen foorumin kohdalla ei MFA:ta nähty tarpeellisena. Vaikuttaakin, että MFA:n helppous ja sen koettu tarpeellisuus vaikuttavat osaltaan käyttöönottoon henkilöillä, jotka eivät muutoin ole niin tietoturvatietoisia.

Vaikka itse käyttöönotossa ei juurikaan havaittu ongelmia niin ongelmia kuitenkin esiintyi, jos autentikointiin käytettävää laitetta piti vaihtaa esimerkiksi rikkoontumisen seurauksena.

> öö, siis isoin ongelma siihen liittyen on ollu se et siis mun puhelin hajos ja tota se on sellainen ongelma, jonka mä oon kokenu eniten hankalaks, et sitte kun se puhelin hajoo niin sun kaikki tokenit on siellä, niin sä oot periaattees niinku lukittu ulos. Toki mulla on varakoodit saatavilla salasanamanageris, mutta sinnekin tarvii 2FA:n, mut sitte saatatki joutua tilanteeseen missä lukitset itsesi ulos… -*H1.*

> se ei varmaan ollu ensi käyttöönotto vaan yritettiin vaihtaa puhelinnumeroa. Et autentikointi ollu numeroon x ja sit oli vaihtunu puhelinnumero ja sit yritettiin siirtää se, niin siinä on tullu hämminkiä useamminkin. Mun mielestäni ohjeet ei ollut kovin hyvät, josta syystä se lähetti vahvistuksia vielä vanhaan numeroon jne. -*H2.*

> Unohduksia ei oo, mutta puhelin hajos kerran, kun oli vielä google authenticator käytössä. Sieltä oli pieni työmaa selvittää. Sillon oli 3–4 palvelua sen takana. Ei se ihan hirveen helppo ollu nollata. Just ongelma, ettei pysty olla kahella laitteella. Jos laite häviää tai varastetaan niin ei oo sitte pelkästään sen varassa. Henkilökohtaisista jutuista nyt selviää, mutta kun on todella kriittisiä työjuttuja, jos pitää mennä hetkessä korjaamaan tai pysäyttämään joku palvelu niin, jos siihen ei pääse niin ois aika paha. -*H5.*

Autentikointiin käytettävän laitteen rikkoontuminen tai katoaminen voikin olla piinallinen prosessi, jos siihen ei ole osannut varautua millään tavalla. Haastateltavilta kysyttiinkin heidän valmiuksiaan laitteen rikkoontumiselle ja/tai katoamiselle. Kukaan haastateltavista ei ole/ollut varautunut laitteen rikkoontumiseen tai katoamiseen, ainakaan ennen ensimmäistä henkilökohtaista tapausta. Haastatelluilla oli kuitenkin hyvin tiedossa, että työpuhelin voidaan tyhjätä myös etätyökaluja käyttäen, joten riski on ennemmin henkilökohtaisen puhelimen osalta.

> En kyllä oo mitenkään varautunut siihen nyt kun kysyit. Mutta toimenpiteet tiedän mitä pitää tehä. Tai lähinnä omassa tilanteessa kun on työsuhdepuhelin niin nuo työhommat on semmosia. Toki ne on hyvin suojattu firman politiikkojen mukaan, mutta jos ois jääny vaikka näytönlukitus pois ja joku on sen pölliny niin tiiän kyllä kuinka pitäisi sillon toimia. -*H2.*

> Hyvä kysymys. En mä välttämättä oo. -*H3.*

> Kyllä ja ei. Koodin oon aikanaan ottanu ja tiedän miten se pitää palauttaa, mutta en tiedä onko mulla sitä koodia(autentikaattoriin). Mun mielestä siihen (verkkopankki) voi edelleen kirjautua, mulla on siis edelleen olemassa se avainlukulista, et sä saat valita, käytätkö sä mobiilitunnistautumista tai avainlukulistaa. -*H4.*

> Joo, meillä firman puhelimet on kaikki etäwipettavissa ja tällee kontrolloitavissa, että siinä tapauksessa meidän ICT:hen yhteydenotto ja se hoituu sitä kautta. Uskoisin tietäväni. Joo, öö, lastpassin salasanan olen joskus unohtanut, mutta sen olen pystynyt palauttamaan. Elikkä tota siinä tapauksessa en usko, että välttämättä olis ongelmaa. Toisaalta en tiiä miten sitten, jos se puhelin ei olisi jostain syystä käytössä enää. Et se faktori siitä puuttuu. En ole vielä tähän tilanteeseen joutunut, en tiiä miten siinä tapauksessa sitten toimis. Eli en ole varautunut siihen. Pankin kanssa sai numerokoodiliuskan kautta hoidettua uuden appin asentamisen. -*H5.*

> Näiden omien nettipankkien kanssa kyllä, et mun tunnuslukulaput tallessa, että niillä pystyy sen sitten välttämään, mutta työpuhelimeen ei oo tietysti. Töissä on sen kautta helppoa, että pystyy ottaa ATK:hen yhteyden, että ne pystyy tekee loitsut. -*H6.*

> No.. äää.. Täytyy sanoa, että en nyt mitenkään hirveen hyvin. Mulla on kyllä joitain palveluita varten on tommonen vanha varaluuri, missä on samat tilit ja muistaakseni myös autentikointipalvelutkin kyllä. Sit no pankkiasioinnin puolesta oon varautunu siihen et se on toisella laitteella myös linkattu se autentikointi. Mutta sit jos ei ois mitään noista laitteista, jos vaikka kävis niin että kaikki hajois tai häviäis niin sitte en kyllä tiedä mitä tekisin tai mitä pitäis tehdä. -*H7.*

> Tiedän, että meillä on käytössä intunen laitehallinta, joka varmaan auttaa siinä tilanteessa jos näin kävisi. Ja se on myös tavallaan kun meillä on niin hyvä IT-osasto tuolla niin tiedän että tälläset jutut meillä on siellä käytössä niin jos näin kävis niin ne sais ne oikeudet pois sieltä puhelimesta. -*H8.*

Henkilökohtaisen laitteen rikkoontumiseen tai katoamiseen tulisikin varautua paremmin, jos tällainen tilanne tapahtuu, vaikka ulkomailla ollessa, eikä siihen ole varautunut voi ongelmia syntyä esimerkiksi maksusuoritteen aikana. Osa pankeista voi vaatia nykyään myös esimerkiksi puhelintunnistautumisen maksun yhteydessä, eikä silloin esimerkiksi avainlukulista riitä maksun suorittamiseen. Haastateltavien äänestä pystyi kyllä tulkitsemaan, että varautumiseen tulisi panostaa enemmän ja osa oli jopa vähän hämmentyneitä kysymyksestä.

Huomattavasti vähäpätöisempi, mutta mahdollinen ongelma on myös autentikointiin käytettävän laitteen unohtuminen. Tämä on etenkin työtä ajatellen mahdollinen. Haastateltavista vain kaksi oli unohtanut autentikointilaitteen paikkaan, missä se ei ollut käytettävissä, kun oli tarve. Seuraamukset kuitenkin olivat pieniä:

> Toissa viikolla piti kirjautua työsähköpostiin, mutta puhelin oli töissä, joten se jäi sitte tekemättä. Mä lähin sitte käymään hakemaan puhelimen seuraavana päivänä, ettei ollu niin akuutti asia. Periaatteessa ois voinu olla mahollisuus pyytää jotain työkaveria käydä kattoo se koodi. -*H7.*

> Onkohan käyny ihan kerran tai kaks jossain asiassa sillä lailla. Mutta jotenkin se puhelin kulkee niin hyvin siinä mukana. Pari kertaa on ollu semmonen et oon hoksan-

> nu etten mä voikkaan tehä sitä kun mulla ei oo puhelinta. Ei siitä varmaan muistaakseni aiheutunu vakavaa haittaa. Kerran mä tein niin et soitin miehelleni, että voitko painella tämmöstä ja tämmöstä numeroa tai jotain. *-H9.*

Muut olivatkin sitä mieltä, että puhelin on niin henkilökohtainen esine, että se pysyy yleensä aina mukana. Osalle se on myös lähes tärkein työväline, joka edesauttaa sen mukana pitämistä.

> …mut ei oo ollu tilannetta et oisin ollu eri paikas kun tuo puhelin, kun puhelin on niin pultattu ihmiseen, jos sulla ei oo sitä saatavilla niin sä kyl käyt hakemassa sen ihan sama missä se on, niin mahollisimman nopeasti siihen, et se tavallaan on niin tärkeä työväline. *-H1.*

> ei ole puhelin jäänyt kotia. Työsuhdepuhelin, joka on myös henk. koht. puhelin niin on entistä skarpimpi pitämään se tallessa. *-H2.*

> En ole ikinä unohtanut työpuhelinta. Mun työhön puhelin liittyy niin olennaisesti et sitä on niin vaikea unohtaa, tai sit pitäis kotia palata joka tapauksessa. Puhelin on melkeen yhtä tärkeä kuin se läppäri on. Ettei oo tämmöstä päässy vielä käymään. Toki jos tää olis joku fyysinen tokenin anto laite, niin sellainen saattais kadota tai hukkua helpommin. Puhelin on kans siitä kätevä, että siihen pystyy aina soittamaan. *-H6.*

Näiden havaintojen perusteella voisimme todeta, että riski laitteen rikkoontumisesta on suurempi kuin sen unohtamisesta, sillä siihen ei olla varauduttu. Yleensä laitteen unohduttua löytyy jokin kiertotie, kuinka saadaan MFA hyväksyttyä tai se voidaan käydä noutamassa. Rikkoontuessa taas se voi vaatia asiointia jopa ulkomaille asti.

> Mutta esimerkiksi Amazonin kanssa piti asiakaspalvelun kanssa jonnekkin Arizonaan jutella, vähän hankala. Et se on niinku semmonen vaikeus ja hankaluus, minkä oon kohdannu. *-H1.*

> Se blizzard oli juurikin, et piti skannata passia ja tämmöstä, että kyllähän siinä jonku verran vaivaa sai nähä, mutta onhan se ihan hyvä että ne haluaa tunnistaa sut, että se oot sinä varmasti, mutta onhan se kyseenalaista lähettää passista kopiota. En toki tiiä oisko parempaa tunnistautumista, paitsi nykyään toki pankkitunnistus. *-H2.*

Kaiken kaikkiaan käyttöönottoa ja käyttöä ei koettu erityisen hankalaksi vaan suurimmalle osalle se oli helppo tai neutraali asia. Riskejä MFA:n osalta tunnuttiin myös pitävän pieninä, sillä mitään erityisiä ongelmia ei haastateltavien mukaan ole ollut. Osa jopa vähän ihmetteli, että kuinka hyvin MFA on toiminut. Osa haastateltavista jäi vielä haastattelujen jälkeen pohtimaan sitä, että tulisiko laitteen katoamiseen tai rikkoontumiseen varautua paremmin, joka voidaan nähdä hyvänä asiana.

Haastateltavat myös mielellään käyttäisi MFA:ta myös paikoissa, missä se ei ole vielä mahdollista.

> Kaikkialla missä on mahdollista. -*H1.*
>
> On semmosia missä käyttäisin mieluusti autentikaattoria, mutta niihin ei saa kuin tilin ja salasanan. -*H2.*
>
> Kyllä sen hyvinkin palveluun ottais käyttöön missä mahdollisuus olis.

5.4 Turvallisuus

Turvallisuusosuudessa kyseltiin henkilöiden kokemuksia MFA:n tuomasta turvallisuudentunteesta ja onko se vaikuttanut henkilöiden turvallisuuskäyttäytymiseen. Kyseltiin myös yhdestä mahdollisesta tietoturvariskistä, eli ulkopuolisesta kirjautumisesta ja kuinka siihen on suhtauduttu. Salasanoihin liittyen vielä kysyttiin, että käyttävätkö he samaa salasanaa MFA:n kanssa ja ilman.

Kaikki haastatelluista kokivat olonsa turvallisemmaksi MFA:n käyttöönoton myötä, eli MFA:lla on selvästi positiivinen vaikutus ainakin turvallisuudentunteeseen.

> nojoooo, vois sanoa näinkin. Eipä sitä oikeen oo sattunukkaa mitään, mut kertahan se on ensimmäinenkin. Kai siitä semmonen pieni turvallisuuden tunne tulee. -*H2.*
>
> Kai, eihän sinne oo sen jälkeen enää kukaan kirjautunu, eli oikeestaan joo. -*H4.*
>
> Tietynlainen turva tulee siinä, se on ehkä vähän sellanen mitä ei tuu ajatalleeks ennen kuin se on tehny. Ettei kukaan tosiaan pääse. Mulla Uplayssa oli käytössä se ja joku oli yrittäny kirjautua, mutta ei ollu päässy kun oli käytössä. Se herätti sitten luottamusta. -*H7.*

Toisaalta myös saatettiin kokea myös negatiivisia tunteita palveluita kohtaan mihin MFA:ta ei saatu käyttöön:

> Koen turvalliseksi, mutta silti edelleen turvattomaksi. Mut se varmaan ei karise ikinä. Koen paljon turvallisemmaksi kuin sillain et on ilman. Nordnettiin ei saa 2FA:ta niin sitte se on must semmonen niinku asia, joka mua pelottaa, et miks tänne ei saa sitä, koska mä haluisin sen sinne. Mä koen sen palvelun sen takia turvattomaksi. Toki sä voit luoda niitä vastatilejä ja muita kiristellä sinne, mutta on jännä, kun rahotusalan palvelu ei tarjoa sitä. -*H1.*

H9 myös toi esiin näkökulman, että turvallisuuden tunne ei ole vain henkilökohtaista vaan turvaa myös ympärillä olevia. Ja tämä on tietysti totta, jos ajatellaan vaikka yritysympäristöä. Jos käytössä ei ole MFA:ta niin periaatteessa koko yrityksen tietoturva on heikoimman salasanan ja salasanakäyttäytymisen omaavan käsissä. Salasanakäyttäytyminen on myös MFA:n kanssa olennainen ongelma, sillä jos samaa salasanaa käytetään palveluissa, joissa MFA on käytössä ja joissa se ei ole käytössä niin kyseinen salasana on kutakuinkin yhtä turvaton, kuin kokonaan ilman MFA:ta. Haastatelluista 3/9 kertoi käyttävänsä aina-

kin joissain tapauksissa samaa tai samankaltaista salasanaa. H5 kertoi jopa, että hän käyttää vain kahta erilaista salasanaa ja nekin samankaltaisia, joka on suuri tietoturvariski, hänen ollessa opiskelija, ei riski kuitenkaan kohdistu esimerkiksi yritykseen vaan ainoastaan henkilökohtaisiin tietoihin.

Haastateltavilta kysyttiin myös, onko MFA kasvattanut heidän tietoturvatietoisuuttaan tai muuttanut käyttäytymistä myös muualla. Osa haastatelluista koki sen tuoneen tietoturvan arkipäiväisemmäksi ja vaikuttaneen käyttöönottoon myös muissa palveluissa:

> No on se madaltunu kynnys ottaa se muuallakin käyttöön. Ja sillee käyny kriittisemmäks pelkkää salasanasuojausta kohtaan. *-H3*

> Ehkä just koittaa pitää salasanaa sillee, että ei oo samaa joka paikassa. Miettii jos pääsee vaikka semmoseen missä on sama sähköposti ja sama salasana niin ei oo iso ponnistus mennä muuallekiin sisään. *-H7.*

> No näkyy se sillee että esimerkiksi tänään oli tullu oudosta numerosta viesti niin en sit lähteny klikkaileen. Et on semmosta tietoturva tietoutta itsessä tullu, että herkästi lähtee tarkistamaan talon IT-pojilta, että uskallanko avata liitteen. Herkemmin nykyään kysyy kuin klikkaa. *-H9.*

Toisena puolena taas sen ei nähty juurikaan vaikuttaneen käyttäytymiseen, koska asiat olivat jo selkeitä:

> Toi on tavallaan niin arkinen juttu varsinkin, kun on käyttäny 10 vuotta 2FA:ta niin sen välillä unohtaa, että kaikki ei käytä. *-H1.*

> Aika vaikea arvioida, en mä ehkä koe et mä oisin mitenkänä varovaisempi sen jälkeen, kun kaksvaiheisen tunnistautumisen ottanu käyttöön. Ehkä sitä oli jo ennenkin tota käyttöönottoa sillee suht tietoinen mahdollisista riskeistä ja tälläsistä. Ei se ihan hirveesti tietoa oo lisänny tai muuttanu käyttäytymistä hirveästi. *-H8.*

H4 toi myös mielenkiintoisen näkökulman keskusteluun oheisella kommentilla:

> Kyllähän se musta automaattisesti paremman ihmisen on tehnyt, mutta mun mielestä tämmösten toimintamallin käyttäminen viestii enemmän siitä tietoisuudesta kuin lisää tietoisuutta. *-H4.*

H4:n kommentti vaikuttaisikin tämän tutkimuksen perusteella pitävän pitkälti paikkaansa. Henkilöt, jotka ovat muutenkin tietoisempia tietoturvakäyttäytymisestään, kuten salasanoista, ovat ottaneet MFA:n hanakammin käyttöön. Tämän perusteella voisi olla mahdollista, että tietoturvatietoisuutta lisäämällä saataisiin ihmiset käyttäytymään turvallisemmin tietotekniikan kanssa. Tähän varmasti pätee samat lainalaisuudet kuin salasanakäyttäytymisen osalta. josta Adams & Sasse toteavat, että puutteellinen tietämys salasanakäytännöistä, sisällöstä ja murtamisesta on yksi juurisyy epäturvalliselle salasanakäyttäytymiselle (Adams & Sasse, 1999).

5.5 Johtopäätökset ja keskustelu

Tässä pro gradu tutkimuksessa haluttiin tutkia MFA:n käyttöönoton syitä ja kokemuksia käytöstä. MFA:n ollessa tutkimusaiheena vielä kohtalaisen uusi oli tarkoituksena myös tutkia kokonaiskuvaa mitä liittyy MFA:han tällä hetkellä. Tutkimuskysymyksinä olivat:

- Mitä käyttöönoton syitä oli MFA:lle?
- Millaisia käytön kokemuksia sinulla on MFA:sta?

Näiden lisäksi tarkoitus oli myös tutkia soveltuvuutta suuremmalle kansanosalle salasanan lisäsuojaksi. Haastatelluista kahdeksan olivat alan opiskelijoita/työntekijöitä/harrastelijoita ja vain yksi oli alan ulkopuolelta, joka teki ainakin viimeisen asian tulkinnasta vaikeampaa. Hänen kokemuksensa käyttöönotosta ja käytöstä kuitenkin oli hyvin samankaltainen muiden kanssa, joten tämän perusteella tutkimuksen tulos voisi olla laajennettavissa suuremmalle joukolle.

Käyttöönoton syitä oli, luonnollisesti, turvallisuuden parantaminen, palvelun ehdotus sekä työpaikalla käyttöönotto. Turvallisuuden parantamisesta ei kukaan erikseen maininnut, mutta kaikki olivat sitä mieltä, että se parantaa turvallisuutta, joten voidaan ajatella, että se on ollut pääsyy käyttöönotolle. Riskeistä puhuttaessa kukaan ei ollut kohdannut erityisiä riskejä, tai ei ainakaan ollut mahdollisia sellaisia. Tunnistautumiseen käytettävän välineen, sekä tunnistautumiseen käytettävän salasanan yhtäaikaista varastamista pidettiin niin epätodennäköisenä. Toisaalta osa henkilöistä käytti samaa salasanaa MFA:n kanssa ja ilman, jolloin voidaan pohtia, onko MFA enää hyödyllinen, usein kun pelkkä salasana voi riittää tilin palauttamiseen jollain keinolla.

Palvelun ehdottamana oli suurin osa haastelluista ottanut MFA:n käyttöön. He myös pitivät sitä merkittävänä tekijänä, etenkin rekisteröitymisvaiheessa. Tutkimuksessa kuitenkin tuli ilmi, että esimerkiksi palvelut missä on reaalista omaisuutta, kuten arvopapereita tai digitaalisia pelejä, vaikuttavat MFA:n käyttöönottoon huolimatta siitä ehdottaako palvelu sitä vai ei. Poikkeuksena henkilö, joka ei kokenut esimerkiksi verkkokaupassa MFA:ta tärkeäksi, vaikka siellä käsitellään luottokorttitietoja. Jos taas palvelu on käyttäjälle mitätön, kuten keskustelufoorumi ei MFA:n käyttöönottoa pidetty tärkeänä.

Moni henkilö oli ottanut MFA:n käyttöön työpaikalla, osa ensimmäisen käyttöönoton jälkeen ja osa ensimmäistä kertaa. Esimerkiksi yksi, joka ei käyttänyt tietotekniikkaa juurikaan arkielämässään oli ottanut MFA:n käyttöön työpaikalla ja pystyi myös suosittelemaan sitä muille. Työpaikan roolia MFA:n käyttöönoton edistäjänä tulisikin vahvistaa ja varmasti moni yritys on tähän ryhtynyt oman turvallisuutensa parantamisen vuoksi. Tässä kuitenkin tulee huomioida, että koulutuksen tarve on suuri, että ei paranneta vain oireita. Tietoturvatietoisuuden lisääminen luultavasti edistäisi MFA:n käyttöönottoa myös ihmisten arjessa.

Kolmen edellä mainitun käyttöönoton syyn lisäksi tutkimuksessa havaittiin, että hyvä salasanakäyttäytyminen oli selvästi liitoksissa MFA:n käyttöönottoon ja vieläpä mitä parempi salasanakäyttäytyminen sen todennäköisemmin MFA oli käytössä useammassa palvelussa. Hyvän salasanakäyttäytymisen omaavat kuitenkin ovat todennäköisemmin myös alan harrastelijoita tai ammattilaisia, joka varmasti vaikuttaa myös uusien turvallisuusteknologioiden käyttöönottoon myönteisesti. Kuitenkin voidaan nähdä, että myös salasanaturvallisuuden lisääminen, esimerkiksi salasanamanagerin käyttöönottoon opastamalla voisi johtaa myös innokkaampaan MFA:n käyttöön.

Käyttöön liittyvät kokemukset olivat pääosin myönteisiä. Käyttöönotossa ei juurikaan havaittu ongelmia, paitsi jos autentikointiin käytettävä laite oli rikkoontunut. Kukaan ei kokenut tätä erityisen hankalaksi ja palveluiden tarjoamat ohjeistukset pidettiin riittävinä käyttöönoton läpikäymiseen. Joskin osa oli sitä mieltä, että ensimmäinen kerta voi vaatia jonkinlaista tietoisuutta miksi palvelu tulisi ottaa käyttöön. Käytettävyyttäkin pidettiin hyvänä ja niin yksinkertaisena, kuin se vaan on mahdollista tuottaa. Käytettävyydessä havaittiin pieniä ongelmia esimerkiksi uudelleenkirjautumisvaatimuksen muodossa, näitä ei kuitenkaan pidetty mitenkään merkittävinä ongelmina.

MFA:n käytön nähtiin myös lisäävän käyttäjien turvallisuuden tunnetta, joten sillä on teknisen tietoturvan lisäksi myös positiivinen henkinen vaikutus. Tämä kuitenkaan ei vaikuttanut olevan merkittävässä roolissa MFA:n käyttöönottoa ajatellen. MFA:n käyttö myös lisäsi joissain tapauksissa hiukkasen tietoturvakäyttäytymistä myös muilla osa-alueilla. MFA:n käyttöönotosta voidaankin nähdä olevan hyötyä myös muuhun tietoturvatietoisuuteen ja ehkä jopa kiinnostukseen tietoturvaa kohtaan.

Merkittävimpänä ongelmana MFA:n kanssa voidaan pitää sitä, että autentikointilaitteen rikkoontumiseen tai katoamiseen ei olla juurikaan varauduttu. Henkilöillä on tiedossa, että yrityksen puhelin voidaan esimerkiksi tyhjätä etänä, mutta oman henkilökohtaisen laitteen palveluista ei tietoa ollut eikä niihin ollut varauduttu, ainakaan ennen ensimmäistä omakohtaista kokemusta. Pahimmassa skenaariossa MFA-tunnistautumiseen käytettävän laitteen katoaminen/rikkoontuminen voi johtaa hyvin epämieluisiin tilanteisiin, esimerkiksi matkalla ollessa. Tätä voidaan pitää yhtenä tutkimuksen kannalta merkittävänä tuloksena. Usea haastateltava olikin sitä mieltä, että varautumiseen tulisi panostaa enemmän.

Haastateltavat myös toivoivat, että MFA voisi olla käytössä useammassa palvelussa ja ottaisivat mielellään käyttöön sen myös muualla, missä se ei ole nyt mahdollista. Tämä on palveluntarjoajien kannalta tärkeä tieto, sillä MFA:n avulla he voivat huomattavasti parantaa käyttäjiensä tietoturvaa.

Edellä mainituilla perusteilla myös voimme vastata kysymykseen laajemmasta käyttäjäkunnasta. Käyttöönoton esteet ovat minimaaliset hyvien ohjeistuksien sekä autentikointiin käytettävän laitteen (puhelin) ollessa lähes aina käden ulottuvilla. Tämän lisäksi käytettävyyttä pidettiin todella yksinkertaisena eikä siihen liittynyt juurikaan turhautumisen tunteita pieniä poikkeuksia lukuun ottamatta, joka edesauttaa käyttöönottoa. Tulee kuitenkin huomioida, että

haasteltavan H9 tavoin, koulutuksen tarve käyttöönottoon on tarpeellista. Eikä pelkästään käytön koulutus vaan myös ymmärrys siitä miksi kyseistä teknologiaa tarvitaan, sillä niin voidaan edistää sen käyttöönottoa myös arkielämässä.

MFA:n käyttöönotto on suositeltavaa kaikille yksityishenkilöille ja yrityksille, sillä pelkkä salasana, etenkin tutkimusten osoittamalla salasanakäyttäytymisellä, ei ole riittävä. Tämän tutkimuksen perusteella käyttöönotto ei myöskään vaadi ylitsepääsemättömiä tietoteknisiä taitoja. Ennen kaikkea kiinnostus ja tietoisuus tietoturvasta riittää jo pitkälle käyttöönotossa. Koulutuksen tarvetta tietoisuuden lisäämiseksi tietoturvan osalta on ja tätä soisi käytävän työpaikoilla sekä eri kouluasteilla.

5.6 Jatkotutkimusaiheita

Tässä tutkimuksessa tutkittiin MFA:n käyttöönoton syitä ja siihen liittyviä kokemuksia. Kokemuksia saatiinkin laajasti ja joitain jatkotutkimukselle soveltuvia aiheita löytyi tutkimuksen edetessä.

Ensinnäkin tässä tutkimuksessa haastateltavaksi päätyi suurimmalta osin IT-alalla työskenteleviä tai harrastelijoita, vastaukset ja kokemukset voisivat olla hyvin erilaiset henkilöillä, jotka käyttävät tietotekniikkaa vähemmän, kuten perinteisillä aloilla työskentelevät tai vanhemmat, keski-iän ylittäneet sukupolvet.

Tutkimuksessa myös havaittiin, että henkilöt ei ole juurikaan varautuneet autentikointiin käytettävän laitteen rikkoontumiseen/katoamiseen. Tästä johtuvia seuraukset kuitenkin jäivät vähäisiksi tässä tutkimuksessa, koska tällaisia tapauksia ei ollut juuri tapahtunut tai ne saatiin ratkaistua kohtalaisen pienellä vaivannäöllä.

Tässä tutkimuksessa MFA:n toinen tunnistautuminen tapahtui puhelimen välityksellä, joko push up -ilmoituksena tai tunnistautumissovelluksen kautta. Tämä toinen tapa voi kuitenkin olla jokin muukin keino, kuten vaikka henkilökortti, kasvotunnistus tai puheäänen tunnistus. Jatkotutkimuksissa voitaisiinkin tutkia, kuinka nämä puhelimelle vaihtoehtoiset tunnistautumismenetelmät toimisivat käytännössä.

Viimeisimpänä tutkimusaiheena on koulutuksen ja tietoturvatietoisuuden merkitys MFA:n käyttöönottoon. Tässä tutkimuksessa havaittiin yhteys hyvän tietoturvatietoisuuden sekä MFA:n käytön välillä, kyse on kuitenkin pienestä otoksesta, joten tämä vaatisi vielä jatkotutkimusta.

6 Yhteenveto

Tässä tutkimuksessa on tutkittu MFA:n käyttöä ja kokemuksia siihen liittyen haastattelututkimuksen keinoin. Tarkoituksena oli selvittää mitä käyttöönoton syitä MFA:n käytölle on ja millaisia kokemuksia sen käytöstä on. Tarkoituksena oli myös selvittää MFA:n soveltuvuutta laajalle käyttäjäkunnalle.

MFA:n merkitys on tietoturvan alalla kasvava. Yleisimpänä tunnistautumiskeinona toimii edelleen salasana, jonka turvallisuus on tavallisen käyttäjän osalta huonohkoa. Jotta salasanoista voitaisiin tehdä tarpeelliseksi turvallisia pitäisi niiden merkkimäärän olla niin pitkä, että se vaikuttaa jo työskentelyn nopeuteen, jos salasanaa tarvitsee kirjoittaa usein. Huonon salasanakäyttäytymisen takia salasanat myös sisältävät muitakin tietoturvariskejä, kuin brute force-tyyppisen salasanojen murtamisen. Pahimmassa tapauksessa oma salasana on käytössä sekä työpaikalla että arkielämässä ja sen tietää useampi henkilö ja se on helposti saatavilla esimerkiksi tietokoneen viereen kirjoitetusta paperista.

MFA vaatii henkilöltä aina kahden eri tunnistautumismenetelmän käyttöä. Tunnistautumismenetelmät voidaan jakaa karkeasti kolmeen eri kysymykseen:

- Mitä omistat?
- Mitä olet?
- Mitä muistat?

Näiden lisäksi toki on kehitetty muitakin menetelmiä, kuten sijainti, eli ’missä olet?’. MFA:n ajatuksena kuitenkin on, että pelkästään yksilöivä tunniste, kuten salasana tai pin-koodi ei riitä sisäänkirjautumiseen vaan vaaditaan myös muu tunnistus käyttäjästä. Yleisin käytössä oleva MFA-sovellutus on mobiililaitteessa toimivat tunnistautumissovellukset ja puhelimeen tulevat push up -ilmoitukset. Matkapuhelin on suurimalla osalla ihmisistä käytössä ja yleensä se on myös käden ulottuvilla, jolloin ei tarvita erillistä laitetta varmistamiseen.

MFA:n käyttöönotto ja käytettävyys on tämän tutkimuksen perusteella yksinkertaista ja toimivaa. Suuremmilta ongelmilta on säästytty ja huonoja kokemuksia MFA:n käytöstä on vain vähän. Toisaalta varautuminen esimerkiksi puhelimen hajoamiseen yksityiskäytössä on vähäistä. Tämän seuraukset voi huonossa tapauksessa olla varsin epämiellyttävät. Työntekijän roolissa asia on

selvempi ja henkilöt pystyvätkin turvautumaan yrityksen IT-tukeen tällaisissa tapauksissa.

Turvallisuuden näkökulmasta MFA:n nähdään lisäävän henkilöiden turvallisuuden tunnetta, joka voidaan nähdä positiivisena asiana. Viitteitä on myös siihen, että MFA:n käyttöönotto vaikuttaa myös tietoturvatietoisuuden lisääntymiseen.

MFA lisää henkilöiden tietoturvaa huomattavasti etenkin niiden henkilöiden osalta, joiden salasanakäyttäytyminen on ”keskimääräistä” tutkimusten mukaan. MFA:n käyttöönotto voi myös olla yrityksen kannalta helpompi keino parantaa tietoturvaa, kuin noudattaa tiukkaa salasanapolitiikkaa. Tämän tutkimuksen perusteella MFA:n käyttöönotto ja käytettävyys on niin yksinkertaista, että sitä voidaan suositella kaikille, joskin koulutuksen tarve etenkin ei niin tietotekniselle henkilölle voi olla välttämätöntä.

LÄHTEET

Adams, A. & Sasse, M. A. (1999). *Users are not the enemy* ACM New York, NY, USA.

Adams, A., Sasse, M. A. & Lunt, P. (1997). Making passwords secure and usable. *People and computers XII* (s. 1-19) Springer.

Aloul, F., Zahidi, S. & El-Hajj, W. (2009). Multi factor authentication using mobile phones. *International Journal of Mathematics and Computer Science, 4*(2), 65-80.

Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E. & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security, 15*(5), 529-560.

Biddle, R., Chiasson, S. & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR), 44*(4), 1-41.

Braz, C. & Robert, J. (2006). Security and usability: The case of the user authentication methods. (s. 199-203)

Campbell, J., Ma, W. & Kleeman, D. (2011). *Impact of restrictive composition policy on user password choices* Taylor & Francis.

Corner, M. D. & Noble, B. D. (2002). Zero-interaction authentication. (s. 1-11)

Dagvatur, Z., Mohaisen, A., Lee, K., Nyang,D. (2019). Secure human authentication with graphical passwords. *Journal of Internet Technology, 20*(4) Haettu osoitteesta https://jit.ndhu.edu.tw/article/view/2100

Das, A., Bonneau, J., Caesar, M., Borisov, N. & Wang, X. (2014). The tangled web of password reuse. (s. 23-26)

Furnell, S., Esmael, R., Yang, W. & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security, 75*, 1-9.

Gnanaraj, J. W. K., Ezra, K. & Rajsingh, E. B. (2013). Smart card based time efficient authentication scheme for global grid computing. *Human-Centric Computing and Information Sciences, 3*(1), 16.

Grassi, P. A., Fenton, J. L. & Burr, W. E. (2017). Digital identity Guidelines–Authentication and lifecycle management: NIST special publication 800-63B.

Ives, B., Walsh, K. R. & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

Keith, M., Shao, B. & Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies, 65*(1), 17-28.

Kim, J. & Hong, S. (2011). A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems, 7*(1), 187-198.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., . . . Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. (s. 2595-2604)

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692.

Microsoft. (2017). Password policy. Haettu osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

Miettinen, M., Asokan, N., Nguyen, T. D., Sadeghi, A. & Sobhani, M. (2014). Context-based zero-interaction pairing and key evolution for advanced personal devices. (s. 880-891)

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2021-2040.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography, 2*(1), 1.

Proctor, R. W., Lien, M., Vu, K. L., Schultz, E. E. & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers, 34*(2), 163-169.

Puusa, A. & Juuti, P. (2020). Laadullisen tutkimuksen näkökulmat ja menetelmät. *Luettavissa: Https://Www.Bookbeat.Fi/Kirja/Laadullisen-Tutkimuksen-Nakokulmat-Ja-Menetelmat-224757 Luettu, 1*, 2020.

Sabzevar, A. P. & Stavrou, A. (2008). Universal multi-factor authentication using graphical passwords. (s. 625-632) IEEE.

Sasse, M. A., Brostoff, S. & Weirich, D. (2001). *Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security* Springer.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., . . . Cranor, L. F. (2010). Encountering stronger password requirements: User attitudes and behaviors. (s. 1-20)

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. & Furlong, M. (2007). Password sharing: Implications for security design based on social practice. (s. 895-904)

Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Stobert, E. & Biddle, R. (2014). The password life cycle: User behaviour in managing passwords. (s. 243-255)

Tam, L., Glassman, M. & Vandenwauver, M. (2010). *The psychology of password management: A tradeoff between security and convenience* Taylor & Francis.

Truong, H. T. T., Gao, X., Shrestha, B., Saxena, N., Asokan, N. & Nurmi, P. (2014). Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication. (s. 163-171) IEEE.

Weirich, D. & Sasse, M. A. (2001a). Persuasive password security. (s. 139-140)

Weirich, D. & Sasse, M. A. (2001b). Pretty good persuasion: A first step towards effective password security in the real world. (s. 137-143)

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies, 63*(1-2), 102-127.

Woods, N. & Siponen, M. (2018). *Too many passwords? how understanding our memory can increase password memorability* Elsevier.

Woods, N. & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies, 128*, 61-71.

Yampolskiy, R. V. (2006). Analyzing user password selection behavior for reduction of password space. (s. 109-115) IEEE, Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology.

Yan, J., Blackwell, A., Anderson, R. & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy, 2*(5), 25-31.

Zhang, J., Luo, X., Akkaladevi, S. & Ziegelmayer, J. (2009). Improving multiple-password recall: An empirical study. *European Journal of Information Systems, 18*(2), 165-176. doi:10.1057/ejis.2009.9

Zviran, M. & Haga, W. J. (1999). *Password security: An empirical study* Taylor & Francis.

LIITE 1 HAASTATTELURUNKO

Taustatiedot:

- **Ikä**
- **Sukupuoli**
- **Ammattinimike**
- **Tietotekninen osaaminen**
- **Laitteiden käyttö päivässä**
- **Suhtautuminen uusiin teknologioihin**

Autentikointimenetelmät:

- **Millainen suhtautuminen sinulla on salasanoihin? (Negatiiviset tunteet, tietoturva yms.)**
- **Pidätkö omaa salasanakäyttäytymistäsi turvallisena?**
- **Mitä muita autentikointimenetelmiä käytät?**
- **Otitko sen käyttöön vapaaehtoisesti vai ”pakotettiinko” käyttöön esim. töissä, miksi päätit ottaa sen käyttöön?**

Tekniset tekijät:

- **Oliko käyttöönotto helppoa?**
- **Onko käyttäminen mielestäsi helppo?**
- **Jos palvelu tarjoaa sulle käyttöönottoa niin otatko käyttöön?**
- **Saitko opastusta käyttöön vai opettelitko itse?**
- **Koitko käyttöönotossa joitain muita ongelmia?**

Ongelmat/riskit

- **Oletko havainnut ongelmia käytettävyydessä?**
- **Oletko unohtanut autentikointiin käytettävän esineen esim. kotia (Puhelin, älykortti, token, joku muu) ja mitä seurauksia siitä aiheutui?**
- **Onko kirjautumisesi joskus estynyt teknisen vian johdosta?**
- **Oletko varautunut siihen, jos autentikointilaitteesi rikkoontuu/katoaa? Tiedätkö miten toimia?**
- **Puhelimen tietoturva**

Turvallisuus:

- **Koetko olosi turvallisemmaksi tämän autentikointimenetelmän kanssa?**
- **Oletko törmännyt tietoturvariskeihin menetelmän kanssa?**
- **Oletko saanut ilmoituksen laitteeseesi kirjautumisesta, jota et itse tehnyt ja miten reagoit?**
- **Onko tämä vaikuttanut tietoturvakäyttäytymiseesi, kuten salasanoihin muissa palveluissa?**
- **Millaista salasanaa käytät autentikointimenetelmän kanssa? Käytätkö samaa salasanaa muualla?**

Muut:

- **Suosittelisitko tätä menetelmää muille?**
- **Käyttäisitkö tätä menetelmää töissä/kotona/muissa palveluissa jos se olisi mahdollista?**
- **Vaikuttaako appi tai sähköpostiviesti**
- **Muuta kysyttävää / sanottavaa?**